Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.4, Aug. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.4.897

기업의 정보보호 활동과 정보침해 사고 간의 관계: 정보보호 인식의 매개효과를 중심으로*

문 건 웅,† 김 승 주‡
고려대학교 정보보호대학원

Relationship between Information Security Activities of Enterprise and Its Infringement : Mainly on the Effects of Information Security Awareness*

Kunwoong Moon,† Seungjoo Kim‡
Center for information Security Technologies(CIST), Korea University

요 약

본 논문은 정보보호 인식을 매개로 기업이 정보보호 활동을 수행했을 때 정보보호 침해 사고 예방에 어떤 효과가 있는지에 초점을 맞춘다. 본 연구 모델로 정보보호 활동과 정보보호 인식이 정보보호 침해 사고를 감소시킨다는 가설을 설정하였다. 분석 대상의 일반적 특성은 빈도 분석을 실시하였으며, 측정 도구의 신뢰도는 Cronbach's α 계수를 활용하였으며 분석 결과, 정보보호 활동과 정보보호 인식 그리고 정보보호 침해 사고의 관계에 대한 가설이 입증되었다.

ABSTRACT

This paper focuses on how the protection of information security incident is effective in via Information security awareness when conducting information security activities of enterprises. Research models have theorized that the information security activity and the information security awareness will reduce the incidence of information security. The general characteristics of analysis targets have been carried out in the frequency analysis, and the reliability of the measuring tool has been utilized to calculate the coefficient of Cronbach's information protection. Evidence has been demonstrated regarding the relationship between information security activities and information security awareness and information security incidents.

Keywords: Information security, information protection, information activities, information awareness

I. 서 론

현대 사회는 나날이 증가하는 사이버 범죄로 인해 기업의 정보보호 활동이 강화되고 있다. 그래서 정보보호 투자에 대한 데이터의 수집이 필수적이다. 다행히 한국정보보호 진흥원인 KISA(Korea Internet and Security Agency)에서는 매년 '기업별 정보보호 실태 조사(A Survey of Information Security)'를 실시하여 기업 부문에 대한 정보보호에 대한 조사 결과를 발표하고 있다. 이 실태 조사에 따르면 2015년 기준으로 조사대상 중 정보보호 교육을 실시한 기업이 금융보험업의 경우 89.3%, 정보서비스업이 40.6% 이지만 전체 기업에서 정보보호 교육을 실시하는 비율은 14.9% 불과하다. 그리고 전체 기업의 18.6%만 정보보호 예산을 편성을 하였다[1]. 이렇게 기업이 정보보호 활동(정보보호 예산 편성)과 정보보호 인식의 제고(정보보호 교육)를 통해 침해사고를 예방하지 않는 것이 현실이다. 또한

Received(06. 10 .2017), Modified(07. 03. 2017), Accepted(07. 03. 2017)
* 이 논문(저서)는 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF- 2016S1A3A2924760)
† 주저자, mku5082@gmail.com
‡ 교신저자, skim71@korea.ac.kr (Corresponding author)

기업의 정보보호 활동이 정보침해 사고 예방에 대해 얼마만큼 효과적인지에 대한 상관관계를 판단하기는 아직까지 어렵다. 무엇보다 정보침해 사고 예방을 위해서는 정보보호 활동이 선행되어야 한다. 정보보호 활동은 정보 자산에 대한 관리적 보안, 시스템 분야에 대한 기술 보안, 그리고 시설에 대한 접근 제한을 위한 물리적 보안 등이다. 이러한 정보보호 활동 이외에도 정보보호에 대한 인식 전환이 필수적이다.

기존의 연구는 정보보호 활동인 관리적 보안, 기술적 보안 및 물리적 보안에 대해 개별적인 활동이 정보침해 사고 예방에 대해 어떤 영향을 미쳤는지에 대해서 이뤄졌다. 그러나 정보침해 사고 예방을 위한 또 다른 중요한 요소인 정보보호에 대한 인식 강화도 중요하며 이에 기반 한 정보보호 활동은 정보보호 인식을 전혀 고려하지 않은 정보보호 활동과 비교해 볼 때 더 높은 강도의 정보침해 사고 예방 효과를 얻을 수 있다.

그러므로 본 논문은 기업이 정보보호 활동을 수행했을 때 정보보호 인식을 매개로 정보침해 사고에 어떠한 효과가 있는지를 실증분석 하였다. 또한 정보보호 인식을 매개로 기업이 정보보호 활동을 수행했을 때의 정보침해 사고예방에 효과가 있는지도 알아본다. 기업은 이를 통해 정보 침해사고를 사전에 예방하기 위한 정보보호 시스템 구입 및 정보보호 운영 인력 고용 등의 정보보호 활동에 대한 예산 확보등을 위한 의사 결정에 도움이 될 것이고 정보보호 인식 제고를 위한 정기적인 정보보호 교육의 중요성에 대해 인식 변화를 이끌어 낼 수 있다. 또한 본 논문은 정보보호 활동과 정보보호 인식제고에 따른 정보침해 사고와의 관계성에 대해 실증분석을 통해 증명함으로써 학문적으로 기여한다.

이를 위해 먼저 Ⅱ장에서는 이론적 배경을 통해 기존의 정보침해 사고와 정보보호 인식에 대한 이론을 살펴본다. Ⅲ장에서는 연구 모형 및 가설을 세우고 Ⅳ장에서는 이에 대해 검증을 하고 Ⅴ장은 요약 및 후속 연구 과제를 논의한다.

Ⅱ. 이론적 배경

2.1 정보보호 활동과 정보침해 사고

정보보호(information security)란 정보를 여러 가지 위협으로부터 보호하는 것을 뜻하며 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 이러한 정보보호의 의미는 공급자 측면에서는 내외부의 위협 요인들로부터 네트워크, 시스템 등의 하드웨어 데이터 베이스, 통신 및 전산 시설 등 정보 자산을 안전하게 보호 및 운영하기 위한 일련의 행위를 뜻한다. 반면에 사용자 측면에서는 개인 정보 유출, 남용을 방지하기 위한 일련의 행위를 뜻한다.

이러한 정보보호의 정의는 출처에 따라서 다양하다. 먼저 ISO27000(2009)에서는 정보보호는 정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보존(Preservation)하고 추가로 진정성(Authentity), 책임성(Accountability), 부인방지(Non-repudation), 신뢰성(Reliability)이 포함된다고 말하고 있다[2].

CNSS(2009년)에서는 정보보호는 기밀성, 무결성 및 가용성의 영향에 좌우된다고 정의하였다[3].

ISACA(2008년)에서는 승인된 접근만 허용하고(기밀성) 부인방지를 포함한 부적절한 정보변경에 대해 감시하고(무결성) 적절하고 신뢰성 있는 정보의 접근만 보장(가용성) 하는 일련의 작업으로 정의하였다[4].

한편 정보에 대한 위협이란 허락되지 않은 접근, 수정, 노출, 훼손, 파괴 등이다. 정보에 대한 위협은 나날이 늘어가고 있기 때문에 모든 위협을 나열할 수는 없으나, Behrouz A. Forouzan(2010)[5]에 따르면 전통적으로 다음의 세 가지가 정보보호의 주요한 목표이다.

- 기밀성 : "기밀정보는 보호되어야 하며 조직은 정보의 기밀성을 위협하는 악의적인 행동들에 대응해야 한다."(p.2)
- 무결성 : "변경이 인가된 자에 의해서 인가된 메커니즘을 통해서만 이뤄져야 한다는 것을 의미한다."(p.2)
- 가용성 : "조직이 생산하고 저장하는 정보는 인가된 자가 사용할 수 있어야 한다. 이용할 수 없는 정보는 쓸모가 없다. 정보는 지속적으로 변화하고 이는 인가된 자가 접근할 수 있어야 한다는 것을 의미한다."(p.3)

한편 정보보호의 활동으로는 첫째, 정보자산에 대한 기업의 정보보호 활동에 대한 정책, 표준, 지침, 절차를 정의하고 이를 실행 감독하는 활동(관리적 보안), 둘째, 정보 시스템에 존재하는 취약점을 제거하고 정보시스템에 발생할 수 있는 외부로부터의 보안

위협을 차단하기 위해 정보 보호 시스템 구축, 운영하는 활동(기술적 보안), 셋째, 정보 자산이 위치한 시설에 대해 허가되지 않은 접근 또는 사용을 차단하고 모니터링하기 위한 활동(물리적 보안) 등이다.

위에서 언급한 정보보호 활동에 대한 선행 연구로는 정보침해 예방을 위한 정보보호 활동에 대한 연구로 김우환, 최중섭, 홍관희(2004)는 인터넷 침해 사고에 대한 추이와 이에 대처하기 위한 인터넷 침해 사고 대응 센터의 대응 체계를 분석하고 효과적인 대응 방안에 대해 연구하였다[6]. 이철수(2008)는 기술유출경험과 산업보안 역량수준 간의 분석에서 유출경험이 산업보안 역량 강화에 미치는 영향력이 미비하다는 것을 밝히면서, 정보보호를 자율적으로 기업에 맡기는 것 보다는 정부의 적절한 개입이 필요하다는 지적을 하였다[7]. 이정호(2008)는 시중 은행의 인터넷 뱅킹 침해사고 발생 현황 조사를 중심으로 최근 발생한 전자 금융 침해 사고의 추이 분석 및 원인과 기존 대응 체계의 현황과 한계점 등을 파악하고 공인 인증서를 중심으로 한 전자 금융 접근 매체의 관리 강화 방안을 제안하였다[8]. 노민선, 이상열(2010)은 중소기업의 산업 보안에 미치는 영향을 순위로직분석(Ordered Logic Analysis)을 사용하여 분석하고 그 결과를 바탕으로 정부 차원에서 추진해야 할 중소 기업에 대한 지원 사항과 보안 관련 정책 및 인식제고를 지원 확대 방안을 제시하였다[9]. 장항배(2010)는 중소기업 산업기술 유출 현황 조사 결과를 바탕으로 델파이 방법을 적용하여 중소기업 산업 기술 유출 방지 관리 체계를 설계하고 이에 대한 적합성을 검증하였다[10]. 최판암(2012)은 기업 정보보호 활동이 산업 기밀 유출 방지에 미치는 영향을 알아보고, 기업의 정보보호 활동이 기술적 측면에서 벗어나 관리적 요인에 중점을 두고 내부 구성원의 정보보호 인식 수준을 높여 관리되어야 함을 보여 주었다[11]. 김상현, 김근아(2012)는 정보보호 관리에 영향을 미치는 기업 환경 요소와 규제자 영향의 조절 효과를 연구하는 데 있어서 기업 환경 요소의 세 변수, 시장 불안정성, 업무 상호의존성, 보안관리 이점은 정보보호관리 인식에 긍정적인 영향을 미치는 것을 보여주었고 실증적 검증을 통해 정보보호 관리에 대한 관리 기준을 제시하였다[12]. 신일순, 장원창, & 박희영(2013)은 정보보호를 위한 기술적 대처에 적극적일수록 정보침해 사고를 경험할 가능성이 높다는 결과를 보여주었다[13]. 조성배, 권두순, 이미영(2014)은 국내 기업의 정보보호 행동에 영향을 미치는 영향 요인들을 파악하고 이들 요인이 기업의 정보보호 행동에 어떠한 영향을 미치는가를 실증 검증하였다. 기업의 정보보호 활동을 촉진할 수 있는 요인들을 찾아내기 위해 건강 신념 모델을 이용하여 연구 모형을 제시하였다. 분석 결과, 건강 신념 모델의 지각된 심각성, 지각된 개연성, 지각된 장애를 통해 매개 변수인 대응성에 유의한 영향을 미치고 종속변수인 기업 정보보호 행동에 유의한 영향을 미침을 보여주었다[14]. 손태연(2015)은 정보 보안성 및 정보 경영성과 간의 구조적 인과 관계를 실증적으로 검증하여 정보보호 활동의 성과와 실효성을 평가하고 경영성과 달성을 위한 합리적 운영 방향을 수립할 수 있도록 하였다[15]. 윤오준, 한복동, 박정근, 서형준, 신용태(2015)는 국가 기반 시설의 전산망 침해 사례와 관련 대책의 이행과정과 운영상 미비점을 분석, 평가하여 기반 업무 수행 체계 재정립, 기반 시설 지원 강화 및 의무 부과, 보안 점검 및 대응 훈련 강화 등 기반 시설 보호 강화를 위한 개선 방안을 제시하였다[16].

2.2 정보보호 인식의 매개효과

만약 자신에게 수신된 전자 우편 중 고위 공무원 부정축재자 명단이 첨부하였다는 메일을 받는다면 첨부를 열어볼 것인가? 만약 유명 금융 기관이 자신의 인터넷 뱅킹 이용 환경이 금융 기관의 시스템 변경으로 계좌 번호, 비밀 번호를 입력하라면 어찌하겠는가? 만약 인터넷 포탈을 검색 중 제대로 관심을 가진 사람이 솔깃한 정보가 있다면 클릭할 것인가? 만약 노트북이 필요한 상황에서 반값에 판매하는 사이트 정보가 있으면 이를 믿고 계좌에 돈을 입력할 것인가?

위에서 언급한 모든 사례가 인터넷을 이용하는 모든 사람이 자칫 잘못하면 자기도 모르게 걸릴 수 있는 온라인에서의 사기라고 할 수 있다.

이밖에도 한 조직에 근무하는 직원이 조직의 보안을 위하여 지켜야만 하는 많은 사항들이 있다. 물론 정보보호를 담당하는 직원이 만든 정보보호 기술 및 솔루션이 하지 못하는 많은 사항들이 직원 개개인이 지켜야만 하는 사항들이다.

정보보호 인식(Security Awareness)은 여러 가지로 정의될 수 있다. 대표적으로 사람들이 자신의 직무를 수행하는 데 있어, 정보보호의 함축된 상태를 잘 알 수 있도록 하는 프로세스이다. 여기에는 정보

보호의 중요성 인식, 보안사고 발생 시 이에 대한 대응 방안과 보고 체제 등이 포함된다[17].

정보보호 기술은 정보보호에 혼자서 생존할 수 없으며, 조직 구성원과 개인정보 보호책임 및 인식 제고 정보보호 프로그램 성공에 가장 중요하다.

조직의 정보 자산에 대해 보안 정책에 따라 조직 구성원에 대한 적절한 정보보호 인식 제고를 수행하여야 한다. 결국 정보보호 인식의 제고는 자산, 정책 및 정보보호 인식 교육이 자리 잡는 것이다.

정보보호 인식 제고는 정보보호 관리 모델에서 볼 때 조직의 정보보호를 이끌어가는 가장 큰 축의 하나이다.

정보보호 인식 제고가 성공적이라면 조직이 갖게 되는 사항은 다음과 같다.

- 조직의 보안 기능을 적절하게 사용할 수 있도록 해준다.
- 직원들이 이상한 보안 문제, 잠재적으로 악의가 있을 사항을 보고하게 한다.
- 보안의 심각성을 깨닫게 하므로 직원들의 근면함을 일깨운다.
- 조직의 위험관리 상 가장 중요한 것임을 깨닫게 한다.

정보보호 인식에 대한 연구 활동으로는 임채호(2006)는 정보보호 인식 제고가 무엇이며, 그 구현 방법, WebSTART를 통한 자기 학습 방법 등을 제시하였다[17]. 김종기, 강다연(2008)은 보안정책, 보안의식, 개인적 특성, 보안효과 간의 관계를 분석하여 보안정책이 보안의식에 영향을 미침으로써 보안효과를 제고한다는 결과를 제시하였다[18]. 이충희, 신민수(2010)는 다양한 동기 부여에 의해 어느 정도의 보안 행위가 이뤄지는지를 파악해 보고 개인의 보안에 대한 인식 수준에 따라서 동기 부여된 보안 행위의 정도에 차이가 있는지를 연구하였다[19]. 백민정, 손승희(2011)는 조직 구성원들의 개인적 차원의 정보보호 인식이 정보보호 행동을 통해 조직의 정보보호 성과에 미치는 영향을 분석하여 정보보호 인식이 정보보호 행동을 추동하여 정보보호 성과를 높인다는 결과를 제시하였다[20]. 장명희, 강다연(2012)은 항만 기업 종사자를 대상으로 정보보호 인식의 영향요인과 정보보호 인식과 정보보호 위험 간의 관계를 분석하였다. 분석결과 정보보호 교육과 의도는 정보보호 인식을 제고하는 요인으로 밝혀졌으며, 정보보호 인식은 정보보호에 대한 위험지각을 높이는 요인으로 밝혀졌다[21]. 손영수(2015)는 정보보호 서비스 활동에 영향을 미치는 요인을 알아보고자 기존 앤더슨 모형과 개인정보 보호 인지도를 매개하여 정보보호 서비스 이용과 정보보호 예방 채택 과정 모형에 미치는 영향을 분산 분석, 카이스퀘어 검증, 로지스틱 회귀 분석을 통하여 검증하였다[22]. 권은경, 이한솔, 채상미, 유경원(2016)은 포아송 회귀 분석 방법을 사용하여 기업의 정보보호 투자 중 정보보호 교육이 침해 사고에 미치는 영향에 대하여 실증 연구를 하였다. 또한 교육 대상을 관리자와 일반 직원으로 분류하여 살펴보고 정보보호 교육 서비스의 아웃소싱 여부에 따른 교육의 효과를 측정하였다[23].

상기의 선행 연구들은 조직 차원에서 정보보호 활동 또는 서비스와 정보보호 효과 간의 관계를 분석하거나 개인적 차원으로 정보보호 인식이나 동기가 정보보호 효과에 미치는 영향을 분석하고 있다. 그러나 정보보호 효과는 개인의 행동을 기반으로 나타나며, 개인의 행동은 조직의 정책이나 활동과 같이 동기부여 요인에 의해 강화될 수 있다는 관점에서 기업의 정보보호 활동과 개인의 정보보호 인식, 조직의 정보보호 성과 간의 관계를 복합적으로 고려한 연구는 아직까지 다소 미흡하다.

이에 본 연구에서는 기업의 정보보호 활동과 정보침해 사고 간의 관계를 정보보호 인식의 매개효과를 중심으로 연구하고자 한다. 이를 위해서 본 논문은 한국정보보호 진흥원인 KISA에서 매년 '기업별 정보보호 실태 조사'를 실시한 기업 부문을 대상으로 한 정보보호에 대한 조사 결과를 이용한다.

III. 연구 방법

3.1 연구 모형 및 연구 가설

본 연구에서는 기업에서의 정보침해 사고를 방지하기 위해서는 정보보호 활동이 우선되어야 함을 증명하고자 하였다. 그러나 기업에서의 정보보호 활동을 강화할지라도 개인의 정보보호 인식을 개선하지 않는다면, 그 성과는 기대에 미치지 못할 가능성이 많다. 이는 개인의 정보보호 인식이 정보보호 활동을 촉진하는 요인이기 때문이다.

이에 본 연구에서는 기업의 정보보호 활동과 개인의 정보보호 인식, 기업의 정보침해 간의 관계를 Fig. 1과 같이 설정하였다.

연구 모형에서 정보보호 활동은 정보보호 인식에 긍정적으로 작용할 뿐만 아니라 정보침해 사고를 감

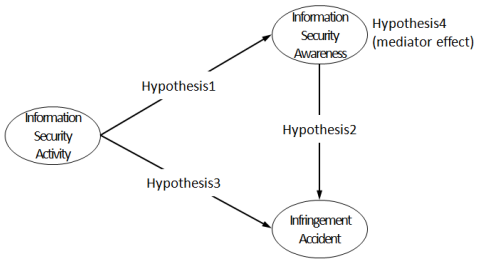

Fig. 1. Study model

소시키는데 영향을 미칠 것으로 예측하였다. 또한 정보보호 인식은 정보침해 사고를 감소시키는 영향이 있을 것이라 예측하였다. 마지막으로 정보보호 인식은 조직 내 구성원이 기업에서의 정보보호 활동과 정보보호에 대한 중요성의 인식 정도(박성욱, 이상호, 2008)로, 인식의 수준은 정보보호에 대한 관심 및 제반 규정 준수에 영향을 미치게 됨으로써 정보침해 사고의 발생 가능성을 감소시키게 된다[24].

연구 모형에 다른 가설은 다음과 같다.

가설 1. 정보보호 활동은 정보보호 인식에 정(+)의 영향을 미칠 것이다.

가설 2. 정보보호 인식은 정보침해 사고에 부(-)의 영향을 미칠 것이다.

가설 3. 정보보호 활동은 정보침해 사고에 부(-)의 영향을 미칠 것이다.

가설 4. 정보보호 인식은 정보보호 활동과 정보침해 사고 간의 관계를 매개할 것이다.

각 가설에 대한 관련 논문에 대해 선행연구 분석에 내용을 다시 정리하면 가설 1인 정보보호 활동과 정보보호 인식 간의 관계는 선행연구(최판암, 2011)의 연구에서 기업의 정보보호 활동이 산업기밀 유출 방지를 위한 정보보호 인식을 높인다는 사실을 밝혔다[11].

가설 2는 선행연구(이충희, 신민수, 2010)에서 조직의 정보보호 행위와 정보보호 인식 간의 관계는 긍정적으로 작용한다고 하였다[19].

가설 3은 선행연구(최판암, 2011)에서 정보보호 활동이 산업기밀유출 사고를 사전에 방지할 뿐만 아니라 효과적으로 대처하는 데 기여한다고 밝혔다[11].

가설 4는 선행연구(장명희, 강다연, 2012)에서 정보보호 인식에 대한 영향을 미치는 요인과의 관계성을 분석하였다[21].

3.2 연구 대상 및 자료

이를 위해 본 연구에서는 '정보보호 실태조사' 자료를 활용하였다. 한국인터넷진흥원 주관으로 실시하는 정보보호 실태 조사에서는 종업원 5인 이상의 사업체 가운데 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 사업체를 대상으로 정보보호 환경, 정보보호 정책, 정보보호 침해 사고로 인한 피해 현황 등을 조사하고 있으며, 정보보호와 관련된 투자, 정보보호 활동, 정보침해 사고 등과 관련된 연구에서 유용한 자료로 활용되고 있다. 정보보호 실태조사 자료는 다수의 기업(2015년도의 경우 8,000개 이상)을 다양한 산업분야에 걸쳐 정보보호에 관한 내용을 체계적으로 수집한 데이터로서 공신력있는 기관인 KISA에서 수행한 결과로 타 논문에서도 많이 이용되는 신뢰성 있는 자료이다[28].

이에 본 연구에서도 2015년 정보보호 실태조사에 응답한 8,121개 사업체의 자료를 바탕으로 실증 분석하였다.

표본설계를 위한 모집단은 통계청 "2013년 기준 전국사업체조사"의 업종별, 규모별 사업체수 및 분포 결과와 한국정보화진흥원 "2014년 정보화통계조사" 결과에서 파악된 네트워크 구축 비율을 이용하여 네트워크에 연결된 컴퓨터를 1대 이상 보유하고 있는 종사자 규모 1인 이상의 국내사업체로서 업종분류는 한국표준산업 분류를 기준으로 13개 업종으로 구분하였으며 Table 1과 같다.

표본추출은 다단계층화계통추출법으로 업종별 및 규모별로 2단 층화한 후 각 사업체들을 지역별로 정렬하여 계통추출을 하였다.

표본의 규모산정은 상대표준오차에 따른 표본의 크기 결정식인 다음 식 (1)을 이용한다.

$$n = \frac{(\sum_{h=1}^{L} W_h S_h)^2}{\sum_{h=1}^{L} W_h S_h^2 / N + (r \sum_{h=1}^{L} W_h P_h)^2} \quad (1)$$

여기에서

L : 층의 개수 (업종×규모)

S_h^2 : h층의 정보보호 정책 수립률의 분산

Wh:: 층별 가중치

N : 총 사업체수

P_h : h층의 정보보호 정책 수립률

$r = \frac{\sqrt{Var(P_{st})}}{P_{st}}$: 목표 상대표준오차

Table 1. Distribution of enterprises with over one employee

Section	Item	Number
Type of Business	Agricultural Fishing	2,763
	manufacturing	175,951
	Construction	61,645
	Wholesale and Retail	350,195
	Transportation	49.156
	Lodging and Restaura수	154,815
	Publication, Film, Broadcasting , Information&Communication	28,901
	Finance & Insurance	37,561
	Realestate & Leasing	63,614
	Specification, Science, Technology	63,450
	Facility Management & Business Support Management	26,245
	Association, Organization, Repair, Individual Business	139,267
	etc	334,964
	Total	1,488,527
Scale	1 - 4 persons	1,002,847
	5 - 9 persons	255,273
	10 - 49 persons	191,540
	50 - 249 persons	35,164
	250 - 999 persons	3,219
	more 1,000 persons	484
	Total	1,488,527

정보보호 정책 수립 여부에 대한 모수를 이용하여 표본크기를 결정하며, 상대표준 오차에 따른 표본의 크기는 아래 Table 2와 같다.

최종 표본의 크기는 상대표준오차가 0.011이 되도록 약 8,000개로 결정한다.

1차 표집틀(sampling frame)은 "2013년 기준 전국사업체조사" 대상 사업체이며 2차 표집틀은 "2014년 정보화 통계조사" 대상 사업체 중 네트워크 구축 사업체이다.

Table 2. Size of sample according to relative standard error

Relative Standard Error	Size of Sample
0.01	9,933
0.011	8,219
0.012	6,912
0.013	5,894
0.014	5,085
0.015	4,431
0.016	3,896
0.017	3,452
0.018	3,080

표본할당 및 추출방법으로서 멱등할당(Power allocation)을 하였는데 2014년도 조사결과 정보보호실태조사 중 '공식 문서화된 정보보호 정책 수립여부'에 대한 추정량을 이용하여 표본오차를 계산하고, p=0.4인 경우를 최적 할당으로 결정하였다. 절사추출로는 종사자수가 1,000명 이상인 사업체와 250~999명인 사업체 일부를 전수조사를 실시하였다[1].

3.3 변수의 정의와 특징

본 연구의 측정문항은 2015년 정보보호 실태 조사의 문항을 활용하였다. 정보보호 활동은 기업에서 정보보호를 목적으로 조직 내 정보 자산의 보안을 위해 구현한 관리 장치로서 기술적, 물리적 장치뿐만 아니라 관리적 장치를 포함하는 다차원적으로 구성된다[25]. 이를 바탕으로 본 연구에서는 정보보호 활동

을 관리적 요인, 기술적 요인, 시스템적 요인의 3개 요인으로 구성하였다.

먼저 관리적 요인은 정보보호 정책 및 조직, 교육, 예산으로 구성하였으며, 기술적 요인은 정보보호 시스템, 보안 점검으로 구성하였다. 시스템적 요인은 정보침해 예방과 사후 관리 체계 및 시스템 운영, 정보침해 대응 활동으로 구성하였다.

또한 정보보호 인식은 정보시스템 사용자 스스로의 인식하는 정보보호에 대한 중요성의 정도로 정보보호 체계 및 시스템에 대한 인식과 개인정보 보호 체계 및 시스템에 대한 인식으로 구성하였다.

정보보호 침해 사고는 네트워크 데이터 또는 시스템의 기밀성(confidentiality), 무결성(integrity) 또는 가용성(availability)을 해치는 컴퓨터 또는 네트워크에 대한 공격을 의미하며, 정보보호 침해 사고 유무와 침해 사고 경험 횟수로 구성하였다.

구체적인 측정 문항과 척도는 Table 3과 같다.

3.4 분석 방법

본 연구는 가설 검증을 위한 분석 방법으로 IBM SPSS Statistics 20.0과 IBM SPSS LISREL 9.2를 이용하여 분석하였다.

분석 대상의 일반적 특성은 빈도 분석을 실시하였

Table 3. Measurement item and criterion

Variable			Measurement Item	Value
General characteristics			Business Form	
			Organization Form	
			Industry	
			Scale(including temporary employee)	
information security activity	Administrative Factor	Policy	General	1=Yes, 0=No
			Privacy	
		Organization	Operation of organization	1=Yes, 0=No
		Education	Execution	1=Yes, 0=No
	Technical Factor	Operation of Information Security System	Network Security	Total Value : 0~9
			Terminal Security	Total Value : 0~4
			Information Leakage Security	Total Value : 0~6
			Authentication(Control)	Total Value : 0~7
			Security Management	Total Value : 0~8
	Systematic Factor	Response of Infringement	Prevention of Infringement and Management Structure	Total Value: 0~8
			Prevention of Infringement and Management System	Total Value: 0~6
Information Security Awareness			Structure	1=Not important ~5=Serious Important
			Privacy Security	
			System	
			Privacy System	
infringement Accident			Accident Status for one year	1=Yes, 0=No
			Number of Experiences	Total Value: 0~8

으며, 측정 도구의 신뢰도는 Cronbach's α 계수를 활용하여 확인하였다. 모형의 타당도 검증은 확인적 요인 분석으로 집중타당도(Convergent Validity)와 판별타당도 (Discrimination Validity)로 검증하였다.

판별타당도는 Fornell and Larcker(1981)[27]의 검증 방법을 따라 평균분산추출값(average variance extracted: AVE)을 계산하여 이의 제곱근 값과 개념 간 상관 계수의 값을 비교하여 모든 개념의 AVE 제곱근 값이 해당 개념과 여타 개념 간의 상관계수 값보다 크면 판별타당도가 확보된 것으로 판단한다.

모형의 적합도 검증은 χ^2, 적합지수(Goodness of Fit Index〔GFI〕), 근사오차평균자승의 이중근(Root Mean Square Error of Approximation〔RMSEA〕), 표준적합지수(Normed Fit Index〔NFI〕), 비교적합지수(Comparative Fit Index〔CFI〕), 증분적합지수(Incremental Fit Index〔IFI〕), 잔차평균자승이중근(Root Means Squar Residual〔RMR〕)을 이용하였다.

매개효과 검증을 위해 Baron & Kenny(1986)[26]의 절차에 의해 정보보호 활동, 정보보호 인식, 정보침해 사고 간의 단순 상관 계수가 유의한 가를 검토하였다. 또한 구조 모형에서 정보보호 활동이 정보침해 사고에 미치는 총효과와 간접 효과가 유의한가를 검토하였다. 마지막으로 Sobel 테스트를 통하여 매개효과의 유의성을 검토하였다.

IV. 분석 결과

4.1 분석 대상의 일반적 특성

본 연구의 대상인 2015년 정보보호 실태조사에 응답한 사업체는 총 8,121개로 일반적 특성은

Table 4. General properties of each items

Section	Item	Frequency	Percentage
Business Form	Single Company	5,305	65.3
	Head Quarter	1,179	14.5
	Factory/Branch	1,637	20.2
Organization Form	Private Business	2,309	28.4
	Corporation	4,538	55.9
	Incorporation	902	11.1
	Organization	372	4.6
Type of Business	Agricultural Fishing	332	4.1
	manufacturing	1,047	12.9
	Construction	634	7.8
	Wholesale and Retail	810	10
	Transportation	613	7.5
	Lodging and Restaura수	503	6.2
	Publication, Film, Broadcasting , Information&Communication	575	7.1
	Finance & Insurance	586	7.2
	Realestate & Leasing	493	6.1
	Specification, Science, Technology	675	8.3
	Facility Management & Business Support Management	727	9
	Association, Organization, Repair, Individual Business	491	6
	etc	635	7.8
Scale	1 - 4 persons	1,586	19.5
	5 - 9 persons	1,374	16.9
	10 - 49 persons	2,163	26.6
	50 - 249 persons	1,802	22.2
	250 - 499 persons	794	9.8
	more 500 persons	402	4.9

Table 4와 같다.

사업 형태는 단독 사업체가 전체의 65.3%로 가장 많았다. 공장 및 지사와 영업소를 보유한 사업체는 20.2%, 본사 및 본점 등을 보유하고 있는 사업체는 14.5%로 나타났다.

조직 형태는 회사 법인이 55.9%로 절반을 넘는 비중을 차지하고 있었으며, 다음으로 개인 사업체가 28.4%의 분포를 보였다.

업종별로는 제조업이 12.9%, 기술 서비스업이 8.3%, 운수업 7.5%, 금융 및 보험업 7.2%, 정보 서비스업이 7.1%의 순으로 나타났다.

규모에서는 10~49명이 26.6%, 50~249명이 22.2%, 1~4명이 19.5%의 순으로 나타났다.

4.2 주요 변수의 통계량

본 연구의 주요 변수인 정보보호 활동과 정보보호 인식, 그리고 정보침해 사고를 구성하는 세부 항목들의 기술 통계량은 Table 5와 같다.

정보보호 활동의 관리적 요인을 구성하는 세부 항목의 기술 통계량을 살펴보면, 정보보호 정책은 평균 0.390, 개인정보 보호 정책은 평균 0.380, 정보보호 조직 운영은 0.310, 정보보호 교육 실시는 평균 0.460으로 나타나 전체의 39%가 정보보호 정책이 있으며, 38%는 개인정보 보호 정책을 운영하는 것으로 나타났다.

또한 31%가 정보보호 조직을 운영하고 있으며, 46%가 정보보호 교육을 실시하는 것으로 파악되었다. 기술적 요인의 네트워크 보안을 위해 운영하는 시스템은 평균 3.009개로 나타났으며, 단말기 보안을 위해 운영하는 시스템은 평균 1.632개, 정보유출을 방지하기 위해 운영하는 시스템은 평균 1.035개, 인증 및 통제를 위해 운영하는 시스템은 평균 0.920개, 마지막으로 보안 관리를 위해 운영하는 시스템은 평균 1.475개인 것으로 나타났다. 시스템적 요인에서 정보침해 예방 및 사후 처리를 위한 체계는 평균 1.024개를 운영하고 있으며, 개인 정보의 안전한 처리를 위한 기술적 조치들은 평균 0.729개를 운영하고 있는 것으로 나타났다.

정보보호 인식에서는 전체적으로 5.0 만점에 평균 4.0이상으로 나타나 정보보호를 중요하게 인식하고 있는 것으로 분석되었다.

마지막으로 정보침해 사고 경험은 평균 0.030으로 나타나 전체의 약 3%가 정보침해 사고를 경험한 것으로 나타났으며, 경험 횟수는 평균 0.044개로 나타났다.

Table 5. Descriptive statistics of subsection

Variables	subsection	min	max	average	deviation
administrative factor	Policy of information security	0	1	0.390	0.487
	Policy of privacy	0	1	0.380	0.486
	Management of information security organization	0	1	0.310	0.461
	Education of information security	0	1	0.460	0.498
Technical factor	Network Security	0	9	3.009	2.994
	Terminal Security	0	4	1.632	1.611
	Information Leakage Security	0	6	1.035	1.802
	Authentication(Control)	0	7	0.920	1.709
	Security Management	0	8	1.475	2.313
Systematic Factor	Prevention of Infringement and Management Structure	0	8	1.024	2.349
	Prevention of Infringement and Management System	0	6	0.729	1.600
Information Security Awareness	Structure	0	5	4.280	0.881
	Privacy Security	0	5	4.320	0.862
	System	0	5	4.240	0.863
	Privacy System	0	5	4.280	0.871
infringement Accident	Accident Status for one year	0	1	0.030	0.182
	Number of Experiences	0	8	0.044	0.351

4.3 측정도구의 타당성과 신뢰성

본 연구에서는 주요 개념들을 구성하는 측정 문항들의 타당성과 신뢰성을 검증하기 위해 탐색적 요인분석과 확인적 요인 분석, 그리고 상관관계 분석을 실시하였다.

탐색적 요인분석 결과 Table 6와 같이 측정문항들은 각 변수로 적재되는 것을 확인하였다. 구체적으로 정보보호 활동은 관리적 요인과 기술적 요인, 시스템적 요인으로 적재되었으며, 정보보호 인식과 정보침해 사고는 각각의 단일 요인으로 적재되는 것으로 나타났다. 적재값은 최소 0.705로 기준인 0.5이상으로 나타났으며, 누적 분산 비율은 80.551%로 나타나 개념타당성은 양호한 것으로 확인되었다.

이와 같은 탐색적 요인 분석의 결과를 바탕으로 정보보호 활동은 관리적 요인, 기술적 요인, 시스템적 요인을 구성하는 각 측정값들의 합산값을 분석에 활용하였다. 또한 신뢰도 검증을 위해 Cronbach's α계수를 살펴본 결과 최소 0.706으로 기준인 0.6보다 높은 것으로 나타나 신뢰성도 확보되었다.

구조 모형을 통한 가설 검증을 위해 확인적 요인분석을 실시한 결과, Table 7와 같이 각 개념을 구성하는 측정치의 적재값(λ)은 모두 유의하며 상당히 큰 것으로 나타나고 있다. 또한 복합신뢰도(composite reliability: CR)는 모든 개념이 기준치인 0.6보다 큰 것으로 나타났다. 평균추출분산(AVE) 값도 기준치인 0.5보다 큰 것으로 나타나 개념타당성이 확보되었다.

판별타당성에 대한 검증을 위해 Fornell & Larcker(1981)[27]의 검증방법을 따라 평균분산추출값(average variance extracted: AVE)을 계산하여 이의 제곱근 값과 개념 간 상관계수의 값과 비교한 결과, Table 8과 같이 모든 개념의 AVE 제곱근 값이 해당 개념과 여타 개념 간의 상관계수

Table 6. Analysis results of measurement item

Concept	Measurement Item	Factor1	Factor2	Factor3	Factor4	Factor5
Information Security Awareness	Awareness of structure of privace	0.939	0.100	0.085	0.060	0.009
	Awareness of information security system	0.938	0.108	0.091	0.042	-0.031
	Awareness of privacy system	0.937	0.080	0.085	0.044	-0.020
	Awareness of privacy structure	0.925	0.111	0.093	0.049	-0.018
Administrative factor	Policy of information security	0.106	0.884	0.235	0.153	0.032
	Policy of privacy	0.110	0.884	0.226	0.159	0.035
	Education of information security	0.120	0.805	0.240	0.113	0.021
	Management of information security organization	0.100	0.744	0.314	0.204	0.060
Technical Factor	Authentication(Control)	0.075	0.044	0.788	0.164	0.015
	Security Management	0.070	0.260	0.770	0.235	0.032
	Information Leakage Security	0.101	0.279	0.768	0.219	0.003
	Network Security	0.090	0.455	0.705	0.147	0.044
	Terminal Security	0.091	0.273	0.688	0.017	0.013
Systematic Factor	Prevention of Infringement and Management System	0.079	0.265	0.294	0.877	0.052
	Prevention of Infringement and Management Structure	0.089	0.266	0.300	0.875	0.042
Infringement Accident	Accident Status for one year	-0.017	0.052	0.018	0.028	0.911
	Number of Experiences	-0.031	0.039	0.036	0.041	0.910
Characteristic Value		6.610	3.074	1.634	1.342	1.033
Variance Ratio(%)		38.885	18.080	9.614	7.895	6.077
Cumulative Variance Ratio(%)		38.885	56.965	66.579	74.474	80.551
Cronbachs'α		0.960	0.915	0.855	0.903	0.706

Table 7. Analysis results of factors

Concept	questions	적재값(λ)	t-값	CR	AVE
Information Security Activity	administrative factor	0.759	70.298	0.797	0.569
	Technical factor	0.820	76.554		
	Systematic Factor	0.677	62.086		
Information Security Awareness	structure of information security	0.893	102.895	0.959	0.856
	structure of privacy	0.911	106.443		
	system of information security	0.950	114.658		
	system of privacy	0.945	113.574		
Infringement Accident	Accident Status for one year	0.771	23.986	0.804	0.673
	Number of Experiences	0.867	24.291		

Table 8. Correlation of concepts

Concept	Information Security Activity	Information Security Awareness	Infringement Accident
Information Security Activity	0.754		
Information Security Awareness	0.302 (26.129)	0.925	
Infringement Accident	0.130 (9.591)	-0.042 -(3.323)	0.820

괄호안은 t-값, 대각선 값은 평균분산추출(AVE)의 제곱근 값임.

값보다 큰 것으로 나타났다. 이상의 분석 결과에 따라 연구 모형에 포함된 개념의 측정치는 판별타당성을 지닌 것으로 평가되었다.

4.4 가설 검증

본 연구에서는 정보보호 활동과 정보보호 인식, 정보침해 사고 간의 관계에 대한 가설을 검증하기 위해 구조방정식 모형을 활용하였다.

구조방정식 모형을 분석한 결과, Table 9과 같이 구조 모형의 적합도는 양호한 것으로 나타났다($\chi^2 = 448.78(df = 24, p = .000)$, GFI=0.894, RMSEA=0.089, NFI=0.914, CFI=0.915, IFI=0.915, RMR=0.022).

각 개념 간의 관계를 추정한 추정값을 살펴보면, 정보보호 활동(β=0.302, t=24.462, p<0.001)은 정보보호 인식에 직접적인 정(+)의 유의한 영향을 미치는 것으로 나타났다. 이는 정보보호 활동의 수준이 높을수록 정보보호 인식이 높아지는 경향이 있다는 것으로 정보보호 활동은 정보보호 인식에 정(+)의 영향을 미칠 것이라는 가설 1은 채택되었다.

정보보호 인식(β=-0.089, t=6.334, p<0.001)은 정보침해 사고에 직접적인 부(-)의 유의한 영향을 미치는 것으로 나타났다. 이는 정보보호 인식의 수준이 높을수록 정보침해 사고 경험이 낮아진다는 것으로 정보보호 인식은 정보침해 사고에 부(-)의 영향을 미칠 것이라는 가설 2는 채택되었다. 그러나 정보보호 활동(β=0.157, t=9.400, p<0.001)은 정보침해 사고에 직접적인 정(+)의 유의한 영향을 미치는 것으로 나타났다. 이는 정보보호 활동의 수준이 높을수록 정보침해 사고경험이 높아지는 경향이 있다. 이와 같은 결과는 정보보호 활동이 정보침해 사고를 감소시킬 것이라는 본 연구의 예측과 상반된 결과로 정보보호 활동은 정보침해 사고에 부(-)의 영향을 미칠 것이라는 가설 3은 기각되었다.

마지막으로 정보보호 활동과 정보침해 사고 간의 관계에서 정보보호 인식의 매개효과를 검증하기 위해 Sobel Test를 실시한 결과(Z=-6.110, p<0.001) 유의하게 나타나 정보보호 인식의 매개효과를 확인하였다. 이는 정보보호 활동은 정보보호 인식을 높여줌으로써 정보침해 사고를 줄이는 데 기여한다는 것으로 정보보호 인식은 정보보호 활동과 정보침해 사고 간의 관계를 매개할 것이라는 가설 4는 채택되었다. 이를 다이어그램으로 표현하면 Fig 2와 같다.

Table 9. Analysis results of structural model

route	ML value (β)	t value	p
Information Security Activity ↓ Information Security Awareness	0.302***	24.462	0.000
Information Security Activity ↓ Infringement Accident	0.157***	9.400	0.000
Information Security Awareness ↓ Infringement Accident	-0.089***	-6.334	0.000
(fit index) χ^2=448.78(df=24,p=.000), GFI=0.894, RMSEA=0.089, NFI=0.914, CFI=0.915, IFI=0.915, RMR=0.022			

*p<0.05, **p<0.01, ***p<0.001

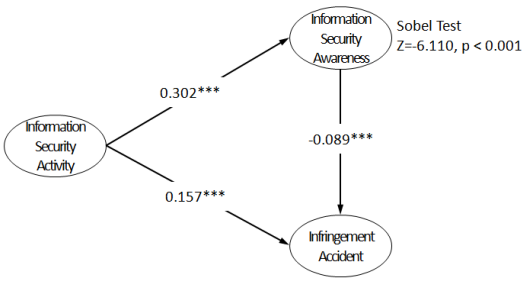

Fig. 2. Diagram of the Result

V. 결 론

본 연구는 정보보호 활동과 정보보호 인식, 정보침해 사고 간의 구조적 관계를 분석하는 것을 주요 목적으로 하고 있다. 이를 위해 한국인터넷진흥원 주관으로 실시하는 2015년 정보보호 실태 조사 원자료를 활용하여 8,121개 사업체의 자료를 바탕으로 실증분석 하였다.

분석 결과, 첫째, 정보보호 활동은 정보보호 인식을 강화시키는 요인임을 확인하였다. 이는 기업의 정보보호 활동이 조직 구성원으로 하여금 정보보호에 대한 인식을 제고시키는 역할을 할 수 있음을 의미하며 이 결과는 최판암(2011)의 연구에서 기업의 정보보호 활동이 산업기밀 유출방지를 위한 정보보호 인식을 높인다는 사실을 밝힌 것과 관련지을 수 있다〔11〕. 기업의 정보보호 활동은 정보침해 사고를 예방하기 위한 관리적, 기술적, 시스템적 활동으로 이는 조직구성원들이 정보보호의 중요성을 인식하고 이를 바탕으로 정보보호 행동을 추동하는 기제로 작용한다. 따라서 기업에서는 정보보호 인식을 제고하기 위하여 정보보호 활동을 강화할 필요성이 제기된다.

둘째, 정보보호 인식은 정보침해 사고를 감소시키는 요인임을 확인하였다. 이와 같은 결과는 조직구성원들의 정보보호 인식은 정보보호를 위한 제 규정 준수 및 정보보호 행동에 긍정적으로 작용하여 정보침해 사고를 사전에 예방할 수 있는 중요한 요인이라는 선행 연구(이충희, 신민수, 2010)에서 조직의 정보보호 행위와 정보보호 인식간의 관계는 긍정적으로 작용한다는 가설과 같은 맥락이며(가설의 입증은 없었음) 본 논문은 실증 분석을 통해 이를 증명하였다〔19〕. 따라서 기업에서는 정보보호 인식을 높이기 위한 다양한 교육과 정보보호를 중시하는 조직 문화의 구축이 필요할 것으로 보인다.

셋째, 정보보호 활동이 정보침해 사고를 감소시키는 데는 크게 영향을 미치지 못하는 것으로 나타났다. 이러한 결과는 정보보호 활동이 산업기밀유출 사고를 사전에 방지할 뿐만 아니라 효과적으로 대처하는 데 기여한다는 선행 연구(최판암, 2011)〔11〕와는 다른 결과를 보이고 있으나, 침해사고가 많은 기업일수록 정보보호 투자를 증가시킨다는 신일순, 장원창, 박희영(2013)〔13〕의 연구와 기업이 기술적 대책을 적극적으로 수립하고 정보보호를 위한 투자를 더 많이 할수록 침해사고를 경험할 가능성이 높아진다는 신일순(2016)〔28〕의 연구 결과와 맥락을 같이 하고 있다. 이와 같은 결과는 정보보호를 위한 활동이 정보침해 사고를 미연에 방지하는 사전적·예비적 행동이라기보다 정보침해 사고의 경험의 결과, 정보보호 활동에 적극적으로 임한다는 사후적 보완책으로 이루어지는 행동에 따라 나타난 결과로 해석된다. 이는 기업이나 개인들은 정보침해 사고 발생 전에는 정보침해 사고의 부정적인 결과나 정보침해 사고로 인한 파급효과를 크게 인식하지 못하는 점에 기인하는 것으로 보인다.

넷째, 정보보호 활동과 정보침해 사고의 간의 관계에서 정보보호 인식의 매개효과를 확인하였다. 이는 정보보호 활동은 정보보호 인식을 높여 정보침해 사고를 감소시킨다는 것으로 이에 관한 선행 연구에서는 가설만 세우고 실증분석을 하지 않거나(이충희, 신민수, 2010)〔19〕, 정보보호 인식에 대한 영향을

미치는 요인과의 관계성만을 분석(장명희, 강다연, 2012)[21]하였으나 본 논문에서는 실증분석을 통해 정보보호 활동과 정보보호 인식 그리고 정보침해사고의 종합적인 관계를 분석하였다. 정보보호 활동은 조직구성원들의 정보보호에 대한 인식을 높임으로써 정보보호에 관한 규정 준수나 행동을 촉진하여 정보침해 사고를 예방할 수 있다. 따라서 기업에서는 정보보호 인식을 높일 수 있는 교육을 강화하고, 정보보호를 위한 행동이 조직의 문화로서 확고히 자리매김을 할 수 있는 방안을 마련하는 것이 필요하다.

위의 연구결과에서 나타난 정보보호 활동, 정보보호 인식 및 정보침해사고의 관계를 토대로 하여 다음과 같은 대안 마련이 필요할 것으로 사료된다. 첫째, 기업 내부 관리적 측면에서 정보보호에 관한 규정과 활동지침 등을 명확히 해야 할 뿐만 아니라 정보보호 교육을 구체적으로 실행할 필요성이 있다. 형식적으로 수행하는 정보보호 교육이기보다는 실제 개인정보 침해사고 사례를 교육자료화하고 정보보호를 중요하게 생각하지 않을 경우 발생할 수 있는 각종 침해사고 사례를 시각화하여 전달함으로써 교육효과를 높일 수 있을 것으로 기대된다. 기업에서 정보교육 전담인력을 확보하지 못할 경우, KISA 및 관련 정보보호 기관과 연계하여 정기적인 교육을 시행하는 방안도 고려될 수 있다.

둘째, 사전적이고 예방적인 정보보호 활동을 위한 기업의 투자를 늘릴 필요성이 있다. 기술적·시스템적 측면에서 예방적 정보보호 시스템 운영의 적절성을 검토하여 비용 투자와 인력의 투입 등 적절한 조치의 필요성이 제기된다고 할 수 있다.

셋째, 기업의 정보보호 전반에 대한 정부는 적절한 개입방법의 일환으로 가이드라인을 통해 기업이 지속적인 정보보호 활동을 강화하도록 유도해야 한다. 즉 기업의 지속적인 정보보호 활동 강화를 위해서 기업의 IT예산 대비 정보보호 투자 예산의 비율을 확보하게 하여 기업이 정보침해사고에 대한 사전 대응을 하도록 유도하는 것이 바람직하다. 기업 자체적으로는 정보보호 예산을 확보하여 지속적인 정보보호 투자를 해야 한다. 정보보호 예산을 확보하기 위해서는 내부적으로 전체 IT 예산대비 최소 투자 비율을 지정하고 지속적인 정보보호 투자를 유도하고 정보보호 전담인력을 확보해야 한다.

넷째, 기업의 정보보호에 대한 경각심을 일깨워줌으로써 정보보호 활동에 적극성을 띠도록 할 필요성이 있음을 제안할 수 있다. 기업의 정보보호 강화 활동을 위해서는 제도적 측면에서 침해사고가 발생 시에도 제외신청형(opt-out) 집단소송제 등(개별 피해자가 제외신청을 하지 않는 한 가입신청이 없더라도 피해자로 추정되는 잠재적 집단 전체에 소송의 결과가 자동으로 미치도록 한 집단소송제)[29]을 적용하여 기업이 침해사고에 대한 대비를 소홀히 했을 경우 그에 대한 부담을 높게 하여 지속적인 정보보호 활동과 정보보호 인식 제고를 하도록 함이 바람직할 것으로 보인다.

이상의 논의를 통하여, 본 연구는 기업의 정보보호 활동, 정보보호 인식 및 정보침해 사고 사이의 관련성을 종합적으로 분석하고 결과를 도출하였다. 즉 정보보호 인식을 높여줌으로써 정보침해 사고를 방지할 수 있다는 것을 확인하였고 기업이 정보보호 성과를 높이기 위해서는 기업의 거시적 노력도 중요하지만, 조직 구성원 개인의 인식도 중요하다는 것을 규명하였다. 특히 정보보호를 위해서는 기업의 투자 및 기술개발에 중점을 두고 논의 했던 기존 연구와는 달리 기업과 개인적 차원의 노력이 같이 진행되어야 실질적인 정보보호 성과를 거둘 수 있다는 점을 밝혔다는 점에서 일차적 의의를 찾을 수 있다.

또한 본 연구는 기업 정보보호 활동으로부터 얻을 수 있는 시사점을 밝히고 나타난 문제점을 보완·강화할 수 있는 대안을 제시하였다. 즉 개인적 수준의 정보보호 인식뿐만 아니라 기업 차원의 정보보호 활동 강화 및 정부 차원의 지원을 제시하였다.

이와 같은 연구는 그동안 정보보호 성과를 기업적 측면과 개인적 측면을 구분하여 살펴본 연구들과는 달리 각각의 측면들 사이의 관련성을 살펴봄으로써 종합적으로 분석하였다는 점에서 정보보호에 관한 연구영역의 확대에 기여함은 물론 후속 연구의 가능성을 확장시킬 수 있을 것으로 기대된다.

References

[1] Jooy-young Kim, Chan-Hyung Cho, and Jung-Hun Lee, You-Jin Lee, "2015 Survery on information security(business)," KISA, 34205, pp. 27-28, 30, Dec. 2015.

[2] ISO(International Organization for Standardization)/IEC(International Electronical Commission), "ISO/IEC 27000:2009 - information security -

Security techniques - information security management systems - overview and vocabulary," ISO/IEC, 2009.
[3] CNSS(Committee on National Security System), "National information assurance (IA) glossary, CNSS instruction," 4009, Apr. 2010.
[4] ISACA(Information Systeam Audit and Control Association), "Glossary of terms 2008," ISACA, p. 10, p. 25, p. 51, 2008.
[5] Behrouz A. Forouzan, "Cryptography and network security," Mcgraw Hill Korea, 2, pp. 2-3, Dec. 2010.
[6] Uh-han Kim, Jung-Sup Cho, and Kwan-Hee Hong, "Present condition of infringement accident of information technology and response system," Journal of The Korean Institute of Communications and Information Science, 21(9), pp. 38-47, Sep. 2004.
[7] Chul-Soo Lee, "Information security auditing framework in industrial control system," Journal of the Korea Institute of Information Security & Cryptology, 18(1), pp. 139-148, Feb. 2008.
[8] Jung-ho Lee, "Prevention of infringement of electronic finance and reinforcement for action," Journal of the Korea Institute of Information Security & Cryptology, 18(5), pp. 1-20, Oct. 2008.
[9] Mean-Sun Noh and Sam-Youl Lee, "Explaining industrial security of SMEs in Korea: An Ordered Logit Analysis," Korean Public Administration Review, 44(3), pp. 239-259, Aug. 2010.
[10] Hang-Bae Chang, "The design of information security management system for SMEs industry technique leakage prevention," Journal of Korea Multimedia Society. 13(1), pp. 111-121, Jan. 2010.
[11] Pan-Am Choi, "The effects of corporate information protection activities on industrial secrets leakage prevention," Graduate School, Kyonggi University, Jun. 2012.
[12] Sang-hyun Kim and Geuna Kim, "A firm's environmental determinants impacting the information security management and the moderating effects of regulatory influence," Korean Operations Research And Management Society, 37(3), pp. 79-94, Sep. 2012.
[13] Il-soon Shin, Won-chang Jang and Heeyoung Park, "Information security investment and security breach: empirical study on the reverse causality," Journal of the Korea Institute of Information Security & Cryptology, 23(6), pp. 1207-1217, Dec. 2013.
[14] Sung-Bae Cho, Do-Soon Kwon and Mi-Young Lee, "A study on the information security behavior of corporations using health belief model," Asia Pacific Journal of Small Business, 36(2), pp. 241-263, Jun. 2014.
[15] Tae-Hyun Son, "The effects of corporate information security activities on the performance of information security and information management," Graduate School, Myongji University, Feb. 2015.
[16] OhJ-un Yoon, Bok-Dong Han, Jeong-Keun Park, Hyung-Jun Seo and Yong-Tae Shin, "A study on models for strengthening infrastructure protection through analysis of cyber intrusions," Convergence security journal, 15(6), pp. 29-36, Oct. 2015.
[17] Cho-Ho Lim, "Effective way of awareness-raising of information security," Journal of the Korea Institute of Information Security & Cryptology, 16(2), pp. 30-36, Apr. 2006.
[18] Jong-ki Kim and Day-eon Kang, "The effects of security policies, security awareness and individual characteristics on password security effectiveness," Journal of the Korea Institute of Information Security & Cryptology, 18(4), pp.

123-133, Aug. 2008.
〔19〕 Choong-Hee Lee and Min-soo Shin, "A study about a relationship between internal & external motivation and security action and influence of security recognition," Journal of Korea society of management information system, pp. 437-442, Aug. 2010.
〔20〕 Min-Jung Baek and Seyung-Hee Sohn, "A study on the effect of information security awareness and behavior on the information security performance in small and medium sized organization," Asia Pacific Journal of Small Business, 33(2), pp. 113-132, Jun. 2011.
〔21〕 Myung-Hee Chang and Da-Yeon Kang, "Factors affecting the information security awareness and perceived information security risk of employees of port companies," Journal of Korean Navigation and Port Research, 36(3), pp. 261-271, Apr. 2012.
〔22〕 Young-su Son, "A study on the relationship between cognition of personal information protection and following protection activities," Sang Myung University, Feb. 2015.
〔23〕 Un-kyung Kwon, Han-sol Lee, Sang-mi Chae and Kyung-won Lyu, "An empirical study of relationship between information security education and information security incidents," Journal of Korea society management information system, pp. 342-348, Aug. 2016.
〔24〕 Sung-Uk Park and Sang-Ho Lee, "An analysis on information security industry in Korea," Study of industry innovation, 24(2), pp. 1-22, Sep. 2008.
〔25〕 Von Solms, B, "Information security-the fourth wave," Computers & security, vol. 25, no. 3, pp. 165-168, Mar. 2006.
〔26〕 Baron, R. M. and Kenny, D. A, "The moderator - mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations," Journal of personality and social psychology, vol. 51, no. 6, p. 1173, Dec. 1986.
〔27〕 Fornell and Larcker, "Factor analysis and discriminant validity: a brief review of some practical issues," Aston Business School, May. 1981.
〔28〕 Il-soon Shin, "Effects and causality of measures for personal information : empirical studies on firm and individual behaviors and their implications," Journal of the Korea Institute of Information Security & Cryptology, 26(2), pp. 523-531, Mar. 2016.
〔29〕 Suk-Hun Shin, "Issues and tasks of exemplary damages and class action system," Korea economic research institute, p. 16, Oct. 2016.

〈저자소개〉

문 건 웅 (Kunwoong Moon) 정회원
1999년 2월: 고려대학교 금속공학과 졸업
2000년 8월: 고려대학교 컴퓨터학과 졸업
2012년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 정보침해 사고 예방

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊 한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년 :국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년 :방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 12월~현재: 카카오 자문위원
2016년 1월~현재: 한국정보화진흥원 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable security