韓國IT서비스學會誌
第19卷 第4號
2020年 8月, pp.13-30

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2020.19.4.013

기업의 특성이 개인정보 유출 사고에 미치는 영향

김택영* · 김태성** · 전효정***

Impact of Corporate Characteristics on Personal Information Breach Accident

Taek-Young Kim* · Tae-Sung Kim** · Hyo-Jung Jun***

■ Abstract ■

Not only does it cause damage to individuals and businesses due to the occurrence of large-scale personal information leakage accidents, but it also causes many problems socially. Companies are embodying efforts to deal with the threat of personal information leakage. However, it is difficult to obtain detailed information related to personal information leakage accidents, so there are limitations to research activities related to leakage accidents.

This study collects information on personal information leakage incidents reported through the media for 15 years from 2005 to 2019, and analyzes how the personal information leakage incidents occurring to companies are related to the characteristics of the company. Through the research results, it is possible to grasp the general characteristics of personal information leakage accidents, and it may be helpful in decision making for prevention and response to personal information leakage accidents.

Keyword : Information Breach, Corporate Characteristics, Personal Information Security

Submitted : July 7, 2020 1st Revision : August 6, 2020 Accepted : August 16, 2020

* 충북대학교 경영정보학과 박사과정, 주저자
** 충북대학교 경영정보학과 교수 및 보안경제연구소 소장, 교신저자
*** 충북대학교 경영정보학과 박사 후 연구원

1. 서 론

초연결사회가 도래함에 따라 개인정보의 가치가 중요해지고 정보보호는 이러한 사회를 지탱해주는 플랫폼으로서 중요성이 더욱 강조 되고 있다(유비용과 권헌영, 2020). 하지만 개인정보는 기업 내부자들에 의한 불법 유통과 기업 외부의 다양한 공격 기법을 활용하는 해커 등 사이버 위협에 노출되어 있다(한창희 외, 2011). 2005년 게임사의 대규모 개인정보 노출을 시작으로 2013년 주요 카드 3사의 개인정보 유출사고로 인하여 국민 대다수의 개인정보가 유출되었으며, 2020년 현재까지도 개인정보 유출이 지속적으로 발생하고 있다(각 사고에 대한 언론보도자료 참고). 개인정보 유출 사고로 인하여 기업 차원에서는 법정 비용의 발생과 기업의 이미지 손상 등을 겪고 있으며, 개인 차원에서는 본인의 정보가 타인에게 사용되어 금융적 피해, 프라이버시 침해 등이 발생하고 있다(조성규 외, 2012).

이러한 공격에 대한 대응방안으로서 개인정보보호법을 포함한 관련법들이 제정되고, 정보보호 및 개인정보보호관리체계(ISMS-P)에 대한 의무화가 시행되고 있으며, 개인정보보호에 대한 내용을 위반할 시에 대한 벌칙 기준이 수립되어 개인정보를 보호할 수 있도록 하고 있다(고형석, 2016). 정보통신망법에 따라 정보보호 및 개인정보보호관리체계 인증의 의무 대상을 기업의 매출액과 종사자 규모에 따라 지정하고 있으며(법제처, 2019), 개인정보보호법에 따라 개인정보가 유출될 경우, 유출한 기업은 매출액을 연평균으로 산정하여 과징금을 부가하고 있다(법제처, 2017).

이렇듯 개인정보와 관련하여 기업의 규모를 기준으로 보호 방안과 벌칙 등을 시행하고 있으나, 여전히 해킹 및 악성코드 등 외부 공격과 내부직원의 실수 및 고의가 원인이 되어 기업의 규모와 상관없이 개인정보 유출사고가 발생하고 있다(김신석 외, 2020). 이에 대하여 기업들은 스스로 위협에 대응할 수 있는 노력에 대하여 더욱 구체화하고 있으며, 학계에서도 개인정보 유출에 대하여 많은 연구가 이루어지고 있다(박준경 외, 2011).

하지만 개인정보 유출 사고에 대한 정보가 부족하여 개인정보 유출과 기업의 규모(매출액, 종사자)가 어떠한 관계를 가지며, 개인정보 유출 사고간의 관계에 대하여 연구가 부족하다. 이는 정보의 민감성으로 인하여 외부자가 정확한 피해 규모, 피해 및 복구비용 등 상세한 데이터를 수집하는 것이 매우 어려운 상황이기 때문이다(신일순 외, 2013).

이에 본 연구에서는 외부 연구자가 접근할 수 있는 언론 매체 및 정부의 보도 자료를 통해 2005년부터 2019년까지 발생한 개인정보 유출 사고에 대한 정보를 수집하고, 이를 바탕으로 개인정보 유출사고 요소간의 관계와 기업의 특성간의 영향관계에 대하여 분석하고자 한다.

본 연구를 통해 한정적인 개인정보 유출 사고 정보로 인하여 활용에 한계가 있던 개인정보보호 관리 분야에 보다 유용한 정보를 제공할 것으로 기대한다. 또한 개인정보 유출 사고로 인한 사회적 현상들에 대하여 연구되기 위해서는 개인정보 유출 사고에 대한 지속적인 정보 수집 및 공개 활동이 필요함을 제언한다.

2. 문헌 연구

개인정보는 개인, 기업, 국가 등 다양한 주체를 통해 발생, 수집, 저장, 활용되기 때문에 과거부터 중요한 자산으로 여겨지고, 다양한 주제로 연구되고 있다(강이주 외, 2001). 본 연구에서는 개인정보 유출 위협과 이에 대응하기 위한 개인정보 보호방안, 개인정보 유출 사고 및 관련 사례에 대한 연구, 개인정보 유출 사고로 인해 발생하는 사회적 문제 및 현상 등 개인정보 유출을 중심으로 이루어지고 있는 연구 주제에 대하여 기존 연구들을 살펴보았다.

2.1 개인정보에 대한 위협과 개인정보보호에 대한 연구

개인정보 유출 위협과 개인정보보호에 대하여 기존

연구들에서는 개인정보의 가치에 대하여 정의하고, 개인정보에 발생할 수 있는 위협을 분류하여 이에 대응할 수 있는 개인정보보호 방안들에 대하여 연구하고 있다. Karger(2006)은 미국 연방 정부 내부에서 보관하고 있는 개인과 개인정보에 대하여 정의하고, 발생 가능한 유출 위협을 분석할 수 있는 암호화 기반의 솔루션을 제안하고, 이와 관련된 표준에 대하여 필요성을 제시하였다. 연구결과를 통해 조직은 개인정보 유출 위협이 발생할 수 있는 다양한 경로를 파악하고, 위협을 식별하고 대처할 수 있는 방안에 대하여 적용해야 함을 주장하였다. 이재광 등(2007)은 개인정보를 보호할 수 있는 구체적인 기술인 개인정보 익명화와 암호화 기술에 대하여 설명하였다. 단순히 기존에 정보시스템에 사용되던 정보보호 기술들을 나열하기보다는 과거 국내에서 발생한 개인정보 유출 사고에서 발생한 위협에 직접적으로 대응할 수 있는 개인정보보호 기술들에 대하여 적용 가능성과 이에 대한 효과를 설명하였다. 이를 통해 개인정보보호 기술들이 일반적인 정보보호 기술과 동일하게 사용될 수 없음을 주장하였다. 엄정호 등(2010)은 외부자 이외에 내부자로 인하여 발생할 수 있는 개인정보 유출에 대응할 수 있는 접근통제 모델을 제시하였다. 개인정보 유출은 외부자에 의하여 주로 발생하지만, 내부자에 의하여 발생하는 경우도 상당하며, 내부자일 경우 내부 시스템에 접근하기 용이하기 때문에 피해규모가 클 것이라고 하였으며, 이를 방지하기 위한 내부자 접근에 대한 통제 모델과 그 기술을 설명하였다. 기술적인 관점에서 개인정보보호 방안에 대하여 설명한 연구들에서는 내부자, 외부자로부터 개인정보를 보호하기에는 기존 정보시스템을 보호하는 기술만으로는 대처할 수 없으며, 개인정보보호에 특화된 기술들을 활용해야하고, 기술적 보호 방안을 적용하기 이전에 앞서 개인정보 위협들을 식별해야 함을 주장하고 있다.

개인정보에 대하여 기술적으로 접근한 연구들과 다르게 관리적인 관점에서 개인정보에 대한 위협과 개인정보보호 방안에 대하여 연구되고 있다. 채승완(2008)은 개인정보 이용에 따른 양의 효과와 음의 효과를 경제적 가치로 측정하여 개인정보 유출로 인한 피해 규모와 비교하여 연구하였다. 연구 결과, 개인정보의 이용은 양의 가치가 크지만, 유출로 인하여 음의 가치도 커지고 있기 때문에 개인정보보호의 체계를 정비하는 것이 필요하다고 주장하였다. 정기석(2014)은 2014년 발생한 개인금융정보 유출사고에 대하여 원인을 도출하고, 정부에서 발표한 대책들이 효과가 있었는지 타당성 분석을 분석하였다. 금융사는 개인정보 유출에 대하여 정부 대책들을 수용할 뿐만 아니라 보안 거버넌스 전략을 수립하고 강력한 실행력을 통해 개인금융정보에 대한 자기정보결정권을 보호해야 함을 주장하였다. 정명수와 이경호(2015)는 개인정보를 보호하기 위해 수립된 개인정보 보호법과 개인정보 관리 수준을 진단하기 위해 시행되고 있는 개인정보보호 관리수준 진단에 대하여 효율성을 평가하고, 기존보다 효과성을 증진시키기 위해 새로운 모델을 고안하였다. 이를 통해 개인정보를 보호하기 위한 관리적 활동들이 단순히 행하는 것만으로는 부족하며, 지속적으로 방법에 대한 개선을 통해 효율성을 증진시켜야함을 주장하였다. 개인정보보호에 대한 관리적 방안들에 대하여 설명한 연구들에서는 개인정보보호를 위해서는 기술적인 관점에만 초점을 두지 않고 관리적 활동을 병행하여 보호 수준을 향상시키는 것이 필요하며, 일련의 활동들을 단순히 실천하는 것이 아니라 방안에 대하여 지속적으로 개선해야 함을 제시하고 있다.

개인정보보호의 기술적·관리적 방안 뿐만 아니라 인간의 행동학적인 측면에서 개인정보와 개인정보보호에 대하여 연구되고 있다. Acquisti(2009)은 개인정보가 가치를 창출함에 따라 개인정보 거래가 활발히 이루어지고 있으며 이에 대한 역기능으로 개인정보를 탈취하는 행위가 발생하는데, 이때 경제학 분야에서는 개인정보의 가치를 한정적으로 제한하였으나 이제는 행동경제학 및 심리학 관점에서 개인정보를 바라보아야하며, 개인의 정보

결정권을 고려해야한다는 주장을 하였다. 조동원(2012)은 개인정보를 유출하고 해킹하는 행위를 정보문화라는 시대적 흐름에 비추어 분석하였으며, 연구를 통해 개인정보의 해킹 및 유출 활동이 자기를 표현하는 방식 중 하나로 해석되며 정보자본주의와 연관이 되어있다고 주장하였다. 김준영과 김태성(2017)은 내부자로 인하여 발생하는 개인정보 유출 사고 수가 상당하며, 이러한 심리를 억제 이론과 합리적 선택 이론에 기반하여 정보유출 의도에 영향을 미치는 심리적 요인들에 대하여 연구하였다. 연구결과, 지각된 이익, 상황불안, 지각된 처벌의 심각성 및 확실성이 내부자들의 정보유출 의도에 영향을 미치는 것으로 나타났다. 이동희 등(2018)은 개인정보를 보호하기 위한 활동의 일환으로 패스워드를 통한 인증방식을 활용하는데, 개인의 민감성, 심각성 이익 등이 실제 행위의도에 어떠한 영향을 미치는지 연구하였다. 연구결과, 패스워드 관리는 개인정보를 보호하기 위한 기초적이고 필수적인 활동으로서, 보안상의 이익을 인식하는 정도에 따라 활동의 수준이 달라진다고 주장하였다. 이러한 심리 및 행동학적으로 개인정보와 개인정보보호에 대하여 접근한 연구들에서는 단순히 개인정보 유출 행동만을 볼 것이 아니라, 개인의 심리 및 시대의 흐름에 비추어 원인과 과정을 살펴보아야 한다고 주장하였다.

개인정보에 대한 위협과 이에 대응하기 위한 개인정보보호 방안들에 대하여 기술적 관점, 관리적 관점, 인간의 심리 및 행동학적인 관점 등 여러 관점에서 연구들이 이루어지고 있다. 하지만 앞선 연구결과들을 통해서 개인정보 유출 사고의 추이를 파악하고 유출 사고의 요소 간의 관계나 유출 사고로 인하여 발생하는 사회적 문제와의 연결고리를 찾아내는 것은 어렵다.

2.2 개인정보 유출로 인한 사회적 현상에 대한 연구

개인정보 유출 사고는 1차적인 정보 주체인 개인뿐만 아니라 개인으로부터 정보를 제공받아서 활용하는 2차적인 정보 주체인 기업에게도 많은 영향을 미친다. 이렇듯 개인정보 유출로 인하여 발생하는 현상에 대하여 연구되고 있다.

개인의 관점에서 유출 사고가 발생한 기업에 대한 이미지와 유출된 정보에 대한 인식 등 유출 사고로 변화하는 요소들에 대하여 다뤄지고 있다. 강이주와 황정선(2001)은 소비자들이 느끼는 기업과 정부의 개인정보보호 노력과 규제에 대한 신뢰도와 실제 경험인 개인정보 유출 피해의 연관성을 분석하였다. 연구결과, 소비자의 정보 유출 피해 경험이 많고, 기업에 대한 신뢰도가 높을수록 보다 높은 개인정보보호 수준을 원하는 것으로 나타났다. 개인정보 유출 사고가 기업에 대한 소비자의 신뢰도에 영향을 주고, 소비자는 보다 높은 개인정보보호 수준을 요구하고 있음을 보여주고 있다. 김소라와 이기춘(2006)은 개인정보 유출 피해에 대하여 소비자들이 지각하고 있는 위험 수준과 개인정보보호에 대한 개인의 노력 수준을 소비자의 유형에 따라 분류하여 연구하였다. 연구를 통해 개인정보 유출에 대한 위험지각이 개인의 정보보호 노력 수준보다 높은 것으로 나타났으며, 이에 따라 개인정보보호 의식을 고양시키는 교육도 중요하지만 노력까지 이어질 수 있도록 실천 행동에 대한 교육을 어렵지 않은 수단으로 제공해야한다고 주장하였다. 윤승욱 등(2008)은 개인정보 유출에 대하여 기업의 신뢰도와 위험 지각뿐만 아니라 서비스에 대한 이용량, 자기 정보 노출량, 대처방안 인지 등을 포함하여 의식의 변화에 대하여 연구하였다. 연구 결과, 서비스 이용량이 상대적으로 높은 사람은 신뢰도로 인하여 지각 불안과 피해가 일반적인 사람보다 낮으며, 오히려 서비스 이용량이 보통인 사람이 지각 불안과 피해가 더 높은 것으로 나타났다. 이를 통해 개인정보 유출에 대하여 신뢰도에 따라 소비자를 분류하여 접근하는 것도 좋지만 일반적인 사람들의 지각 불안과 피해를 줄일 수 있는 방안을 고려해야 한다고 주장하였다. 최근에는 개인의 개인정보 유·노출에

따른 현상은 소셜 네트워크 서비스(SNS) 환경에서도 빈번히 발생하고 있는데, 천명호 등(2013)은 개인의 활동이 활발한 SNS 환경에서도 개인정보 유・노출이 발생하고 있으며, 개인정보 유출 지수, 개인정보 유출 위험도 등이 높다고 제시하였다. 이를 통해 개인정보보호를 위해 개인의 정보에 대한 자기정보통제권을 향상시키는 것이 필요하다고 주장하였다. 여러 환경에서 존재하는 개인정보는 많은 요인들로부터 위협을 받고 있으며, 이러한 위협으로부터 개인정보를 보호하기 위해 개인의 비용이 발생하게 된다. 유승동과 유진호(2014)는 개인정보 침해에 대한 부정적인 효과를 방지하기 위한 지불의사 비용에 영향을 미치는 요인들을 이중양분선택법을 활용하여 도출 및 분석하였다. 연구결과를 통해 통신비용이 월 10만 원 이상인 가구는 10만원 미만인 가구에 비하여 개인정보 보호 지불의사 비용이 월 3,000원 정도 높은 것을 확인하였으며, 이러한 결과는 개인의 성별과 취업 여부에 따라 달라지는 것으로 나타났다.

이렇듯 개인정보 유출에 따른 개인의 변화에 대하여 여러 연구가 이루어지고 있다. 개인의 관점에서 개인정보보호 수준이 점차 증가함에 따라, 기업과 정부에게 개인의 인식 수준보다 더 높은 개인정보보호에 대한 노력을 요구하고 있다. 이와 반대로 개인이 능동적으로 개인정보보호 활동하는 수준과 환경은 여전히 미비한 것으로 나타났다. 많은 연구들에서는 개인정보보호 현상의 원인과 결과간의 관계와 문제 해결 방안들을 제시하고 있다.

개인정보 유출에 대한 사회적 현상을 개인의 관점이 아닌 기업의 관점에서도 연구가 되고 있다. 기업은 영리적 목적을 가지고 있기 때문에 기업의 관점에서 연구된 내용들은 주로 개인정보 유출에 대하여 기업의 경제적 입장에 대하여 연구되고 있다. 유진호 등(2009)은 2005년부터 2007년까지 발생한 국내 개인정보 유・노출 사고로 인하여 발생한 기업의 피해 비용을 정량적으로 산출하여 일본의 사례와 비교하였다. 이를 통해 개인정보 유출사고로 발생하는 기업의 경제적 피해를 단순화하여 객관적으로 측정할 수 있는 방법을 제시하고 더 나아가 기업이 정보 유출 사실을 은폐하는 것이 아니라 오히려 공개하여 신뢰를 회복하는 것이 중요하다고 주장하였다. Kong 등(2012)은 개인정보보호를 포함한 정보보호에 대하여 기업 입장에서 중요한 투자 분야임에도 불구하고 체계적인 성과평가와 방법론이 부족함을 지적하였다. 이에 BSC 관점에서 실증분석하여 보안 투자 시 핵심 성과지표들에 대하여 제시하였다. 김민정 등(2016)은 개인정보 유출 사고와 정보보호 기업의 주가 변동에 대하여 연구하였다. 연구 결과, 개인정보 유출 사고가 발생할 경우, 정보보호 업체의 주가는 상승하였다. 해당 결과를 통해 개인정보 유출 사고가 발생할 경우 개인정보보호 인식이 상승하고 정보보호 수요가 증대됨에 따라 정보보호 관련 업체의 주가 역시 상승하는 것으로 나타났다. 김정규와 이경호(2017)는 개인정보 유출 사고에 대하여 기업의 위험과 손해금액을 산출하기 위해 위험분석 방법론인 FAIR을 국내에서 대표적으로 발생한 개인정보 유출 사례에 적용하였다. 연구 결과를 바탕으로 개인정보 유출 사고가 발생할 경우 대처 비용, 사고에 대한 상세한 정보 등을 법적으로 공개함으로서 개인정보 처리자가 민감하게 수용하고 개인정보를 예방할 수 있도록 공유하는 환경을 구축해야한다고 주장하였다. 이한솔과 채상미(2018)는 정보보호 투자가 개인정보 침해사고에 미치는 영향에 대하여 정보보안 교육 서비스 투자를 중심으로 2014년 정보보호 실태조사 결과를 활용하여 연구하였다. 연구 결과, 취약점 관련 서비스와 정보보호 교육 서비스가 실제 개인정보 유출 사고를 감소시키는데 영향을 미치는 것으로 나타났으며, 이를 통해 단순히 정보보호 관련 서비스를 이용하는 것이 아니라 교육 서비스 역시도 중요한 방안 중 하나가 될 수 있음을 제시하였다. 기업의 관점에서 개인정보 유출로 인한 사회적 현상에 대하여 연구들이 이루어지고 있다. 선행연구들을 통해 개인정보 유출은 기업의 입장에서 경제적 손실을 일으키므로 유출 원인과 정확한 피해 규모 등을 확인하여

유출 방지 대책 및 개인정보 관리 방안을 수립해야 하지만, 근거로서 활용되는 개인정보 유출 사고에 대한 정보가 부족하여 많은 한계점을 지닌다는 것을 알 수 있다.

2.3 개인정보 유출 사고 및 유관 사례 중심의 연구

개인정보 유출과 이에 대응하기 위한 방안들, 유출 사고와 관련이 있는 사회적 현상 등 개인정보 유출 사고를 중심으로 다양한 주제들로 연구가 되고 있으며, 더 나아가 개인정보 유출 사고를 중심으로 사고 내용들 속에 있는 의미에 대하여 연구되고 있다. Angst et al.(2017)은 의료 분야에서의 개인정보 유출에 대한 심각성을 인식하고, 미국 병원의 938건의 위반사항을 수집하여 실제 위반으로 이어지는 가능성에 대하여 연구하였다. 연구 결과, 개인정보 보호를 위해 투자 규모 및 기간은 의료 분야의 개인정보 유출에 직접적인 영향을 미치지 않고, 제도적인 지원이나 장치를 통해 보안 투자가 개인정보 유출을 감소시키는 것으로 나타났다. 이를 통해 단순 IT 보안 투자에는 한계가 존재하며 의료 및 IT 분야의 제도적 지원이 필요하다고 주장하였다. Goode et al.(2017)은 2011년 발생한 소니의 개인정보 유출 사고 정보를 활용하여 개인정보 유출 후 서비스 복구 노력과 사후 보상에 따른 고객의 보상 효과에 대하여 연구하였다. 연구 결과, 개인정보 유출에 대한 서비스에 대한 노력과 사후 보상이 적절할수록 고객에 대한 보상 효과가 영향을 미치는 것으로 나타났다. 이를 통해 개인정보 유출 사고가 발생하면 이에 대한 대응은 단순히 기술적, 관리적 보호 차원의 대응 뿐만 아니라 고객 대상의 서비스 복구 및 보상 역시 중요하다는 것을 알 수 있다. 곽영암(2014)은 2008년과 2011년에 발생한 개인정보 유출 사고 4건의 소송 내용에 대하여 분석하였다. 피해자는 자신에게 발생한 손해의 크기와 범위를 입증하는 것이 어려우며, 피해자들의 피해구재를 위해 입증책임 전환, 징벌적 손해배상제도의 도입 등이 필요하다고 주장하였다. 류승훈(2016)은 빈번히 발생하고 있는 개인정보 유출 사고에 따라 피해가 발생한 소비자들은 집단소송에 의해 손해배상을 청구하고 있는데, 이에 대하여 2차적 피해가 발생해야만 위자료청구가 가능하다는 대법원 판례에 의문을 가지고, 사례를 기반으로 법정손해배상제도에 대하여 연구하였다. 연구 결과, 개인정보가 유출될 경우 2차적 피해 발생 우려가 내재되어 있기 때문에 이에 대하여 적극적으로 배상해야 함을 주장하였다. 박수항과 장경배(2016)는 기존의 개인정보보호 개선 방안에 대한 연구들과 달리 개인정보 유출 사고 내용을 통해 도출하고자 하였으며, 이를 위해 2006년부터 2014년까지 발생한 7건의 대규모 개인정보 유출 사고에 대하여 판례를 분석하였다. 분석 결과를 통해 내부자 유출에 대한 위험성을 경고하였으며, 개인정보 유출 사고로 인해 발생하는 피해를 구제할 수 있는 방안을 구체화하는 것이 필요하다고 제시하였다. 황윤희와 유진호(2016)는 과거부터 현재까지 발생하는 개인정보 유출 사고에 대하여 패턴을 찾고 분포를 추정하기 위해 2011년부터 2014년까지 발생한 개인정보 유출 사고에 대하여 분석하였다. 개인정보 유출 사고 중심의 연구들은 주로 판례를 통해 유출 사고에 대하여 분석하였으며, 일부 연구들의 경우 언론보도 자료를 통해 직접 정보를 수집하여 개인정보 유출 사고의 추이와 분포 등을 추정한 것으로 나타났다. 하지만 개인정보 유출 사고의 정보에 초점을 두고 기업의 특성과 개인정보 유출 사고간의 관계에 대해서는 분석된 경우가 없었다.

본 연구에서 다루고자하는 개인정보 유출 사고에 대한 정보는 2005년부터 2018년까지 언론 보도자료를 통해 공개되어 있는 실제 사건에 대한 정보이다. 이를 통해 개인정보 유출 사고에 보다 중점을 두어 사고의 요소와 기업의 특성이 어떠한 영향 관계에 있는지 연구하고자 한다. 이러한 부분에서 기존 연구들과 차별점을 두고 있다.

〈표 1〉 개인정보 유출에 대한 문헌 연구

연구 분야	저자	연구 내용	연구 주제
개인정보 유출 위협과 개인정보 보호 방안	Karger(2006)	개인정보 보호를 위한 암호화 기반 솔루션	기술적 개인정보 보호
	이재광 외(2007)	개인정보 익명화 암호화 기술	기술적 개인정보 보호
	엄정호 외(2010)	내부자 유출 방지를 위한 접근통제	기술적 개인정보 보호
	채승완(2008)	개인정보의 경제적 가치 효과	관리적 개인정보 보호
	정기석(2014)	개인정보 유출사고에 대한 원인과 정부 대책	관리적 개인정보 보호
	정명수, 이경호(2015)	개인정보보호 관리수준 진단 효율성 평가	관리적 개인정보 보호
	Acquisti(2009)	개인정보의 자기결정권	행동·심리학적 접근
	조동원(2012)	개인정보 해킹 행위에 대한 연구	행동·심리학적 접근
	김준영, 김태성(2017)	정부유출의도에 대한 영향 요인	행동·심리학적 접근
	이동희, 김태성(2018)	패스워드 보안 행위 의도에 대한 영향 요인	행동·심리학적 접근
개인정보 유출 사고로 인한 사회적 현상에 대한 연구	강이주, 황전선(2001)	개인정보 유출과 개인정보 보호 의식에 대한 연구	개인 관점의 개인정보 유출
	김소라, 이기춘(2006)	개인정보 유출 피해에 대한 소비자 유형별 분석	개인 관점의 개인정보 유출
	윤승욱 외(2008)	개인정보 유출에 따른 위험성 인지에 대한 연구	개인 관점의 개인정보 유출
	천명호 외(2013)	개인정보 유출 방지를 위한 개인정보 유출 위험도 측정	개인 관점의 개인정보 유출
	유승동, 유진호(2014)	개인정보 보호를 위한 지불의사비용 결정요인	개인 관점의 개인정보 유출
	유진호 외(2009)	개인정보 유출에 따른 기업의 손실 비용 추정	기업 관점의 개인정보 유출
	Kong et al.(2012)	BSC 관점의 정보보호 투자에 대한 연구	기업 관점의 개인정보 유출
	김민정 외(2016)	개인정보 유출 사고와 정보보호 기업의 주가 변동	기업 관점의 개인정보 유출
	김정규, 이경호(2017)	FAIR 방법을 활용한 개인정보 유출에 따른 기업 손해금액 산출	기업 관점의 개인정보 유출
	이한솔, 채상미(2018)	정보보호 투자가 침해사고에 미치는 영향에 대한 연구	기업 관점의 개인정보 유출
개인정보 유출 사고 및 관련 사례에 대한 연구	Angst et al.(2017)	의료분야 위반 사례를 중심으로 의료 분야 개인정보 유출 가능성 분석	의료 분야, 개인정보 위반 가능성
	Goode et al.(2017)	소니 유출 사고를 중심으로 개인정보 유출에 대한 보상과 개인의 보상 효과에 대한 연구	특정 사고, 유출 사후 소비자와의 관계
	곽영암(2014)	2008년~2011년 4건의 개인정보 유출 사건 판결 분석	판례, 손해배상
	류승훈(2016)	개인정보 유출에 따른 손해배상 관련 분석	판례, 손해배상
	박수황, 장경배(2016)	2006년~2014년 7건의 개인정보 유출 사례 분석을 통한 피해구제 방안 도출	판례, 피해구제
	황윤희, 유진호(2016)	2011년~2016년 개인정보 유출 사고 분석을 통한 분포 추정	개인정보 사고 패턴 및 분포 추정

3. 개인정보 유출 사고 조사

3.1 조사 개요

2005년부터 2019년까지의 개인정보 유출사고를 조사하기 위해 google을 활용하였으며, '개인정보 유출', '개인정보 침해', '개인정보 노출', '개인정보 해킹'이라는 4가지 개인정보 유출 사고와 관련된 주요 키워드를 활용하여 미디어 매체 및 정부 기관에서 발표하는 언론 보도 자료를 조사하였다. 여러 보도자료에서 개인정보 유출에 대하여 개인정보 노출, 개인정보 침해 등이 뜻이 다르더라도 혼용하여 사용하고 있기 때문에 단순히 개인정보 유출이라는 키워드만을 활용하지 않고 유사한 단어들을 모두 키워드로 사용하였다.

조사 항목은 사고 발생 시기(연도, 월), 인지 시기(연도, 월), 기업명, 유출된 정보 건 수, 유출 정보 유형, 사고 내용 등 6개이다. '사고 발생 시기'는 기

업에 개인정보 유출사고가 발생한 시기이다. '인지시기'는 개인정보 유출 사고가 발생한 기업의 조사 혹은 정부 기관의 수사로 인하여 개인정보 유출 사고 사실에 대하여 인지한 시기이다. '기업명'은 개인정보 유출사고가 발생한 기업의 명칭이다. '유출 정보 건 수'는 유출된 정보의 수이며, 유출 정보 주체의 수를 뜻하는 것은 아니다. 언론 보도 자료에서 유출된 정보의 수와 정보 주체의 수를 혼동하여 개인정보 유출 사고의 규모를 설명하고 있기 때문에 공통적으로 도출할 수 있는 유출된 정보의 수를 유출 정보 건수로 정의하였다. '유출 정보 유형'은 유출된 정보의 유형으로 이름, 주민등록번호, 이메일 주소, 연락처 등이다. '사고 내용'은 구체적으로 사고의 원인부터 결과에 이르는 상세적인 내용이다.

개인정보보호와 관련된 기업의 특성은 기업의 규모로 선정하였다. 개인정보보호법과 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에서는 기업의 규모에 따라 그 기준을 지정하고 있기 때문에 기업의 규모를 기업의 특성으로 선정하고, 기업의 규모를 대표적으로 나타내는 '매출액'과 '종사자 수'를 선정하여 개인정보가 유출된 기업의 정보를 함께 조사하였다. 유출 사고 발생 기업의 규모를 조사하기 위해 기업의 매출액과 종사자에 대한 정보를 공개하고 있는 '잡코리아', '사람인' 등의 구인구직 사이트를 활용하였다.

3.2 조사 결과

개인정보 유출 사고 사례를 언론 및 정부기관 보도 자료를 통해 조사한 결과, 2005년부터 2019년까지 발생한 사고 사례 80건을 수집하였으나, 개인정보 유출 사고에 대하여 상세하게 정보를 제공하고 있지 않은 10건이 존재하여 이를 제거하고 최종적인 조사 결과 및 분석 자료로서 활용하였다. 또한 70건의 개인정보 유출 사고가 발생한 기업의 특성(규모)을 별도로 조사하였다(<표 2> 참조).

보도 자료의 내용을 기반으로 하고 있어 공식적으로 발표되지 않은 내용에 대해서는 조사할 수 없다. 유출 정보 유형의 경우 모든 유출 정보 유형을 공개하고 있지 않고 개괄적으로 공개하고 있는 경우가 다수이다.

〈표 2〉 개인정보 유출 사고 사례 정보

구분	기업명	개인정보 유출 사고 관련 정보(언론보도자료)					기업 관련 정보 (기업 규모)	
		발생시기	인지시기	사고 유형	유출 정보 건수	유출 정보 유형 수	매출액 (억 원)	종사자 (명)
1	**소프트	2005.05	2008.05	내부 실수 및 부주의	500,000	2	15,299	3,683
2	다*	2008.03	2008.04	외부자 해킹	7,000	1	5,020	1,590
3	옥*	2008.02	2008.04	외부자 해킹	10,810,000	6	6,625	899
4	***텔레콤	2008.04	2008.04	내부자 유출	85,000,000	6	117,000	5,377
5	**칼텍스	2008.07	2008.08	내부자 유출	11,190,000	5	355,195	3,271
6	**캐피탈	2009.09	2010.03	외부자 해킹	90,000	4	6,073	372
7	I**캐피탈	2009.09	2010.02	외부자 해킹	35,765	7	3,607	199
8	****공단	2010.06	2010.07	내부자 유출	100,000	4	214,000	5,623
9	**캐피탈	2010.01	2013.01	내부자 유출	5,000	4	9,681	449
10	**카드	2010.01	2011.08	내부자 유출	470,000	11	32,537	1,961
11	****공단	2011.01	2011.01	내부 실수 및 부주의	15,556	4	214,000	5,623
12	넥*	2011.11	2011.11	외부자 해킹	13,200,000	4	16,386	4,500
13	***손	2011.08	2011.08	외부자 해킹	350,000	4	1,351	91
14	** *트랙	2008.08	2011.08	외부자 해킹	210,000	2	14,000	2,047
15	*TV	2011.08	2011.08	외부자 해킹	300,000	5	79	86
16	**커뮤니케이션즈	2011.07	2011.07	외부자 해킹	35,000,000	6	416	300
17	**즌	2010.06	2011.05	외부자 해킹	1,400,000	10	15	12
18	I**캐피탈	2011.01	2013.05	내부자 유출	6,000	4	3,607	199

19	****카드	2011.07	2011.09	내부자 유출	97,000	3	8,845	486
20	N***증권	2011.06	2011.06	내부 실수 및 부주의	15,000	3	89,515	2,969
21	솔****증권	2011.05	2011.05	외부자 해킹	32	0	5,386	237
22	리***증권	2011.05	2011.05	외부자 해킹	13,000	3	890	133
23	*****보험	2011.03	2011.05	외부자 해킹	157,901	3	74,229	3,243
24	*****원	2011.05	2011.05	외부자 해킹	8,000	0	2,089	530
25	솔****정보	2011.04	2010.06	외부자 해킹	751	0	297	150
26	**캐피탈	2011.05	2011.06	외부자 해킹	1,750,000	2	29,819	2,371
27	**S	2012.05	2012.05	외부자 해킹	4,000,000	6	2,496	622
28	*T	2012.02	2012.07	외부자 해킹	8,700,000	10	173,565	23,389
29	하***증권	2012.04	2012.05	내부 실수 및 부주의	2,300	5	8,146	769
30	**텔레콤	2011.08	2012.03	내부자 유출	198,000	8	117,000	5,377
31	*T	2012.02	2012.04	외부자 해킹	198,000	0	173,565	23,389
32	코**	2013.06	2013.06	외부자 해킹	1,980,000	4	23,954	5,011
33	***화재	2011.11	2013.11	내부자 유출	163,925	6	83,914	2,845
34	****은행	2014.12	2014.12	외부자 해킹	130,000	8	28,206	4,383
35	**은행	2014.03	2014.03	내부 실수 및 부주의	130,000	3	30,428	3,528
36	******력	2014.03	2014.04	외부자 해킹	10,799	7	88,587	12,392
37	****회	2011.03	2017.07	외부자 해킹	13,900	7	1,071	2,615
38	**교육	2014.12	2014.12	외부자 해킹	1,048,576	3	859	351
39	**교육	2014.09	2014.10	외부자 해킹	3,500,000	7	1,850	523
40	**통	2012.04	2014.03	외부자 해킹	130,000	4	220	20
41	판**TV	2013.02	2014.03	외부자 해킹	110,000	6	191	57
42	***조이	2011.04	2014.03	외부자 해킹	420,000	4	80	100
43	*T	2012.12	2014.03	외부자 해킹	12,000,000	4	173,565	23,389
44	****터	2011.02	2014.03	외부자 해킹	1,130,000	4	4,972	1,300
45	*T	2012.01	2014.01	내부자 유출	7,070,000	4	173,565	23,389
46	*****밴드	2014.01	2014.03	외부자 해킹	7,070,000	3	31,588	1,721
47	***플러스	2013.04	2014.04	내부자 유출	7,070,000	4	120,900	10,735
48	**버	2009.06	2015.03	내부자 유출	100,000,000	4	42,000	2,512
49	****카드	2012.09	2015.03	내부자 유출	53,000,000	4	30,405	1,571
50	****카드	2011.12	2015.03	내부자 유출	26,000,000	4	122,552	16,875
51	**카드	2013.09	2014.03	내부자 유출	25,000,000	2	15,017	1,631
52	**캐피탈, **캐피탈	2013.08	2014.08	외부자 해킹	34,000	3	3,724	319
53	**마트	2014.05	2014.05	외부자 해킹	2,500,000	5	102,177	18,012
54	*마트	2013.02	2014.04	내부 실수 및 부주의	3,112,000	3	131,000	25,797
55	*플러스	2011.06	2014.04	외부자 해킹	7,120,000	8	85,134	19,045
56	****통운	2015.08	2015.09	외부자 해킹	382	7	62,282	6,379
57	****통운	2016.05	2016.07	외부자 해킹	1,000	9	62,282	6,379
58	**모리	2016.04	2016.04	내부자 유출	500,000	3	1,690	163
59	B**	2017.06	2017.06	외부자 해킹	510,000	3	2,300	350
60	스킨**	2017.06	2017.06	내부 실수 및 부주의	550,000	5	652	97
61	**파크	2017.03	2017.03	외부자 해킹	25,000,000	2	4,385	1,293
62	****항공	2016.12	2017.03	내부자 유출	45,000	4	62,012	9,054
63	*썸	2013.09	2017.07	외부자 해킹	30,000	6	3,916	324
64	**프	2011.05	2017.07	외부자 해킹	35,000	6	4,294	1,800
65	J*****은행	2018.04	2018.04	외부자 해킹	284,000	0	2,243	555
66	**투어	2017.07	2017.07	외부자 해킹	574,405	4	5,420	2,522
67	****선물	2013.09	2017.07	외부자 해킹	300,000	6	742	78
68	**유업	2011.05	2017.07	외부자 해킹	1,000,000	6	10,706	2,523
69	***소프트	2017.02	2017.09	외부자 해킹	133,800	2	215	185
70	***쇼핑	2018.04	2018.04	외부자 해킹	1,950	5	1,254	47

〈표 3〉 개인정보 유출 사고 유형 분류 기준

구분		위협의 특징	
		우연적	고의적
위협 원천	외부	자연재해 → 우연적 외부 노출	악성코드, Dos, 산업스파이 → 외부자 해킹
	내부	업무상 실수 → 내부 실수 및 부주의	정보 유출, 물리적인 파괴, 태업 → 내부자 유출

조사 내용 중 유출 사고 유형의 경우, 위협의 원천과 특징을 기준으로 분류하였다(<표 3>참조)(김태성, 2002).

4. 표본의 특성

4.1 연도별 개인정보 유출 사고 규모

개인정보 유출 사고의 분포와 추이를 확인하기 위해 유출 사고 건 수와 규모를 연도별로 분류하였다(<표 4> 참조). 분류 시 개인정보 유출 인지 시기가 아닌 실제 발생한 시기를 기준으로 분류하였다.

〈표 4〉 연도별 개인정보 유출 사고 규모

연도 구분	개인정보 유출 사고 수	유출된 개인정보 수	개인정보 유출 사고 1건당 평균 유출 정보 수
2005	1	500,000	500,000
2006	0	0	0
2007	0	0	0
2008	5	107,217,000	21,443,400
2009	3	2,625,765	875,255
2010	4	1,975,000	493,750
2011	23	163,089,816	7,090,862
2012	8	133,804,300	16,725,538
2013	8	51,084,382	6,385,548
2014	7	20,964,699	2,994,957
2015	1	1,950,000	1,950,000
2016	3	25,284,598	8,428,199
2017	5	1,363,027	272,605
2018	2	3,900	1,950
합계	70	509,862,487	7,283,750

2005년 5월부터 2018년까지 개인정보 유출 사고를 연도별로 분석한 결과, 2011년에 23건으로 가장 많이 발생하였다. 2012년, 2013년에 8건으로 두 번째로 많은 개인정보 유출 사고가 발생하였다. 2005년부터 2018년까지 발생한 개인정보 유출 사고로 유출된 개인정보는 5억 개 이상이며, 개인정보 유출사고 1건당 7백만 개 이상의 개인정보가 유출되는 것으로 나타났다. 개인 정보 유출 사고는 2011년에 가장 많이 발생하였고, 2011년 이후 2014년까지 개인정보 유출 사고 수가 다른 연도에 비하여 대규모로 빈번히 발생한 것을 알 수 있다. 또한, 개인정보가 가장 많이 유출된 시기는 2011년이었지만 개인정보 유출 사고 1건당 유출된 개인정보가 많았던 시기는 2012년이었다는 것을 알 수 있다. 개인정보 보호법이 시행된 연도인 2011년에는 개인정보 유출사고가 가장 많은 시기였으나, 개인정보 유출에 대한 법적 책임이 강화되고 기업의 기술적, 관리적 개인정보 보호 활동이 증가함에 따라 유출 사고의 수와 그 규모가 감소하게 되는 기점으로도 볼 수 있다. 하지만 이후로도 개인정보 유출 사고 수는 꾸준하게 발생하고 있는 상황이다.

개인정보 유출 규모는 개인정보 유출 사고의 결과를 대표하는 요소로서 유출 사고의 연관성을 규명하는데 핵심요소가 된다.

4.2 피해 유형별 개인정보 유출 사고

개인정보 유출 사고 수는 전체 73건으로 내부자 유출이 26건이고 외부자 유출은 47건으로 나타났다(<표 5> 참조).

〈표 5〉 피해 유형별 개인정보 유출 사고

구분	내부자 유출	내부 실수/부주의	외부자 해킹	우연적 외부 노출	합계
유출 사고 수	17	7	46	0	70
비율(%)	24.3	10	65.7	0	100.0

유출 사고의 대부분은 외부 협력업체, 유출된 기업과 관계가 없는 제 3자(해커 포함) 등 기업 외부자에 의하여 발생한 개인정보 유출 사고 수가 기업 내부자의 의도적 혹은 단순 실수 등으로 인하여 발생한 개인정보 유출 사고 수 보다 많은 것(65.7%)으로 나타났다. 하지만 내부자로 인한 유출 사고 수 역시 24.3%로 많은 비중을 차지하는 것으로 나타났다. 이를 통해 개인정보 유출 사고 방지를 위해서는 외부의 위협을 방지하는 것이 중요하지만, 내부의 위협을 지속적으로 줄일 수 있는 방안에 대하여 고민해야 함을 알 수 있다.

개인정보 유출 사고가 내부와 외부 중 발생지 위치에 따라 그 규모가 달라질 수 있다.

4.3 개인정보 유출 사고 발생시기와 인지시기의 차이

개인정보를 보유한 기업은 보안 모니터링 수준에 따라 개인정보 유출 사실을 확인하는 시기가 다르다. 기술적 및 관리적으로 보안 모니터링 수준이 높은 기업은 개인정보 유출 사고가 발생할 경우 빠른 시기에 유출 사실을 인지하고 즉각적인 대응을 할 수 있으나, 보안 모니터링 수준이 낮은 기업은 상대적으로 유출 사실을 뒤늦게 확인하게 되며, 대응 역시 늦어져 사고로 인한 피해가 증가하게 된다. 2005년부터 2018년까지 발생한 개인정보 유출 사고 역시 유출 발생 기업마다 발생 시기와 인지시기의 차이가 다양하게 나타났다(<표 6> 참조).

개인정보 유출사고 발생시기와 인지시기 간의 차이가 1개월 미만으로 발생한 사고는 23개(32.9%)이며, 1개월 이상인 사고가 18개(25.7%)로 많은 비중을 차지하고 있다. 시기 차이가 1년 이상 차이나는 사고는 29개(41.4%)로 일정 부분을 차지하는 것으로 나타났다. 유출사고 발생 시 즉각적으로 인지하고 대응함으로써 유출사고로 인한 피해를 줄여야 함에도 불구하고, 기술적·관리적 보안 활동의 부족으로 개인정보 유출사고 발생을 늦게 인지하는 경우가 많은 것으로 나타났다. 이러한 차이를 통해 개인정보를 수집하고 관리하는 기업은 개인정보에 대한 지속적인 모니터링을 실시하고, 개인정보 유출사고 관리 방안을 수립하여 즉각적으로 유출사고에 대응할 수 있도록 사전에 준비해야 함을 알 수 있다.

〈표 6〉 개인정보 유출 사고 발생과 인지시기의 차이

구분	개인정보 유출 사고 수(건)	비율 (%)
1개월 미만	23	32.9
1개월 이상~6개월 미만	18	25.7
6개월 이상~1년 미만	4	5.7
1년 이상~3년 미만	13	18.6
3년 이상~5년 미만	8	11.4
5년 이상	4	5.7
합계	70	100.0

분석 결과를 통해 개인정보 유출 발생시기와 인지시기간의 차이는 개인정보 유출 사고가 발생한 기업의 개인정보 유출에 대응할 수 있는 개인정보보호 수준을 간접적으로 표현할 수 있는 요소로 활용 될 수 있음을 확인하였다.

4.4 유출된 개인정보의 유형

유출된 개인정보의 유형은 이름, 아이디, 비밀번호, 암호화된 주민등록번호, 전화번호, 주소 등 다양하다(<표 7> 참조).

개인정보 유출 사고를 통해 평균적으로 유출되는 개인정보 유형 수는 4개이며, 가장 많이 유출된 정보 유형의 수는 11개였으며, 1개의 개인정보 유형만 유출된 사고도 존재한다.

〈표 7〉 유출된 개인정보의 유형

구분	평균	표준편차	중앙값	최대값	최소값
유출된 개인 정보 유형 수	4	2	4	11	1

5. 연구 설계 및 분석

본 연구에서는 개인정보 유출 사고라는 실제 일어난 사건의 데이터를 기반으로 하고 있다. 개인정보 유출 사고 데이터의 경우, 각 사고별로 유출 정보의 수와 유출 정보의 유형이 각기 다르기 때문에 데이터가 균질적이지 않다. 데이터가 균질적이거나 군집화되지 못할 경우 데이터의 신뢰성과 타당성을 분석하는데 한계가 존재한다. 더 나아가 요인간의 관계를 확인하는데 일반적으로 사용되는 다중회귀모형을 적용할 수 없다. 이에 본 연구에서는 SPSS를 활용하여 상관관계분석을 통해 설정한 가설에 대하여 검증하였다.

5.1 변수 선정 및 가설 설정

개인정보 유출 사고 요소간의 연관성을 분석하기 위해 개인정보 유출 사고의 결과를 표현하는 유출 사고의 규모를 기준으로 유출 사고 유형, 유출 시기와 인지 시기간의 차이, 유출된 개인정보 유형 수의 상관관계를 분석하였다.

또한 기업의 특성인 규모와 개인정보 유출 사고간의 관계를 분석하기 위해 유출 사고가 발생한 기업의 매출액과의 종사자 규모와 개인정보 유출 사고의 요소들 간의 관계를 가설로 설정하였다.

개인정보 유출 사고의 유형은 앞서 설명한 바와 같이, 위협의 특징과 원천에 따라 4가지로 분류될 수 있다. 본 연구에서 재해석한 개인정보 유출 유형은 내부자 유출(내부, 고의적), 내부 실수 및 부주의(내부, 우연적), 외부자 해킹(외부, 고의적), 우연적 외부 노출(외부, 우연적)으로 구분하였다. 숫자 1에 가까울수록 내부에서 고의적인 의도로 발생한 사고이며, 숫자 4에 가까울수록 외부에서 우연적으로 발생한 사고로 정의하였다. 사고의 유형과 관련하여 정익재 등(1996)은 재난의 유형과 재난 사고 및 관리에 대하여 연구하였다. 실제 재난 사고의 유형이 재난 사고 결과와 관계가 있으며, 유형별로 관리가 필요하다는 것을 간접적으로 제시하였다. 개인정보 유출사고는 재난의 속성과 많이 유사하고, 유출 사고 역시 유형별로 결과가 다를 것으로 표본의 특성에서 확인하였기 때문에 이를 상관관계 분석에서 확인하고자 한다. 이에 본 연구에서는 다음과 같은 가설을 도출하였다.

가설 1 : 개인정보 유출 사고가 내부 요인으로 인하여 발생할수록 개인정보 유출 사고의 규모는 커진다.

개인정보 유출사고의 발생 시기와 인지 시기간의 차이는 유출사고가 발생한 기업의 정보보호 수준을 뜻한다. <표 5>를 통해 시기간의 차이가 개인정보 유출 사고의 규모를 증가시키는데 관계가 있을 것으로 분석된다. 행정학 분야에서는 정책에 대한 시차문제가 정책 효과에 영향을 미치는 것으로 연구되고 있다. 김상봉 등(2008)에서도 시차에 대한 문제가 사회현상에 영향을 미치고 더 나아가 특정 시점에 대한 분석이 필요하다고 주장하였다. 정보보호 분야의 취약점과 관련된 연구들에서는 취약점 발견시기와 패치시기간의 차이에 대하여 중요하게 다루고 있다. 또한 취약점에 대한 정보를 공개함으로써 시스템에 발생하는 공격의 발생 시간을 늦추고 공격 확산 확률 및 피해규모를 감소시키는 등 공격으로부터의 피해규모를 줄일 수가 있다(Ransbotham 외, 2012). 이렇듯 일반적인 정보보호 분야에서는 취약점 발견과 패치시기와 관련되어 연구되고 있으며, 해당 시기를 일(day)을 기준으로 하고 있다. 하지만 개인정보 유출 사고의 경우 발생 연도(year)와 월(month)까지는 대부분 공개되지만 일(day)까지는 공개되는 경우가 드물기 때문에 본 연구에서는 개월 수를 단위로 분석하고자 한다. 이에 본 연구에서는 다음과 같은 가설을 도출하였다.

가설 2 : 개인정보 유출 사고가 발생한 시기와 인지한 시기간의 차이가 클수록 개인정보 유출 사고의 규모는 커진다.

유출된 개인정보의 유형 수는 유출된 개인정보의 종류를 뜻한다. 유출되는 정보의 유형 수가 많을수록 개인정보 유출 규모가 커진다고 판단할 수 있다. 이에 본 연구에서는 다음과 같은 가설을 도출하였다.

가설 3 : 유출된 개인정보의 유형 수이 다양할수록 개인정보 유출 사고의 규모는 커진다.

기업의 특성 중 하나인 규모는 매출액과 종사자 수로 표현된다. 특히 개인정보 유출 시 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의거하여 과징금 범위, 정보보호관리체계(ISMS-P) 인증 의무 대상자 기준, 손해배상을 위한 사이버 보험 가입 대상자의 범위 및 기준 등을 매출액에 따라 분류하고 있다. 특히 개인정보 유출사고로 인하여 발생하는 피해와 그 보상에 대하여 완화할 수 있는 방안으로서, 정보통신망법 제 32조와 동법 시행령 18조의 2에서는 사이버 보험에 가입하도록 하고 있다(법제처, 2019). 사이버 보험의 가입액의 경우 최근 사업연도의 매출액과 직전연도 기준 최근 3개월간 일일 평균 이용자 수에 따라 금액을 다르게 책정하고 있다. 이는 기업의 매출액 규모에 따라 정보보호 책무를 부과하는 것으로 판단할 수 있다. 이에 따라 매출액이 클수록 정보보호 책무를 다하고 있으며 정보보호 수준이 높기 때문에 개인정보 유출사고의 규모가 작을 것으로 판단된다. 이에 본 연구에서는 다음과 같은 가설을 도출하였다.

가설 4 : 기업의 매출액이 클수록 개인정보 유출 사고의 규모가 작다.

기업의 특성인 종사자 규모에 대한 설명은 다음과 같다. 개인정보 유출사고의 98%가 중소기업에서 발생하고 있으며, 종사자 10인 미만의 기업 60% 이상이 IT예산이 적었고, 정보보호 예산이 없는 상황이다. 또한 종사자 수가 250인 미만인 기업들은 별도로 정보보호 전담 인력을 배치할 여력이 없는 것으로 나타났다(한국인터넷진흥원, 2019). 이를 통해 기업의 종사자 규모가 작은 기업일수록 정보보호 수준은 낮고, 정보보호에 투자할 여력이 없으며 더 나아가 개인정보 유출에 더욱 노출되어 있음으로 판단된다. 이에 본 연구에서는 다음과 같은 가설을 도출하였다.

가설 5 : 기업의 종사자가 작을수록 개인정보 유출 사고의 규모가 크다

5.2 분석 결과

개인정보 유출 사고 요소간의 상관관계와 기업의 특성과의 관계를 분석하기 위해 SPSS의 상관관계 분석을 진행하였으며, 그 결과는 <표 8>과 같다.

〈표 8〉 개인정보 유출사고 요소 간의 상관관계와 기업 특성간의 관계에 대한 분석 결과

구분		종사자	매출액	유출 규모	유출 사고 유형	유출 정보 유형	발생시기와 인지시기의 차이
종사자	상관계수	1					
	유의확률	.000					
매출액	상관계수	**.651****	1				
	유의확률	**.000**	.000				
유출 규모	상관계수	.050	.119	1			
	유의확률	.897	.327	.000			
유출 사고 유형	상관계수	-.127	**-.406****	**-.349***	1		
	유의확률	.294	**.000**	**.003**	.000		
유출 정보 유형 수	상관계수	.104	.104	.023	-.016	1	
	유의확률	.393	.393	.847	.892	.000	
발생시기와 인지시기의 차이	상관계수	.033	-.095	.185	-.111	.168	1
	유의확률	.784	.434	.125	.359	.165	.000

*, **는 각각 5%, 1% 수준에서 유의함.

상관관계 분석 결과, 매출액과 종사자는 양의 상관관계를 갖는 것으로 나타났다($r = .651$, $p < 0.01$). 유출 사고 유형은 유출 규모와 음의 상관관계를 갖는 것으로 나타났다($r = -.349$, $p < 0.05$). 유출 사고 유형은 매출액과 음의 상관관계를 갖는 것으로 나타났다($r = -.406$, $p < 0.01$). 상관관계 분석 결과를 바탕으로 가설에 대한 검증 결과를 확인하였다.

가설 1에 대하여 검증한 결과, 상관관계가 있는 것으로 나타났다. 해당 결과를 통해 개인정보 유출 유형이 내부에서 고의적으로 일어날수록 개인정보 유출 사고 규모가 커짐을 나타낸다. 내부 직원이 고의적인 의도로 개인정보에 접근하여 유출할 경우 그 유출 규모 및 피해 규모는 커짐을 의미한다. 이를 통해 기업은 개인정보 유출 사고에 대응하기 위해 외부의 위협을 막을 수 있는 정보보호 대책을 적용해야 할 뿐만 아니라, 내부의 위협을 관리할 수 있는 기술적·관리적 방안을 수립하고 지속적으로 실행해야 함을 뜻한다.

가설 2에 대하여 검증한 결과, 상관관계가 없는 것으로 나타났다. 해당 결과를 통해 개인정보 유출 발생 시기와 기업이 유출이 발생했다고 인지한 시기간의 차이가 개인정보 유출 규모에 영향을 미치지 않는 것으로 나타났다. 이러한 결과는 시기간의 차이가 기업의 정보보호 수준을 설명하지 않는다는 것을 의미한다.

가설 3에 대하여 검증한 결과, 상관관계가 없는 것으로 나타났다. 해당 결과를 통해 기업에 보관되어 있다가 위협으로부터 유출된 개인정보의 유형 수는 개인정보 규모에 아무런 영향이 없다는 것을 의미한다.

가설 4에 대하여 검증한 결과, 상관관계가 없는 것으로 나타났다. 해당 결과는 기업의 특성 중 하나인 기업의 규모가 개인정보 유출 사고 규모와 아무런 영향이 없다는 것을 의미한다. 이를 통해 기업의 규모가 작거나 크거나 개인정보 유출 사고의 규모는 크거나 작을 수 있으며, 더 나아가 기업의 규모에 상관없이 개인정보 유출 사고가 발생할 수 있음을 의미한다. 현재 정보통신망법과 정보보호 관리체계 인증 의무대상자, 손해배상을 위한 사이버 보험 가입 대상자 및 보험가입액 기준 등은 기업의 규모에 그 의미를 부여하고 있다. 각 기준에서 제시하고 있는 능력은 개인정보 유출에 대응 및 보상할 수 있는 능력과 관련이 있으나, 실제 발생하는 개인정보 유출 규모와는 직접 관련이 없다는 것을 의미한다. 그렇기 때문에 기업의 규모와 관계없이 기업의 개인정보보호에 대한 관리가 필요하며 이를 지속적으로 관찰하고 지원할 수 있는 방안이 필요하다.

가설과는 별개로 매출액과 유출사고 유형간의 관계가 음의 상관관계를 갖는 것으로 나타났다. 매출액이 클수록 내부적, 고의적 의도로 인한 유출사고가 발생할 수 있음을 의미한다. 이를 통해 큰 규모의 기업일수록 외부 뿐만 아니라 내부적 자원으로 인하여 발생할 수 있는 유출사고에 대응할 수 있는 대비책을 마련해야함을 알 수 있다.

6. 결 론

개인정보 유출 사고는 대기업과 중소기업 등 기업의 특성과 관계없이 발생하고, 그 피해규모 역시 예측할 수 없는 상황이다. 또한 기업은 개인정보 유출이라는 사회적 문제에 대하여 내·외부적으로 위험한 상황이다. 이에 본 연구에서는 개인정보 유출 사고 데이터를 수집하고 이를 분석하여 개인정보 유출 사고 요소 간의 상관관계를 찾아내는 것이 중요하며, 그 이전에 개인정보 유출 사고 데이터를 지속적으로 수집하고 분석하는 선행 단계가 필요함을 제시한다.

본 연구의 시사점은 다음과 같다. 첫째, 개인정보 유출 사고는 기업의 규모와 관계없이 발생하게 되며, 그 피해규모 역시 기업의 특성과 관계없이 크거나 작을 수 있는 것으로 나타났다. 하지만 개인정보 유출에 대하여 법적 구속력을 갖고 있는 사전 예방 차원의 개인정보보호 및 정보보호 관리체계 인증 의무와 사후 대응 차원의 손해배상을 위한 사이버 보험에 대한 의무 가입 기준은 기업의 규모인 매출액

및 종사자 수로 되어 있다. 개인정보 유출 사고 규모는 단순히 매출액이나 종사자 규모, 일일 이용자 수 등 기업의 규모가 아니라, 기업이 축적해온 이용자들의 개인정보의 규모에 비례하며 영세한 업체일수록 유출사고가 발생할 가능성이 높기 때문에 해당 기준들이 현실의 상황을 반영하지 못하고 있는 실정이다. 이에 따라 최근 3개월의 이용자수가 아니라 누적 이용자 수를 기준으로 정하고, 최근 매출액 등 인증 가입과 보험 가입 및 피해 보상에 대한 여력이 부족한 기업에게는 정책적인 지원을 함으로써 개인정보 유출사고로 발생하는 피해에 대하여 현실적인 예방 또는 보상이 이루어져야 한다. 더 나아가 기준을 수립하는 정부와 보호방안을 이행하는 기업 양측 모두 기업의 규모와 관계없이 개인정보 유출을 방지할 수 있는 전사적 대책을 강구해야 한다.

둘째, 개인정보 유출사고에 대응하기 위한 기술적・관리적 대책들은 주로 외부적인 위협에 대응하기 위한 방안들이 주로 이루고 있으나, 실제 유출사고는 내부와 외부 원인 모두에 의해 발생하고 있는 것으로 나타났다. 이를 통해 개인정보 유출사고에 대응하기 위해 내・외부적 위협 모두에 대응할 수 있는 체계적인 시스템이 필요하다고 판단된다. 또한, 그 기업의 규모가 클수록 내부적 요인으로 인한 위협에 더욱 주의하고 관리해야 한다는 것이다.

셋째, 개인정보 유출 사고 정보의 중요성에 대해서 제시하고 있다. 개인, 기업, 정부는 과거부터 현재까지의 개인정보 유출 사고에 대하여 전반적인 추이를 파악하고 이에 대응할 수 있는 정보를 보유하지 못하고 있는 상황이다. 이러한 정보는 민감성으로 인하여 수집 및 분석하는데 많은 어려움이 있다. 그러나 지속적으로 발생하는 개인정보 유출 사고에 대응하기 위해서는 데이터 획득 및 분석의 어려움을 해결하고 유출 사고에 대하여 면밀히 파악하는 것이 필요하다.

넷째, 기존의 개인정보보호 주제의 연구들에서는 주로 개인의 입장에서 영향 요인을 다루거나 개인정보보호를 위한 기술적, 관리적 방안 등에 대하여 연구되었으며, 특정 사건을 중심으로 개인정보 유출 사고의 파급효과를 분석하거나 발생 분포를 추정하였다. 하지만 앞선 연구결과들을 통해서 개인정보 유출 사고들의 추이를 파악하고 유출 사고의 요소 간의 관계나 유출 사고로 인하여 발생하는 사회적 문제와의 연결고리를 찾아내는 것은 어려웠다. 이에 본 연구에서는 2005년부터 2018년까지 언론 보도자료를 통해 공개되어 있는 실제 사건에 대한 정보를 분석하여 개인정보 유출 사고에 보다 중점을 두어 사고의 요소와 기업의 특성이 어떠한 영향 관계가 있는 지에 대하여 연구하였으며, 이를 통해 개인정보보호 분야에서 보다 더 넓게 연구 범위를 확장하였다는 점에서 의의를 갖는다.

본 연구에서는 개인정보 유출 사고라는 실제 사건을 기반으로 하는 데이터를 활용하고 있어, 데이터의 균질적이지 못하고, 군집화되지 못하여 일반적인 회귀분석을 활용하는데에는 한계가 존재하기 때문에 상관관계 분석을 활용하였다. 또한 일반적으로 정보보호 분야에서 사용되는 시기(시점)의 단위는 '일'(day)이지만 개인정보 유출 사고의 경우 발생한 시기와 인지한 시기에 대하여 연도, 월까지만 공개한 경우가 많기 때문에 월(month)을 기준으로 분석하였다. 이를 통해 개인정보 유출 사고에 대하여 정확하고 상세하게 분석하기 위해서는 지금보다 더 상세한 개인정보 유출 사고 관련 정보를 확인할 수 있는 수단과 환경이 필요하다. 이에 따른 본 연구의 한계점이 존재한다.

향후에는 개인정보 보호법 시행, 데이터 3법 개정 등 주요 환경 변화가 개인정보 유출 사고에 미치는 영향에 대한 분석이 추가로 필요할 것이다. 또한, 해외의 개인정보 유출 사고 및 환경과 비교함으로써 국내 개인정보보호 생태계의 특징들을 도출하는 과정이 필요하다.

참고문헌

강이주, 황정선, "전자상거래 소비자의 개인정보 보호의식에 관한 연구-사업자신뢰도와 정보유출 피해경험 효과를 중심으로", *소비문화연구*, 제4권,

제2호, 2001, 85-106.
고형석, “정보보호인증제도의 확대에 관한 연구”, *법과 정책연구*, 제16권, 제2호, 2016, 411-441.
곽영암, “개인정보유출 사건 판결에 관한 연구”, *전자상거래학회지*, 제15권, 제2호, 2014, 63-81.
김민정, 허남길, 유진호, “개인정보 유출 사고 시 정보보호 기업의 주가 변동에 관한 연구”, *정보보호학회논문지*, 제26권, 제1호, 2016, 275-283.
김상봉, 강주현, “정책과정의 시차문제에 관한 연구 : 서울시 대중교통정책 개편 사례”, *지방정부연구*, 제12권, 제1호, 2008, 7-29.
김소라, 이기춘, “온라인상에서의 개인정보유출피해에 대한 위험지각과 개인정보보호수준에 따른 소비자 유형화 및 유형별 관련요인 고찰”, *소비자정책교육연구*, 제2권, 제2호, 2006, 45-64.
김신석, 유혜정, “중소기업의 개인정보 기술적 보호조치 방안 연구”, *한국정보기술학회논문지*, 제18권, 제1호, 2020, 157-169.
김정규, 이경호, “FAIR를 통한 개인정보 유출에 따른 기업의 손해금액 산출에 대한 연구”, *정보보호학회논문지*, 제27권, 제1호, 2017, 129-145.
김준영, 김태성, “정보유출의도에 대한 영향요인 : 일반 억제 이론 및 합리적 선택 이론을 기반으로”, *정보보호학회논문지*, 제27권 제6호, 2017, 1507-1517.
김태성, “정보시스템 통제 및 감사 : 정보보안관리”, 서울, 淸文閣, 2002.
류승훈, “개인정보 유출에 따른 손해배상청구와 관련하여”, *법학연구*, 제47집, 2016, 125-146.
박수황, 장경배, “개인정보 유출 사례 분석 및 시사점 : 판례를 중심으로”, *보안공학연구논문지*, 제13권, 제3호, 2016, 249-283.
박준경, 김범수, 조성우, “기업정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인”, *경영학연구*, 제40권, 제4호, 2011, 955-985.
법제처, 개인정보 보호법, 2017. 10. 19. 시행.
법제처, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 2019. 6. 25. 시행.
신일순, 장원창, 박희영, “정보보호 투자와 침해사고의 인과관계에 대한 실증분석”, *정보보호학회논문지*, 제23권, 제6호, 2013, 1207-1217.
엄정호, 박선호, 정태명, “내부자의 불법적 정보 유출 차단을 위한 접근통제 모델 설계”, *정보보호학회논문지*, 제20권, 제5호, 2010, 59-67.
유비용, 권헌영, “제3자의 행위에 의한 개인정보침해사고로 발생한 손해배상책임의 합리적 배분”, *정보보호학회논문지*, 제30권, 제2호, 2020, 231-242.
유승동, 유진호, “개인정보 보호를 위한 지불의사비용 결정요인”, *정보보호학회논문지*, 제24권, 제4호, 2014, 695-703.
유진호, 지상호, 임종인, “개인정보 유 · 노출 사고로 인한 기업의 손실비용 추정”, *정보보호학회논문지*, 제19권, 제4호, 2009, 63-75.
윤승욱, 박원준, 김인경, “휴대전화 이용자와 인터넷 이용자의 개인정보 유출에 따른 위험성 인지에 관한 연구 : 지각 불안, 지각 피해, 개인정보 유출의 가능성, 대처방안 인지 정도를 중심으로”, *커뮤니케이션학 연구*, 제16권, 제3호, 2008, 105-130.
이동희, 김태성, 전효정, “패스워드 보안행위의도에 영향을 미치는 요인”, *정보보호학회논문지*, 제28권, 제1호, 2018, 187-198.
이재광, 장종수, 박기식, “사이버공간에서의 개인정보보호”, *정보사회와 미디어*, 제12권, 2007, 51-62.
이한솔, 채상미, “정보보안 투자가 침해사고에 미치는 영향에 대한 실증분석 : 정보보안 교육 서비스 투자를 중심으로”, *정보보호학회논문지*, 제28권, 제1호, 2018, 269-281.
정기석, “금융사 개인정보 유출 방지 방안에 관한 연구”, *융합보안논문지*, 제14권, 제4호, 2014, 109-116.
정명수, 이경호, “DEA 모형을 이용한 개인정보보호 관리수준 평가방법에 대한 연구”, *정보보호학회논문지*, 제25권, 제3호, 2015, 691-701.

정익재, 정창무, “재난의 유형과 재난관리 : 신문사설 내용 분석”, *한국행정학보*, 제30권, 제1호, 1996, 93-112.

조동원, “개인정보 해킹・유출의 정보문화”, *문화연구*, 제1권, 2012, 84-116.

조성규, 전문석, “개인정보보호를 위한 개인정보 유출 모니터링 시스템의 설계”, *정보보호학회논문지*, 제22권, 제1호, 2012, 99-106.

채승완, “개인정보보호의 경제적 효과”, *소비자문제연구*, 제33호, 2008, 43-64.

천명호, 최종석, 신용태, “SNS에서 개인정보유출방지를 위한 개인정보 유출위험도 측정 방법”, *정보보호학회논문지*, 제23권, 제6호, 2013, 1199-1206.

한국인터넷진흥원, “2018 정보보호 실태조사”, 2019.

한창희, 채승완, 유병준, 안대환, 박채희, “기업의 개인정보 유출로 인한 경제적 피해규모 산출방법”, *한국전자거래학회지*, 제16권, 제4호, 2011, 17-31.

황윤희, 유진호, “개인정보유출 사고의 분포 추정에 관한 연구”, *정보보호학회논문지*, 제26권, 제3호, 2016, 799-808.

Acquisti, A., “Nudging privacy : The behavioral economics of personal information”, *IEEE Security and Privacy*, Vol.7, No.6, 2009, 82-85.

Angst, C.M., E.S. Block, J. D’arcy, and K. Kelley, “When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches”, *MIS Quarterly*, Vol.41, No.3, 2017, 893-916.

Goode, S., H. Hoehle, V. Venkatesh, and S.A. Brown, “User compensation as a data breach recovery action : An investigation of the Sony Playstation network breach”, *MIS Quarterly*, Vol.41, No.3, 2017, 703-727.

Karger, P.A., “Privacy and security threat analysis of the federal employee personal identity verification(PIV) program”, *In Proceedings of the Second Symposium on Usable Privacy and Security*, 2006, 114-121.

Kong, H.K., T.S. Kim, and J.D. Kim, “An analysis on effects of information security investments : a BSC perspective”, *Journal of Intelligent Manufacturing*, Vol.23, No.4, 2012, 941-953.

Ransbotham, S., S. Mitra, and J. Ramsey, “Are markets for vulnerabilities effective?”, *MIS Quarterly*, Vol.36, No.1, 2012, 43-64.

About the Authors

김 택 영 (ecac987@naver.com)

충북대학교 경영정보학과에서 학사, 정보보호경영학과에서 석사 학위를 취득하였다. 현재 충북대학교 경영정보학과에서 박사 과정에 재학 중이다. 주요 관심분야는 개인정보보호, 기업 정보보호, 정보보호 정책이다.

김 태 성 (kimts@cbnu.ac.kr)

KAIST 산업경영학과에서 박사를 취득하고, 한국전자통신연구원에서 선임연구원으로 근무한 후, 현재 충북대학교 경영정보학과에서 정교수, 보안경제연구소장, 보안컨설팅연계전공 및 대학원 융합보안전공 주임교수로 재직하고 있다. 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, 한국전력 정보보안 자문위원, ISMS/PIMS 인증위원회 위원으로 활동하고 있으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다

전 효 정 (phdhyo@naver.com)

충북대학교 경영정보학과에서 학사, 석사, 박사 학위를 취득하였다. 석사학위 후 한국전자통신연구원 사업기획팀에서 근무하였으며, 박사 학위 후 현재 충북대학교 경영정보학과 글로컬 보안컨설팅 전문인력 양성사업단 박사후연구원으로 근무하고 있다. 주요 관심분야는 정보보호 인력 및 정책이다.