https://doi.org/10.15813/kmr.2021.22.1.015

정보보호 공시제도의 운영실태와 효과성 분석[1)]

A Study of the Effectiveness and Status of the Information Security Disclosure System

백승준 (Seung Jun Baek) 한국정보통신진흥협회[2)]
이홍주 (Hong Joo Lee) 가톨릭대학교[3)]

〈 국문초록 〉

정보보호 공시제도는 이해관계자 보호 및 알권리를 보장하고, 기업의 자발적인 정보보호 투자를 촉진하기 위하여 2016년부터 시행된 제도이다. 정보보호 공시제도(ISDS)에 대해서는 해당 제도의 시행을 촉구하는 연구들이 있었으나, 제도 시행 후에 공시된 내용을 분석하거나 개선방향을 제시하는 연구는 부족한 편이다. 본 연구에서는 정보보호 산업진흥 포털에 2020년까지 공시되었던 정보보호공시의 내용을 분석하여 그 현황을 정리하고, 제도의 개선방향을 제시하였다. 공시제도를 통해 정보보호 관련 정보를 공개한 기업들에서 전담인력을 늘리는 경우가 있었으며, 정보보호 관련 인증을 취득하기도 했음을 알 수 있었지만, 투자의 증/감에는 영향을 발견하지 못했다. 현재의 공시제도는 개별 기업들이 공시를 해야하는 유인을 주는 데 어려움을 가지고 있기 때문에 활성화되지 못하고 있고, 이로 인하여 제도의 취지였던 기업의 정보보호 위험을 이해관계자들에게 공개하는 것이나 기업의 정보보호 투자를 활성화하는 것을 달성하지 못하고 있다. 현재 의무화되어 활성화되고 있는 정보보호 관리체계 인증제도(ISMS)에 포함하여 활성화하는 방안을 제시하였으며, 현재의 공시제도에서 기업의 이해관계자나 고객이 공시의 내용을 확인하는 것이 어렵기 때문에 이를 보다 인지하기 쉽도록 하는 방안으로 개인정보 처리방침 또는 개인정보 이용내역 통지의 내용에 포함하는 방법을 제시하였다.

주제어: 정보보호 공시제도, 정보보호 관리체계, 정보 보안, 정보보호 정책

---

1) 이 논문은 2017년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구이며 (NRF-2017S1A5A2A01025690), 2020년도 가톨릭대학교 교비연구비의 지원을 받았습니다.
2) 제1저자, sjbaek@kait.or.kr
3) 제2저자, 교신저자, hongjoo@catholic.ac.kr

논문접수일 2021년 01월 20일 | 1차 수정 2021년 03월 03일 | 게재확정일 2021년 03월 10일

1. 서론

기업의 위험 관리 측면에서, 정보보호는 이제 중요한 영역이 되었다(김기현 외, 2020; 권영옥, 김병도, 2007; 홍일유 외, 2015; 황해수, 이희상, 2015). 최근 5년 사이의 가장 큰 개인정보 유출사고 였던 A사 개인정보 유출사고는 약 천만명 이상의 개인정보가 유출되었었다. 이 사고로 인하여 A사는 정보통신 서비스 부문 매출액의 1.5%인 44억 8천만원의 과징금을 추징받았으며, 아직까지도 이에 대한 행정소송과 유출 피해자로부터의 민사소송을 치르고 있다. 지난 2019년 11월에는 B사 등 개인정보보호 법규 위반사업자에 대한 과징금 부과가 있었는데, 이 부과에 관한 사례는 이슈가 되었다. 일시적인 시스템 장애 상황에서 이십명 정도의 유출이 벌어진 것이나, 방통위에서는 18억원이라는 액수의 과징금을 처분한 것으로, 피해자당 1억원 정도의 과징금이 부과된 것이다. 이제 회사의 보안사고로 인해 직접 영향을 받게 되는 고객은 물론이고, 회사의 금전적 피해로 인해 영향을 받게 되는 채권자, 주주 등의 이해관계자도 회사가 어느 정도의 보안 수준을 가지고 있는 지 알 필요가 있다 (백승익, 정유영, 2014).

이를 위해 기업들이 정보자산을 효과적으로 보호하고 있는 지를 인증하는 정보보호 관리체계 인증과 정보보호 활동에 대해 공시하도록 하는 정보보호 공시제도를 운영하고 있다. 정보보호 관리체계(ISMS) 인증은 기업이 각종 보안위협으로부터 정보자산을 보호하기 위해 수립, 관리, 운영하는 종합적인 체계의 적합성에 대해 인증을 부여하는 제도이다. 개인정보 보호(PIMS)와 통합된 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)도 운영하고 있다. ISMS는 정보보호 관리체계 수립 및 운영에 대한 4가지 분야, 보호대책 요구사항에 대한 12가지 분야를 검토하여 인증을 부여한다. ISP, IDC는 의무대상자이며, 매출규모와 방문자 수에 따라 상급종합병원, 학교, 사업자, 정보통신서비스 사업자도 인증 의무대상이 된다. 의무대상자는 아니지만 기업이 자율적으로 인증을 신청할 수 있다[1].

정보보호 공시제도(과학기술정보통신부, 2019)는 이해관계자 보호 및 알권리를 보장하고, 기업의 자발적인 정보보호 투자를 촉진하기 위하여 2016년부터 시행된 제도이며, 기업이 행하고 있는 중요 정보보호 활동을 공개하도록 하고 있다. 그러나 제도 시행은 5년이 경과하였으나 정보보호 활동 공지가 의무 사항이 아니기에 활성화되어 있지 못하다. 2020년 말까지 공시를 했었던 회사는 52곳뿐이며, 그나마 그 중 7개사는 공시를 중단하였다. 2019년 초에 정부에서는 가이드라인을 개정하면서 공시 제도를 보다 쉽게 할 수 있도록 하였으나, 2019년에 새로 공시를 한 곳은 11곳, 2020년에 새로 공시를 한 곳은 19곳에 그치고 있다. 그나마 2018년까지 공시를 하였던 곳 중 1곳이, 2019년까지 공시를 하였던 곳 중 4곳이 공시를 중단하기도 하였다. 이에 따라 제도의 목적이었던 기업 정보의 공개를 통한 이해관계자 보호, 정보보호 투자의 촉진에 대해서는 그다지 효과가 발생하지 않고 있다.

정보보호 관리체계(ISMS) 인증 등 정보보호 강화를 위하여 시행되고 있는 제도들에 대한 연구는 많은 편이며(배영식, 2012), 특히 ISMS는 의무화 이후에 여러 가지 분석 연구가 있었다(공희경 외, 2016; 조중기, 최상현, 2016). 정보보호 공시제도에 대해서는 해당 제도의 시행을 촉구하는 연구들이 있었으나(전효정, 김태성, 2012), 제도 시행 후에 공시된 내용을 분석하거나 개선방향을 제시하는 연구는 부족한 편이다. 본 연구는 정보보호산업진흥포털에 2020년까지 공시되었던 정보보호 공시의 현황과 내용을 분석하여 공시 업체와 주요한 공시 정보를 파악하였다. 이를 통해 정보

1) 한국인터넷진흥원 https://isms.kisa.or.kr/main/

보호 공시제도의 도입 목적에 부합하게 제도가 운용되고 있는 지를 분석하고, 현황에 비추어 제도 활성화를 위한 개선방향을 제시하고자 한다.

2. 선행 연구

조직의 정보보호를 어떻게 향상시킬 수 있는 지에 대해서 많은 연구가 수행되었다. 조직의 정보보호에 영향을 미치는 요인을 파악하는 연구들이 수행되었으며, 정보보호 관련제도의 도입이 기업 가치와 정보보호 활동에 미치는 연구들도 수행되었다. 정보보호와 같이 조직입장에서 비용으로 인식되는 활동에 대해서는 규제나 관련 제도 등이 많은 영향을 미친다. 정보보호가 조직 활동에 미치는 영향과 정보보호 분야의 인증 제도 도입이 기업에 미치는 영향을 분석한 연구를 정리하였다.

2.1. 정보보호와 조직 활동

조직의 정보보호 활동에 영향을 미치는 조직 구성원의 특징 및 조직 요인은 다양한 방면에서 분석되었다(Bulgurcu et al., 2010; Cram et al., 2019; Spears and Barki, 2010). Cram et al. (2019)는 메타 연구를 통해서 다양한 연구들이 제안한 정보보호 준수에 영향을 미치는 선행 요인을 파악하였다. 합리적 행동이론(Theory of reasoned action) 또는 계획 행동이론(Theory of planned behavior)을 적용한 연구가 있었으며(Bauer and Bernroider, 2017; Bulgurcu et al., 2010; Foth 2016; Ifinedo 2012; Siponen et al., 2014), 억지 이론(deterence theory)(D'Arcy and Herath, 2011)과 보호 동기이론(protection motivation theory)(Boss et al., 2015) 또한 다양한 관점에서 적용되었다.

정보보호에 대한 태도(attitude)와 규범적 신뢰(normative beliefs)와 같은 태도 요인, 인지된 효용과 유용성(perceived benefits/usefulness), 보상(rewards), 자기 효능(self efficacy)과 같은 긍정적인 요인, 발각 정도(detection certainty), 벌칙 수준(punishment severity), 비용(response cost)과 같은 부정적인 요인들의 영향도 많이 분석되었다. 조직구성원의 정보보호 원칙 준수와 태도에는 준수에 따른 이익과 비용, 준수하지 않았을 때의 비용이 영향을 미치는 것으로 파악되었다(Bulgurcu, Cavusoglu, and Benbasat, 2010).

준수에 따른 이익에는 안전과 조직의 보상, 내적인 효용이 포함되었고, 준수에 따른 비용에는 업무 방해를 사용하였다. 준수하지 않았을 때의 비용으로는 내적인 비용, 취약성이 분석되었다. 조직 구성원의 정보보호활동 참여가 조직 수준의 정보보호 인식과 성과에 긍정적인 영향을 미치는 것으로 분석되었으며(Spears and Barki, 2010), 개인의 정보보호 활동 뿐만이 아니라 조직 구성원 집단의 정보보호 활동이 조직의 정보보호 성과에 영향을 미치는 것으로 파악되었다(Yoo, Goo, and Rao, 2020).

2.2. 정보보호 인증이 기업가치에 미치는 영향

조직의 보안 투자나 정보보호 인증이 기업가치에 미치는 영향 또한 연구되었다(박재영, 정우진, 김범수, 2016; 박재영, 정우진, 2019; 신현민, 김인재, 2020; 엄재하, 김민정, 2016). 사건연구 방법론을 활용하여 정보보호 인증이라는 사건이 기업가치 변동에 단기적으로 영향을 미치는 것을 밝혔으며, 사건에 시장이 긍정적으로 반응했다(박재영, 정우진, 김범수, 2016). 또한 기업의 정보보호 공시에도 시장이 긍정적으로 반응했다는 것을 밝혔다(박재영, 정우진, 2019). Lee et al. (2016)는 PCI-DSS 제도를 중심으로, 표준 준수와 컴플

라이언스가 통제에 주는 영향에 대하여 다루고, 회사의 보안과 사회적 복지 측면에서 최적의 표준과 표준의 문제점이 무엇인지 분석하였다.

공희경 등 (2016)은 정보보호 인증 및 제도에 대한 경제성 관련 연구에 대하여, 29개의 논문 및 보고서를 분석하여 주제중심으로 분류하였다. 이를 통하여 연구 동향을 보안 인증 및 제도에 대한 연구, 보안인증 및 제도의 경제적 효과에 대한 연구, 표준의 경제적 효과에 대한 연구 3가지로 분류하고, 연구 방법론으로는 정확한 수치를 제시하는 정량적인 연구보다는 사례조사 등의 경험적 연구와, 기존 제도의 문제점 및 개선방향을 도출하는 연구 및 정책의제에 관련된 연구가 대부분을 차지한다고 보았다.

다양한 정보보호 관리체계들이 제안되어 왔으며 각 체계들의 비교와 도입 효과들도 연구되었다. 백남균, 박성갑 (2017)은 정보보호 관리체계(ISMS), 정보보호 제품 평가(CC), 정보보호 전문서비스 기업 제도, 보안관제 전문기업 지정 등 국내 정보보호 의무제도 동향을 연구하였다. 이들은 각 제도의 개념, 법적 근거, 인증 방법, 추진 경과, 추진 체계, 절차 등을 분석하였다. 박태완, 오경희 (2016)는 ISO/IEC 27009 국제표준을 중심으로 정보보호 경영시스템 인증에 관련된 국제표준들과 동향을 분석하였다. 이들은 ISO/IEC 27001에서 제시된 요구사항과 ISO/IEC 27002에서 제시된 통제항목(대응책), 그리고 개인정보, 통신, 클라우드 등과 같은 특정 영역에서의 정보보호 경영요구시스템 요구사항을 문서화 하는 방법을 기술하는 표준인 ISO/IEC 27009간의 관계를 분석하여 국제 시장 변화에 대응하기 위한 역량 확보의 필요성을 주장하였다.

2.3. 정보보호 공시제도 선행연구 및 연구방법

전효정, 김태성 (2012)은 정보보호 공시 제도 도입 전인 2012년도에 기존 공시제도의 고찰을 통해 정보보안 분야 공시제도(안)을 제시하고, 공시제도 전문가들의 검토의견을 수렴하여 정보보안 공시제도의 필요성과 정보보안 공시제도 도입의 타당성을 분석하였다. 이 연구에서 이들은 공시제도 운영 관련 전문가와의 심층인터뷰, 심층인터뷰를 통해 정리된 공시제도 초안에 대한 서면조사를 수행하였고, 공시제도 운영기관(금융감독원, 한국거래소), 공시자료 작성 및 검증기관(회계법인), 공시제도 시행기관(금융기관 CIO) 등의 관계자 검토를 거쳤다. 아울러, 초안은 현재 진행되는 공시제도와 보안제도를 벤치마킹하여 마련하였으며, 정보보안 공시제도 도입 효과 분석은 인과지도(causal-loop diagram)을 이용하여 분석하였다.

민현우, 이희조(2016)는 제도가 도입된 2016년도에 공시로 인한 경제성이 자본비용 감소에 있다고 보고, 선행연구를 바탕으로 일반적인 공시를 통해 기업과 외부 정보이용자간의 정보 불균형을 줄이면 회사의 자금조달 비용 감소를 위해 공시가 적극적으로 실시된다고 보았다.

김경석(2018)은 2018년 2월 미국증권거래위원회(SEC)가 승인한 “사이버 보안 위험에 대한 공개를 준비하는 해석지침”을 분석하였다. 다른 사업적 리스크와 마찬가지로 사이버보안 위험도 회사의 가치에 미치는 영향을 판단할 수 있는 구체적인 내용을 공시하여야 한다는 점을 강조하였다. 다만, 사이버보안 위험은 정량적 평가가 쉽지 않기 때문에, 정량적 평가 방법에 대한 추가적인 논의가 필요하다. 이러한 논의는 기업의 내부통제 제도 안에서 회사의 위험에 영향을 줄 수 있는 관점으로서의 사이버위험에 대한 공시 제도를 검토하고 있다.

이경준, 김현경(2020)은 현행 정보보호 및 관리·감독제도에 대한 현황과 한계를 검토하였다. 해당 연구에서 정보보호 및 개인정보보호 관련 제도로써 개인정보 영향평가, 정보보호 및 개인정보보호 관리체계 인증 제도(ISMS-P), 정보보호 관리등급 부여 제도, 클

〈표 1〉 정보보호 공시 관련 법률

정보보호산업의 진흥에 관한 법률 제13조(정보보호 공시)
① 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. 이 경우 「자본시장과 금융투자업에 관한 법률」 제159조에 따른 사업보고서 제출대상 법인은 같은 법 제391조에 따라 정보보호 준비도 평가 결과 등 정보보호 관련 인증 현황을 포함하여 공시할 수 있다. ② 제1항에 따라 정보보호 현황을 공개한 자가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항에 따른 정보보호 관리체계 인증을 받고자 하는 경우에는 납부하여야 할 수수료의 100분의 30에 해당하는 금액을 할인받을 수 있다.

라우드 보안인증 제도, 정보보호 공시 제도, 정보보호 준비도 평가의 6가지 현황을 다루었다. 이 중, 준비도 평가에 대하여, 2019년 말까지 공시 기업수가 40개에 그친다는 점을 들어 공시 제도 실효성에 대한 의구심이 제기된 바 있었다는 근거를 제시하였다. 특히, 정보보호 공시 제도에 자율성을 둔 것으로 인해 한계가 있다는 점을 지적하였다.

정보보호 공시제도(과학기술정보통신부, 2019)는 이용자의 안전한 인터넷 이용과 기업의 정보보호 투자 활성화를 위해 기업의 정보보호 투자・인력・활동 등에 관한 정보를 공개하도록 하는 자율 공시제도이다[2]. 기업의 정보보호 관련 투자 현황(액수 및 IT비용대비 비율), 정보보호 관련 직원 채용 현황, 정보보호 관련 인증 등을 취득한 내용을 공개하도록 하고 있으며, 또한 기업이 행하고 있는 중요 정보보호 활동을 공개하도록 하고 있다. 공시는 의무화되어 있지는 않으며, 기업의 선택에 따라 공시할 수 있도록 운영되고 있고, 다른 기업 공시와 같이 한국거래소에 공시할 수도 있으나, 과기부에서는 정보보호산업진흥포털 (https://www.ksecurity.or.kr/)에 공시 할 수 있는 게시판을 만들어 관리하고 있다.

2016년 정보보호산업의 진흥에 관한 법률에 정보보호 공시 제도에 관한 사항이 포함되었으며, 그 내용은 <표 1>과 같다[3].

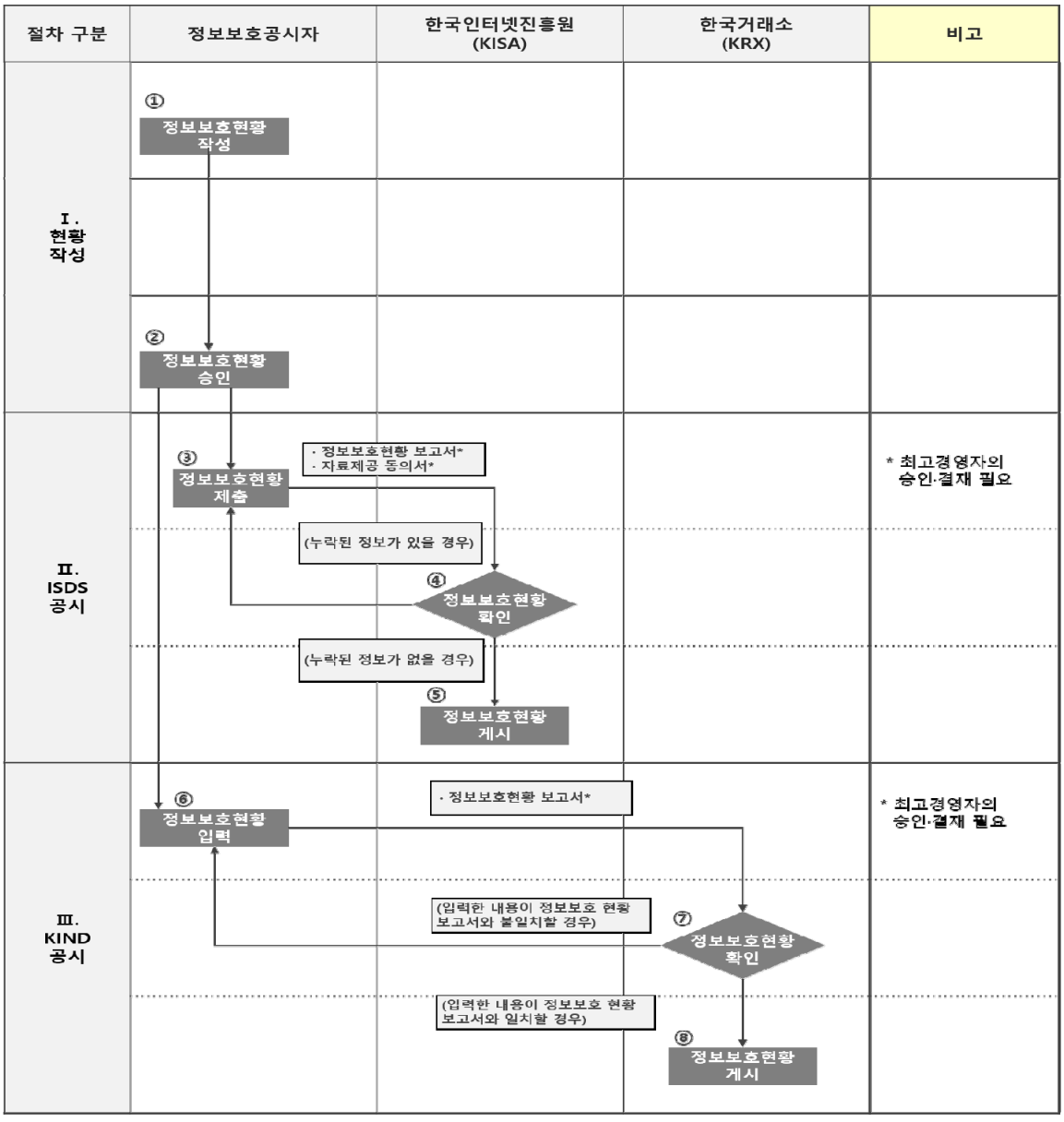
정보보호 공시제도의 목적은 기업의 정보보호 현황이 자생적으로 유통되지 않는 현실을 개선하기 위한 것에 있다. 이 제도를 통하여 주주 등 이해관계자는 기업의 잠재적 재무상태 변화에 주요한 영향을 미칠 수 있는 알권리를 확보하고, 소비자・고객・국민은 기업의 정보보호 수준을 간접적으로 파악하여 소비자 선택권을 강화하며, 기업은 정보보호 수준을 객관적으로 파악하고, 안전한 기업 이미지 및 신뢰도 제고를 노릴 수 있다는 것이 제도의 시행 당시 정부의 입장이었다. 즉, 기업의 투자자들로 하여금 기업이 정보보호에 어느 정도의 노력을 기울이고 있는지 알도록 하여 위험 관리 측면에서 이해관계자를 보호하는 한편, 기업의 보안활동이 외부로 알려지도록 함으로써 정보보호 투자를 촉진하도록 하기 위한 기대가 있었다.

본 연구에서는 정보보호 공시가 이루어지기 전 또는 제도 도입 첫 해에 그 필요성을 제기했던 연구에 대응하여, 정보보호 공시가 5년간 이루어진 현재의 관점에서, 지난 기간 동안 이루어진 정보보호 공시가 어떠한 내용을 담고 있었고, 투자 / 인력 / 기타 공시 내용의 측면에서 어떤 차이점을 가져오게 되었는 지에 대하여 현황을 분석하는 방식으로 본 연구를 진행하였다. 아울러, 이를 바탕으로 활성화되지 않고 있는 공시제도에 대한 활성화를 위한 정책 제언을 제시하였다.

2) 정보보호산업진흥포털 https://www.ksecurity.or.kr/kisis/subIndex/33.do

3) 정보보호산업의 진흥에 관한 법률 https://www.law.go.kr/법령/정보보호산업의%20진흥에%20관한%20법률

〈표 2〉 공시 절차



3. 정보보호 공시제도 현황

3.1. 정보보호 공시 절차 및 공시 내용

정보보호 공시 제도는 정보보호 산업의 진행에 관한 법률을 근거로 하며, 공시를 할 경우 정보보호 관리체계(ISMS) 인증 수수료의 30%를 할인하도록 하는 유인을 제공하였다. 공시의 방법은 다른 공시와 같이, 한국거래소의 전자공시시스템(KIND)에 공시하는 방법도 있으나, 과기부에서는 별도의 전자공시 시스템[4]을 만들어서 이곳에서도 공시할 수 있도록 하였다. 초기에는 기업의 공시 내용을 신뢰할 수 없다고 보았기

4) https://www.ksecurity.or.kr/user/extra/kisis/34/disclosure/disclosureList/jsp/LayOutPage.do

〈표 3〉 정보보호 현황 서식

1. 정보보호 투자 현황	정보기술부문 투자액(A) (원)		
	정보보호부문 투자액(B) (원)		
	B / A (%)		
2. 정보보호 인력 현황	총임직원(내부인력) (명)		
	정보기술부문 인력(C) (명) (내부인력 + 외주인력)		
	정보보호부문 전담인력(D)	내부인력 (명) (정규직+계약직)	
		외주인력 (명)	
		계 (명)	
	D / C (%)		
3. 정보보호 관련 인증 · 평가 · 점검 등에 관한 사항			
4. 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황			

때문에, 공시 과정에서 회계법인 또는 정보시스템 감리업체의 확인을 거치도록 하였으나, 2019년 1월 공시제도를 활성화하기 위한 목적으로 이 확인은 거치지 않도록 절차를 변경하였다. 다만, 샘플링을 통하여 점검하는 절차가 만들어졌다. 정보보호 공시절차는 다음 <표 2>와 같다(과학기술정보통신부, 2019).

공시되는 내용은 크게 정보보호에 대한 투자 현황, 정보보호 인력 현황, 정보보호 관련 인증 / 평가 / 점검 등에 관한 사항, 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황으로 나누어서 공시된다. 이에 대한 현황 서식은 다음 <표 3>과 같다(과학기술정보통신부, 2019).

2020년까지 1회 이상 공시를 한 회사는 52개사이며, 공시 건수로는 총 107건이 공시되었다. 과학기술정보통신부 전자공시시스템(ISDS)의 현황을 바탕으로, 각 기업별 공시일자를 정리하면 <표 4>와 같다.

〈표 4〉 정보보호 공시 현황

회사명	2016	2017	2018	2019	2020
공시건수	2	10	20	30	45
테크빌교육	2016-12-28	2017-12-20	2018-12-18	2019-12-30	2020-12-31
케이티		2017-05-23	2018-06-07	2019-05-29	2020-09-03
LG유플러스		2017-05-23	2018-07-12	2019-08-05	2020-09-24
SK텔레콤		2017-05-25	2018-05-28	2019-06-07	2020-08-13
SK브로드밴드		2017-05-29	2018-08-06	2019-08-12	2020-10-30
씨디네트웍스		2017-10-25	2018-11-30	2019-12-04	2020-12-16
포뎁스		2017-11-15	2018-12-17	2019-12-31	2020-12-30
건국대학교병원		2017-12-06	2018-12-27	2019-12-30	2020-12-31
비바리퍼블리카			2018-05-14	2019-03-12	2020-02-21
후후앤컴퍼니			2018-05-17	2019-05-27	2020-05-29
에듀윌			2018-05-30	2019-06-13	2020-07-01
충북대학교병원			2018-06-07	2019-05-29	2020-05-11
스트리미			2018-08-23	2019-06-14	2020-07-06

회사명	2016	2017	2018	2019	2020
크래프톤(블루홀)			2018-10-05	2019-05-02	2020-07-13
펍지주식회사			2018-10-05	2019-05-03	2020-07-13
메가스터디교육			2018-12-04	2019-12-10	2020-12-09
그린카			2018-12-24	2019-07-30	2020-04-29
팍스넷				2019-01-25	2020-12-23
커리어넷				2019-05-27	2020-05-11
NHN				2019-06-05	2020-06-01
인프라웨어				2019-09-30	2020-10-13
카사코리아				2019-11-01	2020-11-06
에이스솔루션				2019-12-30	2020-12-23
넥스트소프트				2019-12-30	2020-12-28
메인정보시스템				2019-12-30	2020-12-28
경상대학교병원				2019-12-31	2020-12-09
한국중부발전					2020-01-07
백패커					2020-05-11
한국신용데이터					2020-08-25
CJ ENM(오쇼핑 부문)					2020-08-27
퀴즈톡					2020-09-25
숙명여자대학교					2020-10-22
경희대학교					2020-11-05
에스알					2020-12-16
우리은행					2020-12-28
디지털플러스시스템					2020-12-28
피플인비즈					2020-12-28
웹투어					2020-12-29
케이쓰리아이					2020-12-30
삼지티엔씨					2020-12-30
코어닥스					2020-12-31
에이치아이엔티					2020-12-31
에프원시큐리티					2020-12-31
씨큐하이					2020-12-31
케이에스아이					2020-12-31
삼성웰스토리	2016-12-29				
티몬		2017-11-15			
서울아산병원		2017-10-23	2018-11-01		
토파스여행정보			2018-09-03	2019-09-25	
부산디지털대학교			2018-12-28	2019-11-29	
한국동서발전				2019-10-18	
부산은행				2019-12-06	

<표 3>의 서식처럼, 주된 공시 내용은 정보보호 투자 현황, 인력 현황, 정보보호 관련 인증·평가·점검 등에 대한 사항, 정보보호 활동에 대한 사항으로 나눌 수 있다.

3.2. 정보보호 공시 내용 분석

공시를 시행한 회사에 대하여, 정보기술부문 투자액에 비하여, 정보보호부문 투자액의 비율은 다음과 같이 변화하였다.

또한, 정보기술부분 인력에 대비하여 정보보호부분 전담인력의 비율은 다음과 같이 공시하였다.

정보보호 투자 및 인력에 대한 공시에서 특기할 만한 사항은, 정보보호에 대한 투자를 0원으로 표기하거나, 정보보호에 대한 인력 투입을 0명으로 하는 회사가 존재하였다는 점이다. 전체 107건의 공시 중에서 2019년의 1개 회사, 2020년의 2개 회사는 자사가 정보보호에 투자를 하지 않는다는 사실을 공시하였으며, 인력에 대해서도 2017년과 2018년에 각각 1개 회사, 2019년에는 6개 회사, 2020년에는 8개 회사가 정보보호 부분에 인력을 배정하지 않는다는 사실을 공시로 밝혔다. 실무적으로는 작은 규모의 회사라고 하더라도 PC에 사용하는 백신 정도는 존재할 것이며, 정보보호 관련 전담인력을 두지 않더라도 타 업무 담당자에게 정보보호 업무 또는 보안 업무에 대한 겸임 업무를 분장하는 것이 일반적이기 때문에 공시 시점에 조금만 관심을 가졌다면 어느 회사든지 투자액수와 투입 인력수를 0으로 표시하지는 않을 수 있었을 것이다. 공시를 하는 것이 의무가 아닌 상황에서도 자사가 정보보호에 관심이 없다는 사실을 굳이 밝히는 회사가 존재한다는 것은, 다른 측면에서 보자면 이 공시로 정보보호에 대해 관심이 없다는 것이 알려지더라도 회

〈표 5-1〉 정보기술부문 투자액 대비 정보보호부문 투자액 비율

(법인수 / 전체 공시건수 대비 비율)

정보기술부문 투자액 대비 정보보호부문 투자액 비율	2016년		2017년		2018년		2019년		2020년	
공시건수	2		10		20		30		45	
0%							1	3%	2	4%
5% 이하			5	50%	9	45%	12	40%	13	29%
10% 이하	2	100%	4	40%	6	30%	9	30%	13	29%
15% 이하			1	10%	4	20%	5	17%	13	29%
15% 이상					1	5%	3	10%	4	9%

〈표 5-2〉 정보기술부분 인력 대비 정보보호부분 전담인력 비율

(법인수 / 전체 공시건수 대비 비율)

정보기술부분 인력 대비 정보보호부분 전담인력 비율	2016년		2017년		2018년		2019년		2020년	
공시건수	2		10		20		30		45	
0%			1	10%	1	5%	6	20%	8	18%
5% 이하			5	50%	5	25%	7	23%	8	18%
10% 이하	1	50%	4	40%	13	65%	13	43%	19	42%
10% 이상	1	50%			1	5%	4	13%	10	22%

사에 부정적인 영향이 가지 않을 것이라는 고려가 있었다고 볼 수도 있을 것이다.

공시를 통하여, 투자 또는 인원의 변동이 있는 지를 확인하기 위하여, 2017년도와 2018년도에 공시를 한 9개사 / 2018년도와 2019년도에 공시를 한 19개사 / 2019년도와 2020년도에 공시를 한 26개사를 비교하였을 때, 투자 및 전담인력 비율의 증/감을 보인 회사의 수는 다음과 같았다. 계속하여 공시를 수행하는 회사에 대하여, 대부분의 회사는 -2%~2% 내의 사이의 투자변동 및 전담인력의 변동을 보이지만, 2%이상 증가하는 회사들을 살펴볼 때는 투자 및 전담인력의 변동 부분에 대하여, 2019년도 → 2020년도의 전담인력 변동의 한 경우를 제외하고는 증가되는 회사가 감소하는 회사보다는 미세하게 많은 것으로 나타나 정보보호 공시를 지속한 회사의 경우, 정보보호에 관한 투자 비율 또는 전담인력의 비율이 증가하는 경우가 감소하는 경우보다 많은 것은 확인할 수 있었으나, 공시를 실시하지 않은 표본과의 대조가 어려운 점이 존재한다.

아울러, 정보보호 인증·평가·점검에 관하여 공시된 내용은 다음과 같다. 인증·평가·점검에 관한 공시 부분에서 기존에 공시하지 않았던 인증을 공시한 사례는 총 5개이다. 2018년도에 1개 회사는 2017년도에 공시하지 않았던 PCI-DSS와 ISO 27001을 새로 공시하

〈표 6〉 공시회사의 투자 및 전담인력 변동

(법인수 / 대상건수 대비 비율)

변동비율	2017 → 2018				2018 → 2019				2019 → 2020			
	투자변동		전담인력변동		투자변동		전담인력변동		투자변동		전담인력변동	
대상건수	9				19				26			
4%이상 증가	0	0%	0	0%	1	5%	2	11%	6	23%	1	4%
2%이상 증가	1	11%	1	11%	4	21%	0	0%	0	0%	0	0%
−2% ∼ 2% 내의 변동	8	89%	8	89%	11	58%	16	84%	16	61%	23	88%
2%이상 감소	0	0%	0	0%	2	11%	1	5%	3	12%	0	0%
4%이상 감소	0	0%	0	0%	1	5%	0	0%	1	4%	2	8%

〈표 7〉 정보보호 인증 · 평가 · 점검

(법인수 / 전체 공시건수 대비 비율)

정보보호 인증 · 평가 · 점검	2016년		2017년		2018년		2019년		2020년	
공시건수	2		10		20		30		45	
ISMS	1	50%	6	60%	13	65%	20	66%	24	53%
PIMS	1	50%	3	30%	2	10%	5	20%	2	4%
ISMS-P									3	7%
정보보호 준비도 평가			1	10%	1	5%	1	3%	1	2%
Cloud 보안인증			1	10%	1	5%	2	7%	2	4%
ISO 27001			4	40%	5	25%	10	33%	13	29%
ePRIVACY					1	5%	1	3%	2	4%
PCI DSS			1	10%	3	15%	4	13%	4	9%
기타 국제인증			2	20%			1	3%	1	2%
기타 점검 / 진단			2	20%	3	15%	3	10%	5	11%

였으며, 2019년도에는 3개사가 ISMS를, 1개사가 PIMS를, 1개사가 ISO 27001을, 1개사가 PCI-DSS를 새로 공시하였다. 마찬가지로, 2020년도에는 2개사가 ISMS를, 1개사가 ISO 27001을 새로 공시하였다. 이 사례는 기존에 누락하였던 인증을 공시하였거나, 공시로 인한 보안 강화 노력 과정에서 인증을 취득한 사례가 있었던 것으로 볼 수도 있다.

정보보호 활동은 정보보호 투자 활성화 / 임직원의 정보보호 인식제고 교육 및 지원 / 정보보호 전담인력 관리 활동 / 이용자 정보보호 인식 제고활동 등의 사항이 공시되는 데, 각 회사마다 기준이 다른 탓으로 기업간 활동을 비교하거나, 연간 활동이 증/감하였음을 비교하기는 어렵다. 다만, 주로 공시된 사항을 정리하자면 <표 8>과 같다.

정보보호 활동의 경우, 각 회사마다 매년 수행한 활동의 세분화 기준이 정해져 있지 않고, 공시 연도에

〈표 8〉 정보보호 활동 관련 공시내용

구분	세부 활동
정보보호 투자활성화	정보보호컨설팅 / 개인정보영향평가 수행 정보보호 관련 표창 사이버보호체계 정립 및 위협대응 강화 정보보호 솔루션 도입(DB암호화 / DLP / 망분리 / 접근제어 등) 정보보호 솔루션 업그레이드 GDPR 대응준비 개인정보보호 배상 책임보험 가입
임직원의 정보보호 인식제고 교육 및 지원	정보보호 / 개인정보보호 관련 교육 실시 CleanDesk / 물리보안 점검 실시 사이버위기대응 모의훈련 악성메일 모의훈련 보안수칙홍보 / 보안이슈사항 공지 / 매뉴얼 배포 활동 정보보호의 날 활동 협력업체 점검 및 교육활동 보안 공모전 실시
정보보호 전담인력 관리 활동	취약점 점검 및 모의해킹 보안관련 협의회 참석 내부 정책 / 지침 / 가이드 수립 및 배포 정보보호 위험평가 / 수준진단 / 보안감사 정보보호 위원회 / 실무협의회 개최 연간 정보보호계획 수립 및 시행 위험대책 수립 및 보완조치 이행 재해복구모의훈련 실시 시큐어 코딩 등 정보시스템 개발 / 운영자 교육 컨퍼런스 / 교육 참석, 자격증 취득 등 전문성 증진 활동
이용자 정보보호 인식제고 활동	비밀번호 변경 안내 정보보호 온라인 콘텐츠 제작/배포 정보보호 활동 공지 정보보호 캠페인 실시 개인정보 이용내역 통지 고객피싱 및 스팸메일 방지 활동 홍보 이용자 피해 예방 정보 게시 / 책자 제공 보이스피싱 피해방지 홍보 악성코드 감염 고객 공지

〈표 9〉 전년도에 공시하지 않은 카테고리를 공시한 기업 수

(법인수 / 대상건수 대비 비율)

해당 카테고리를 새로 공시한 법인의 수	2017 → 2018		2018 → 2019		2019 → 2020	
대상건수	9		19		26	
정보보호 투자활성화	1	11%	3	16%		0%
임직원의 정보보호 인식제고 교육 및 지원						
정보보호 전담인력 관리 활동			2	11%	1	4%
이용자 정보보호 인식제고 활동			1	5%		0%

수행한 모든 활동을 포함한 것도 또한 아니기 때문에 개별 활동 별로 비교하는 것은 어려움이 있다. 다만, 공시제도에서 예시로 제시하였던 4가지 카테고리를 기준으로 하여, 전년도에 공시하지 않았던, 카테고리를 새로 공시한 기업의 수는 <표 9>와 같다. 이 부분에 관하여 각 회사의 정보보호 관련 활동을 이해관계자가 확인할 수 있고, 또한 각 회사간의 정보보호 활동을 비교하도록 해야 하는 제도의 취지에서 볼 때 현재의 공시제도의 정보보호 활동 부분에 대한 공개 항목은 보완할 필요가 있다.

2016년의 공시건수 2건에 비하여 2020년 공시 건수가 45건으로 증가하기는 하였으나, ISMS의무대상이 되는 법인이 600개에 달하는 것을 보더라도 주요 정보통신서비스 제공 사업자에 중에서도 적은 수 만이 공시에 참여하고 있다. 한편으로, 지속되는 공시가 투자나 인력의 증가를 부른다고 보기도 어렵다. 투자액수 기준으로 10%이상을 투자하는 업체는 2016년부터 2020년까지, 0건 -> 1건 -> 5건 -> 8건 -> 17건으로 증가하였으나, 5%이하를 투자하는 업체 또한 0건 -> 5건 -> 9건 -> 13건 -> 15건으로 증가하였다. 인력비율에서도 10%이상을 투입하는 업체는 1건 -> 0건 -> 1건 -> 4건 -> 10건으로 증가하였으나, 5% 이하를 투입하는 업체 또한 0건 -> 6건 -> 6건 -> 13건 -> 15건으로 증가하였다. 건 수에서 모두 증가하였지만 비율 상으로는 투자비율과 인력비율 모두에서 증가를 보였다고 보기는 어렵다. 지속적으로 공시를 한 업체의 80%이상이 2% ~ -2% 내에서만 변동이 있었고, 투자비율에서도 2% ~ -2% 내의 변동을 보인 업체가 58%에서 89%를 나타내어 대부분의 회사가 크게 변동되지 않았다.

4. 정책적 제언

4.1. ISMS 인증 대상 기업에 대한 정보보호 공시 의무화 실시

제도 설계 당시에 기대했던 효과를 위해서는 규모가 큰 기업들이 먼저 정보보호 공시에 참여하여야 하는데, 실제로 기업 차원에서 정보보호 공시하는 것에 대한 유인이 별로 없다. 법령상의 유인은 ISMS 인증 수수료의 할인 뿐인데, 150만원~300만원 수준에 그친다. 아울러, 제도 초기에는 회계법인이나 정보시스템 감리법인이 검증하도록 하는 규정까지 있어서 그에 따른 비용이 수수료 할인 금액을 상회했었다. 2019년부터는 이 규정을 삭제하여, 검증 없이도 공시를 할 수 있지만, 7개 회사를 제외하고는 신규 업체들도 감리법인 또는 회계법인의 검증을 받고 공시하고 있어 제도적 실익은 많지 않아 보인다.

지난 5년간의 제도 운영 상황에서 본 것처럼, 공시제도가 의무화되기 전에 자율적인 공시 상태에서는 기업의 참여는 기대하기 어렵다. 기업에 유인을 줄 수 있는 방안이 별로 없기 때문이다. 따라서 이미 정보통

신서비스 부문 매출액 100억원 이상의 정보통신서비스 제공자, ISP, 상급종합병원 및 대학 등에게 강제화되어 있는 정보보호 관리체계 인증의 요구사항 중 하나로 정보보호 공시를 포함시키는 방법을 제안한다. 이를 통해 실시할 경우, 정보보호관리체계를 유지하고 있는 600여개 기업은 공시 의무를 갖게 된다.

기존의 정보보호 관리체계 인증 신청에서도 투자 비율과 정보보호 관련 인원수를 적도록 하고 있기 때문에, 이 신청서의 내용을 확인할 수 있는 체계만 추가하고, 이를 공시하도록 변경하면 된다. 아울러, 정보보호 활동을 점검하는 것이 인증 심사의 주요 활동이므로, 정보보호 활동 부분도 인증 심사 과정에서 확인하도록 할 수 있다. 즉, 제도를 통합하는 것에 있어서 기업의 부담이 크지 않은 반면 공시 제도를 확산하는 데 크게 기여할 수 있다.

다음 <표 10>에서 보이는 것처럼, 기존의 정보보호 관리체계 신청서 내용에서 운영현황을 제출하도록 하고 있으며, 해당 운영현황에서는 IT인력, 정보보호 전담인력, 개인정보보호 전담인력의 규모와 예산 규모를 포함하고 있다. 아울러, 정보보호 관리체계 인증기준에서도 1.1 관리체계 기반 분야의 세부항목으로 1.1.6 자원 할당을 두어 "최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다."는 사항을 점검하도록 하고 있으므로, 해당 항목을 보완하면 공시 제도의 실행을 강제화할 수 있도록 할 수 있다.

〈표 10〉 정보보호 관리체계 인증신청서 서식 일부

붙임2 **정보보호 및 개인정보보호 관리체계(ISMS-P) 운영현황**

아래는 정보보호 및 개인정보보호 관리체계(ISMS, ISMS-P) 인증 신청 기업·기관을 대상으로 운영현황과 제도개선 사항을 파악하고자 질문으로 구성하였으니 답변하여 주시기 바랍니다.

1. 귀 사(기관)에서 운영하는 전체 서비스 관련 회원 및 일일 평균 이용자수에 대해 각각 기입해 주십시오. (B2B 포함)

회원수(명)		일일 평균 이용자수(명)	

2. 귀 사(기관)의 정보보호 및 개인정보보호 조직 운영방식은 무엇입니까? ( )

1) 전담조직1) 2) 겸임조직 3) 기타방식 (※ 간단히 내용 작성)

3. 귀 사(기관)의 정보보호 및 개인정보보호 등을 포함한 인력 규모는 어느 정도입니까?

(단위 : 명)

회사內 전체 인력	IT 인력	정보보호 전담인력	개인정보보호 전담인력

4. 귀 사(기관)는 최근 1년 이내에 정보보호 또는 개인정보보호 인력을 신규 채용하였습니까?

1) 아니오 2) 예 (명)

5. 귀 사(기관)의 정보보호 및 개인정보보호 예산 규모는 어느 정도입니까?

(단위 : %)

전체예산 대비 IT 예산	IT예산 대비 정보보호 예산	IT예산 대비 개인정보보호 예산

4.2. 공시정보의 접근성 강화

아울러 공시 제도 자체의 실효성도 문제가 되고 있다. 주주나 고객이 공시 제도 자체를 잘 모른다. ISDS라는 과기부 홈페이지에 들어가지 않는 한, 개별 회사의 홈페이지에서도 공시 내용을 찾을 수 없기 때문에, 주주나 고객이 이를 확인하기가 어렵다. 또한, 정보보호 활동 현황을 기업 별로 비교하는 것도 어려움이 있다. 활동 현황은 각 회사별로 선택적으로 공시할 수 있기 때문에, 해당 활동이 공시한 회사에서만 이루어진 것인지, 다른 회사에서도 그 활동을 수행하는 지에 대한 것은 파악하기 어렵다.

〈표 11〉 개인정보 처리방침 및 이용내역 통지 관련 법령

개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)
제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. 1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다) 3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다) 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다) 5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항 6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처 7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다) 8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항 ② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다. ③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다. ④ 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.
개인정보보호법 제39조의8(개인정보 이용내역의 통지)
제39조의8(개인정보 이용내역의 통지) ① 정보통신서비스 제공자 등으로서 대통령령으로 정하는 기준에 해당하는 자는 제23조, 제39조의3에 따라 수집한 이용자의 개인정보의 이용내역(제17조에 따른 제공을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니한다. ② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다.
개인정보보호법 시행령 제48조의6(개인정보 이용내역의 통지)
제48조의6(개인정보 이용내역의 통지) ① 법 제39조의8제1항 본문에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다. 1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장 · 관리되고 있는 이용자 수가 일일평균 100만명 이상인 정보통신서비스 제공자등 ② 법 제39조의8제1항에 따라 이용자에게 통지해야 하는 정보의 종류는 다음 각 호와 같다. 1. 개인정보의 수집 · 이용 목적 및 수집한 개인정보의 항목 2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다. ③ 법 제39조의8제1항에 따른 통지는 서면등의 방법으로 연 1회 이상 해야 한다.

공시 제도가 그 목적을 달성하기 위해서는, 공시 내용을 해당 회사에 대해 관심있는 사람이 쉽게 찾고 정보를 비교할 수 있도록 해야 한다. 이 측면에서 정보보호산업진흥포털(www.ksecurity.or.kr) 에서 정보보호 공시 메뉴를 찾아 들어가야 확인할 수 있는 현재의 정보 확인 방법은 문제가 있다. 심지어 네이버나 다음의 검색에서 정보보호 공시제도를 검색해도 정보보호산업진흥포털이 검색되지 않아, 해당 사이트에서 공시가 이루어진다는 사실을 아는 사람만이 공시 정보를 확인할 수 있다.

정보보호에 관련하여, 기업이 고객의 개인정보를 어떻게 처리하는 지에 대하여 공개하는 방법으로 두 가지 방법이 사용되고 있다. 첫 번째는 회사의 메인 홈페이지에 게시하는 방법이다. 현재의 개인정보 처리방침이 이 방법을 사용하고 있다. 개인정보 처리방침은 홈페이지의 하단에 다른 항목과 표시나는 폰트 및 글자색 등으로 표시하여 확인할 수 있도록 하고 있다. 다른 방법은 주기적으로 정보보호에 관한 사항을 관계자에게 메일 / 문자 등으로 통보하도록 하는 방법이다. 개인정보 이용내역 통지가 이 방법을 사용한다. 정보통신서비스 제공자가 매년 1회 이메일 등을 통하여 고객의 개인정보를 어떻게 이용하고 있는 지를 통보하도록 하고 있다. 현재의 공시제도가 다른 기업 공시와 같은 절차를 가지고 있는 것이 아니며, 또한 그 취지가 공시라는 형식을 유지하는 것을 중시하는 것은 아니므로, 정보보호 공시 내용을 이해관계자가 쉽게 찾게 하려면 이 두 가지 방법을 사용하는 것이 바람직해 보인다. 즉, 개인정보 처리방침의 내용에 포함하여 홈페이지에서 쉽게 찾게 하거나, 개인정보 이용내역 통지에 포함하여 1년 주기로 안내하도록 하는 방법이 있을 것이다.

개인정보보호법 제30조에서 개인정보 처리방침에 포함하여야 하는 사항을 정하고 있으므로, 해당 사항에 정보보호 공시의 내용을 포함하도록 하고, 아울러, 개인정보보호법 시행령 제48조의6에 정해져 있는 통지하여야 하는 정보에 정보보호 공시의 내용을 포함하도록 할 수 있다. 이렇게 하면, 이용자들이 많지 않은 정보보호포탈에만 공시하는 것 보다도 실제의 이용자들이 접근할 수 있는 가능성이 커지므로 정보보호 공시의 접근성을 높여서 실효적인 공시가 이루어지도록 할 수 있다.

4.3. 공시정보의 비교가능성 강화

정보보호 활동에 대한 사항은 각 회사 간 활동을 비교할 수 있도록 하기 위하여, 현재보다 세분화된 템플릿을 제공하고 해당 활동을 하였는지를 표시하게 하면 동종 업계 내에서 활동을 비교할 수 있을 것으로 보인다. 즉, 위에서 정리한 것처럼 현재의 4개 대분류보다도 세분화하여, “정보보호 컨설팅을 실시하였는지?”/ “정보보호 솔루션을 증설하였는지?”/ “재해복구 모의훈련을 실시하였는지?” 등을 세부적으로 묻되, 어떤 항목을 물을 지는 매년 가이드라인을 변경하여 항목을 정하게 하고, 회사에서 추가적으로 홍보하고자 하는 사항을 기타항목에 넣도록 하면 개별 회사들이 진행하는 정보보호 활동을 비교하기 쉬워질 것이다.

위에서 정리하였던 <표 8>을 참조하여, 기존에 주로 공시되었던 세부 활동을 기준으로 이러한 공시를 위한 예시를 제시한다면 다음 <표 12>의 내용과 같다. 각 세부 활동 별로 해당 활동을 자사가 실시하였는 지를 기록하게 하고, 이 경우 몇 회를 실시하였는 지를 표기하도록 할 수 있다. 특히 솔루션 도입 / 컨설팅 범위 / 교육의 종류 등에 대한 세부사항을 표기하도록 하기 위하여 비고를 놓고, 범주화되지 않은 기타 정보보호 활동을 표기하도록 하기 위하여 기타를 둘 수 있다.

〈표 12〉 정보보호 활동 관련 공시내용(예시)

구분	세부 활동	여부	횟수	비고
정보보호 투자활성화	정보보호컨설팅 / 개인정보영향평가 수행			
	정보보호 관련 표창			
	사이버보호체계 정립 및 위협대응 강화			
	정보보호 솔루션 도입(DB암호화 / DLP / 망분리 / 접근제어 등)			
	정보보호 솔루션 업그레이드			
	GDPR 대응준비			
	개인정보보호 배상 책임보험 가입			
임직원의 정보보호 인식제고 교육 및 지원	정보보호 / 개인정보보호 관련 교육 실시			
	CleanDesk / 물리보안 점검 실시			
	사이버위기대응 모의훈련			
	악성메일 모의훈련			
	보안수칙홍보 / 보안이슈사항 공지 / 매뉴얼 배포 활동			
	정보보호의 날 활동			
	협력업체 점검 및 교육활동			
	보안 공모전 실시			
정보보호 전담인력 관리 활동	취약점 점검 및 모의해킹			
	보안관련 협의회 참석			
	내부 정책 / 지침 / 가이드 수립 및 배포			
	정보보호 위험평가 / 수준진단 / 보안감사			
	정보보호 위원회 / 실무협의회 개최			
	연간 정보보호계획 수립 및 시행			
	위험대책 수립 및 보완조치 이행			
	재해복구모의훈련 실시			
	시큐어 코딩 등 정보시스템 개발 / 운영자 교육			
	컨퍼런스 / 교육 참석, 자격증 취득 등 전문성 증진 활동			
이용자 정보보호 인식제고 활동	비밀번호 변경 안내			
	정보보호 온라인 콘텐츠 제작/배포			
	정보보호 활동 공지			
	정보보호 캠페인 실시			
	개인정보 이용내역 통지			
	고객피싱 및 스팸메일 방지 활동 홍보			
	이용자 피해 예방 정보 게시 / 책자 제공			
	보이스피싱 피해방지 홍보			
	악성코드 감염 고객 공지			
기타	기타 정보보호 활동			

5. 결론

5.1. 연구결과 요약 및 논의

본 논문에서는 정보보호 공시제도 실시 이후 2020년까지의 공시내용을 분석하여 현황을 파악하였으며, 정보보호 공시제도 활성화를 위한 대안을 제안하였다. 현재 공시된 내용을 살펴볼 때, 지금까지 공시제도를 통해 정보보호 관련 정보를 공개한 기업들에서 전담인력을 늘리는 경우가 있었으며, 정보보호 관련 인증을 취득하기도 했음을 알 수 있었다. 정보보호 공시에 밝혀진 내용으로는 투자의 증/감에 대한 영향을 발견하지 못했다. 다만, 현재 공시제도에 참여한 회사의 수가 많지 않기 때문에, 공시제도로 인하여 전담인력 또는 인증 취득에 영향을 준 측면이 있었는 지는 확인하기 어렵다.

현재의 정보보호 공시제도는 개별 기업들이 공시를 하도록 하는 유인을 주지 못하고 있고, 이로 인하여 제도의 취지였던 기업의 정보보호 위험을 이해관계자들에게 공개하는 것이나 기업의 정보보호 투자를 활성화하는 것을 달성하지 못하고 있다. 이에 본 연구에서는 정보보호 공시제도를 현재 의무화되어 활성화되고 있는 정보보호 관리체계 인증제도에 포함하여 활성화하는 방안을 제안하였다. 아울러, 현재의 공시제도에서 기업의 이해관계자나 고객이 공시의 내용을 확인하는 것이 어렵기 때문에 이를 보다 접근하거나 인지하기 쉽도록 하는 방안으로 개인정보 처리방침 또는 개인정보 이용내역 통지의 내용에 포함하는 방법을 제시하였으며, 또한 정보보호 활동을 보다 세분화하여 공개하는 것이 필요할 것으로 보았다.

각종 정보보호 사건이 발생하면서, 정보보호에 대한 각종 제도는 개별적으로 추가되었다. 개인정보보호법이 제정되면서 개인정보의 암호화에 대한 사항을 포함하는 안전성 확보 조치가 의무화되었고, 정보통신망서비스제공자를 대상으로 하는 망분리 의무화가 생겨났으며, 정보보호관리체계(ISMS) 인증 의무화, 정보보호 최고책임자의 지정, 개인정보 유출 사고에 대비하는 보험/공제의 가입 등 개별적인 제도들이 사고시 마다 늘어났다. 이제 현실적으로 개별제도를 추가하여 의무화 하는 것은 지양해야할 시기가 되었으며, 기업의 정보보호 강화를 위해서는 기존에 있는 제도를 활용하여 틀을 갖추게 하는 것이 필요해 보인다.

그래서 본 논의에서는 기존에 운영되고 있는 ISMS 인증의 틀에서 정보보호 공시를 포괄하고, 또한 기존에 운영되는 개인정보 처리방침 / 개인정보 이용내역 통지 범위 하에서 공시의 효과를 달성하게 하는 것을 제안하였다. 이 방안이 현재 별도의 사이트를 알아서 찾아가야 하는 공시방법 보다는 현실적이고 효과적으로 보이기 때문이다. 공시를 하는 내용을 실제 사용자가 확인할 수 없는 상황에서는 유인책을 주기 어렵고, 정보보호를 잘 하는 업체와 관심이 많지 않은 업체를 사용자가 구분할 수 없다면 공시를 한 것이 이익이 되지 않기 때문이다.

의무공시를 달성하는 방법에는 여러 가지가 있을 수 있으며, 그 방법이 현재 운영되고 있는 정보보호 제도의 범위 내에서 선택하는 것보다 전자공시시스템 등의 다른 방법을 활용하게 하는 것이 정보보호의 강화 측면에서 도움이 될 수 있다. 다만, 이 방법은 현재 IT투자 자체에 대한 별도의 공시 체계가 없는 한 정보보호만을 가지고 실행하기에는 한계가 존재한다. 정보보호에 관한 기업의 위험이 존재하는 것이 현실이고, 또한 이를 향상하기 위해 일정 부분의 정보를 공개하는 것이 필요하다면, 목적을 달성하기 위한 다른 대안도 논의될 필요가 있다.

5.2. 시사점 및 향후 연구방향

본 논문에서는 기존에 의무로 운영되고 있는 정보보호 관리체계 인증제도를 활용하여 정보보호 공시제도를 활성화하는 방안을 제시하였다. 또한, 공시제도가 처음 실시된 2016년부터 2020년까지의 공시데이터를 분석하여 공시되는 내용의 경향을 파악하였다. 이러한 분석은 공시된 항목의 제한과 건수의 제한으로 인하여 한계가 있기는 하였으나, 공시제도의 데이터를 활용하여 현재의 정보보호 수준을 확인할 수 있다는 점에서는 의미를 가진다. 제도화, 접근성 강화, 비교가능성 강화 측면에서의 정보보호 공시제도 활성화 방안을 제안하였다.

본 연구는 공시된 항목의 한계와 공시되지 않은 법인의 데이터에 접근하는 것이 제한된다는 한계로 인해, 정보보호 공시제도를 활용하는 회사들이 정보보호 투자와 인력의 보강을 실시하는 지 여부를 확인하여 못하였다. 또한, 정보보호 수준을 판단할 수 있는 지표를 확인할 수 없었기 때문에 정보보호 공시제도가 정보보호 수준의 개선에 도움을 주는 지 여부도 확인할 수 없었다. 한국인터넷진흥원과 개인정보보호위원회, 과학기술정보통신부 등 정부 기관은 연간 정보보호 백서를 제작하고, 또한 정보보호 관리체계 신청서 등 제도 운영 과정에서 집적되는 정보를 통하여 정보보호 투자 수준 및 인력에 대한 설문 결과를 가지고 있으므로 이를 적절히 비식별화하여 공개한다면 더 나은 실증 연구가 가능할 것이다.

〈참고문헌〉

[국내 문헌]

1. 과학기술정보통신부 (2019, 1월 4일). **정보보호 공시 가이드라인, 공고 제2019-0005호**.
2. 권영옥, 김병도 (2007). 정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향. ***Information Systems Review, 9***(1), 105-120.
3. 공희경, 전효정, 이송하, 강민성, 김태성 (2016). 보안인증의 경제적 효과에 대한 연구동향 분석. **정보보호학회논문지, 26**(3), 821-835.
4. 김경석 (2018). 사이버보안과 내부통제. **중앙법학, 20**(3), 249-270.
5. 김기현, 조혜진, 임소희 (2020). 4차산업혁명 핵심기술 도입 및 정보보호조직에 관한 탐색적 연구: 성과측면에서의 비교분석. **지식경영연구, 21**(1), 41-59.
6. 민현우, 이희조 (2016). 정보보호 공시 제도의 기대효과 및 도입에 따른 경제성 분석. **한국IT서비스학회 추계학술대회 논문집**, 295-298.
7. 박재영, 정우진, 김범수 (2016). 기업의 정보보호 인증이 기업가치에 미치는 영향. **한국IT서비스학회지, 15**(3), 51-69.
8. 박재영, 정우진 (2019). 기업의 정보보호 공시가 기업가치에 미치는 영향. **지식경영연구, 20**(4), 39-55.
9. 배영식 (2012). 정보보호관리체계[ISMS] 인증이 조직성과에 미치는 영향에 관한 연구. **한국산학기술학회논문지, 13**(9), 4224-4233.
10. 백남균, 박성갑 (2017). 국내 주요 정보보호 의무제도 동향. **전자공학회지, 44**(10), 32-40.
11. 백승익, 정유영 (2014). 정보유출 사고가 기업가치에 미치는 영향. **한국경영정보학회 추계학술대회**, 97-308.
12. 박태완, 오경희 (2016). 분야별 정보보호 경영시스템 인증 동향. **한국정보보호학회지, 26**(4), 16-21.
13. 신현민, 김인재 (2020). 정보보호 전문서비스 기업의 인증 및 상장여부가 재무적 성과에 미치는 영향. **지식경영연구, 21**(3), 197-213.
14. 엄재하, 김민정 (2016). 정보보안사고가 투자주체별 투자성과에 미치는 영향: 개인정보유출사고 중심으로. **정보보호학회논문지, 26**(2), 463-474.
15. 이경준, 김현경 (2020). 데이터 경제와 정보보호 관리 · 감독 제도의 개선에 대한 검토. **IT와 법 연구, 21**, 119-170.
16. 전효정, 김태성 (2012). 정보보안 공시제도 도입을 위한 타당성 분석과 운영체계 제언. **정보보호학회논문지, 22**(6), 1393-1405.
17. 조중기, 최상현 (2016). 정보보호 관리체계 인증 취득 후 기업가치의 변화에 관한 연구. **한국융합학회논문지, 7**(6), 237-247.
18. 황해수, 이희상 (2015). 정보보안 사고가 기업가치에 미치는 영향분석: 한국 상장기업 중심으로. **정보보호학회논문지, 25**(3), 649-664.
19. 홍일유, 이재훈, 강성민 (2015). 정보보안 사고에 대한 공시가 시장에서 기업의 주식가치에 미치는 영향. ***Entrue Journal of Information Technology, 14***(2), 33-56.

[국외 문헌]

20. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. ***MIS Quarterly, 34***(3), 523-548.
21. Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. ***The DATA BASE for Advances in Information Systems, 48***(3), 44-68.
22. Boss, S. R., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. ***MIS Quarterly, 39***(4), 837-864.
23. Cram, A., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. ***MIS Quarterly, 43***(2), 525-554.
24. D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. ***European Journal of Information Systems, 29***(6), 643-658.
25. Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and

deterrence. *European Journal of Information Systems, 25*(2), 91-109.

26. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

27. Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research, 27*(1), 70-86.

28. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

29. Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

30. Yoo, C. W., Goo, J., & Raghav, R. H. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*(2), 907-931.

저 자 소 개

백 승 준 (Seung Jun Baek)

현재 한국정보통신진흥협회 부설 정보통신인증센터에 재직중이다. 충남대학교 컴퓨터전공을 졸업하고, 연세대학교 공학대학원에서 공학석사를 , 한국방송통신대학교 대학원에서 법학석사를 취득하였으며, 가톨릭대학교 경영학전공 석/박사통합과정에 재학중이다. 주요 관심분야는 정보보안, 개인정보보호, 정보보호제도 등이다.

이 홍 주 (Hong Joo Lee)

현재 가톨릭대학교 경영학전공 교수로 재직 중이다. KAIST 산업경영학과를 졸업하고 KAIST 테크노경영대학원에서 석사 및 박사학위를 취득하였다. 주요 관심분야는 데이터 분석, 지능형 정보시스템, 온라인 사용자들의 상호작용 등이다. 지금까지 International Journal of Electronic Commerce, Expert Systems with Applications, Journal of Electronic Commerce Research, Government Information Quarterly 등 주요 학술지에 논문을 발표하였다.

〈 Abstract 〉

A Study of the Effectiveness and Status of the Information Security Disclosure System

Seung Jun Baek*, Hong Joo Lee**

The information security disclosure system (ISDS) has been implemented since 2016 to ensure the protection of stakeholders and the right to know, and to promote voluntary investment in information protection by companies. Regarding the information security disclosure system, there have been studies that urge the implementation of the system, but studies that analyze the contents disclosed after the implementation of the system or suggest improvement directions are few. In this study, the contents of the information security disclosure system that had been announced on the information security industry promotion portal until 2019 were analyzed, the current status was summarized, and the direction of system improvement was suggested. In some cases, companies that disclosed information through the disclosure system increased the number of personnel in charge and obtained certifications related to information security, but did not find any effect on the increase/decrease in investment. The current disclosure system has not been activated because it has difficulty in giving individual companies incentives to disclose. Thus, this study suggests the inclusion of ISDS to information security management system (ISMS), which is currently mandatory for certain companies. In the current disclosure system, it is difficult for the company's stakeholders or customers to check the contents of the disclosure. As a way to do this, a method of including in the contents of the personal information processing policy or the notification of the use of personal information was suggested.

Key Words: Information Security Disclosure System, Information Security Management System, Information Security, Security Policy

* Korea Association for ICT Promotion

** The Catholic University of Korea