연구논문 정보화정책 제19권 제4호, 2012년 겨울호, pp.63~82

빅 데이터 시대 위험기반의 정책*
– 개인정보침해 사례를 중심으로 –

문 혜 정**, 조 현 석***

요 약 우리나라의 정보인프라는 세계 최고 수준이다. 그러나 심각한 보안 사고의 위험 또한 동반하고 있다. 최근 일어난 주요 사고만 정리해도 유출된 개인정보는 우리나라 인터넷 사용인구의 세 배를 넘는다. 이제 개인정보 침해 등의 정보보안의 사고는 국가의 일급재난에 해당하는 정책문제가 되었다. 이 논문은 빅 데이터 시대의 정보보안을 위한 정책적 논의를 사회과학 차원에서 탐구하였다. 이를 위해 최근 사고가 급증한 개인정보침해 사례를 위험기반으로 분석하였다. 사례분석결과는 다음과 같다. 첫째, 발생가능성과 영향에 따라 정보통신기술의 위험의 상황은 '심각, 강력, 집중, 기본'으로 구분되었다. 둘째, 위험의 상황에 따라 해당집단은 '계층주의, 평등주의, 운명주의, 개인주의' 문화유형을 지니며 '회피, 전가, 완화, 수용'의 대응정책을 적용하였다. 셋째, 위험상황에 따라 정보통신기술은 '대용량, 고성능, 다양성'의 빅 데이터의 특성을 보였다. 이 연구의 시사점은 다음과 같다. 첫째, 위험상황별 문화유형과 빅 데이터의 특성을 이해하여 포괄적인 정책을 수립하고 적용할 수 있는 정부의 전담조직이 필요하다. 둘째, 빅 데이터 시대 정보통신기술에 대한 위험관리는 '기술, 규범, 법, 시장' 측면의 균형 있는 정책의 적용이 필요하다.

주제어: 빅데이터, 개인정보침해, 기술위험, 문화유형, 정보통신기술정책

Risk based policy at big data era: Case study of privacy invasion

Hyejung Moon, Hyun Suk Cho

Abstract The world's best level of ICT(Information, Communication and Technology) infrastructure has experienced the world's worst level of ICT accident in Korea. The number of major accidents of privacy invasion has been three times larger than the total number of Internet user of Korea. The cause of the severe accident was due to big data environment. As a result, big data environment has become an important policy agenda. This paper has conducted analyzing the accident case of data spill to study policy issues for ICT security from a social science perspective focusing on risk. The results from case analysis are as follows. First, ICT risk can be categorized 'severe, strong, intensive and individual' from the level of both probability and impact. Second, strategy of risk management can be designated 'avoid, transfer, mitigate, accept' by understanding their own culture type of relative group such as 'hierarchy, egalitarianism, fatalism and individualism'. Third, personal data has contained characteristics of big data such like 'volume, velocity, variety' for each risk situation. Therefore, government needs to establish a standing organization responsible for ICT risk policy and management in a new big data era. And the policy for ICT risk management needs to balance in considering 'technology, norms, laws, and market' in big data era.

Keywords: big data, privacy invasion, technological risk, cultural types, ICT policy

2012년 11월 1일 접수, 2012년 11월 2일 심사, 2012년 12월 26일 게재확정

* 이 논문은 2011년도 정부재원(교육과학기술부 사회과학연구지원 사업비)으로 한국연구재단의 지원을 받아 연구되었음(NRF-2011-330-B00034)

** 서울과학기술대학교 IT정책전문대학원 박사 수료(hyejung.moon@gmail.com)
*** 교신저자, 서울과학기술대학교 교수(hyunsuk@snut.ac.kr)

Ⅰ. 서 론

정보화로 인한 사생활 침해, 불건전 정보 유통, 시스템 파괴, 데이터 해킹 및 훼손 등 정보사회의 부작용과 문제점은 날로 증가하고 있다(Beck, 1998). 세계 최고 수준의 우리나라 정보인프라에서 발생한 보안 사고의 피해는 매우 심각하다. '2008년 2월 옥션 1800만명, 2011년 4월 현대캐피탈 43만명, 2011년 8월 SK컴즈3500만명, 2011년 11월 넥슨코리아 1300만명, 2012년 5월 EBS 400만명, 2012년 7월 KT 800만명' 등 주요 개인정보유출 사고만 정리해도 유출된 개인정보는 우리나라 인터넷 사용인구의 3배가 넘는다(서울경제, 12/07/30). 이미 전 국민의 개인정보가 유출되어 중국, 필리핀 등에 팔려나가 남용되고 있는 것이다. 누출된 개인정보는 주민등록번호, 신용카드번호, 주소, 전화번호 등 민감한 개인정보를 포함하고 있다. 이제 개인정보침해를 비롯한 정보화의 위험은 국가의 일급재난에 해당하는 피할 수 없는 중요한 정책문제가 되었다.

이러한 사회문제는 우리나라 정보인프라의 발전과 인터넷 사용자의 증가로 인해 야기되는 빅 데이터 현상으로 인해 더욱 심각해지고 있다. 대용량, 고성능, 다양성의 특성을 가진 빅 데이터가 지니고 있는 정보의 중요성과 여기서 파생되는 새로운 가치 발굴 기회도 많으나 내포한 위험 또한 간과할 수 없다. 그렇다면 빅 데이터 시대 정보보안을 위한 정책적 논의는 어떻게 마련되어야 할 것인가? 이 논문은 이러한 기본적인 의문에서 출발한다. 최근 정보보안 침해는 기계적 오류나 기술적 취약점뿐만 아니라 사용자의 심리와 조직의 관리 취약성을 이용하고 있다(Gonzalez, et al., 2002). 정보보안의 문제는 기술의 문제인 동시에 사람과 조직을 포함하는 사회문제인 것이다. 이 연구는 정보보안 문제를 정보사회의 위험이라는 시각으로 접근하고, 이를 관리하기 위한 정책적 논의를 문화적 특성에 기본을 두고 어떻게 대응 정책을 수립해야 할지 연구하겠다(Douglas, et al., 1982).

정보보안을 위험관리 차원에서 접근하는 것은 여러 가지 정책적 함의를 전달한다. 무엇보다 정보보안의 문제가 기계적 오류나 시스템 파괴로 인식하는 수준을 넘어서 사회적 경제적 문제로 조명할 수 있는 단초를 제공한다. 즉, 정보보호를 위한 기술적 대응 조치는 물론이고 보안문제에 따른 비용과 손실을 관리하기 위한 개인 · 조직 · 정부의 역할과 의무에 대한 재고가 필요하다(소영진 외, 2001). 위험은 불확실성을 전제로 한다는 점에서 정보보안 문제발생은 불가피하며, 정보통신기술의 발달과 이를 활용하는 데 자연스럽게 수반된다. 결국 모든 위험으로 자유로울 수 없다는 현실을 인정한다면, 어느 정도의 위험을 수용하고 회피할 것인가를 판단해야하는 것이 정보보안 문제를 다루는 현실적인 접근이다(정익재, 2007). 이 논문은 최근 빅 데이터 현상으로 인해 피해사례가 급증한 개인정보침해사고를 사례로 분석하여 정보통신기술로부터 발생하는 위험에 대한 대응 정책의 수립에 대한 구체적인 방향을 제시하고자 한다.

Ⅱ. 이론적 배경 및 선행연구 검토

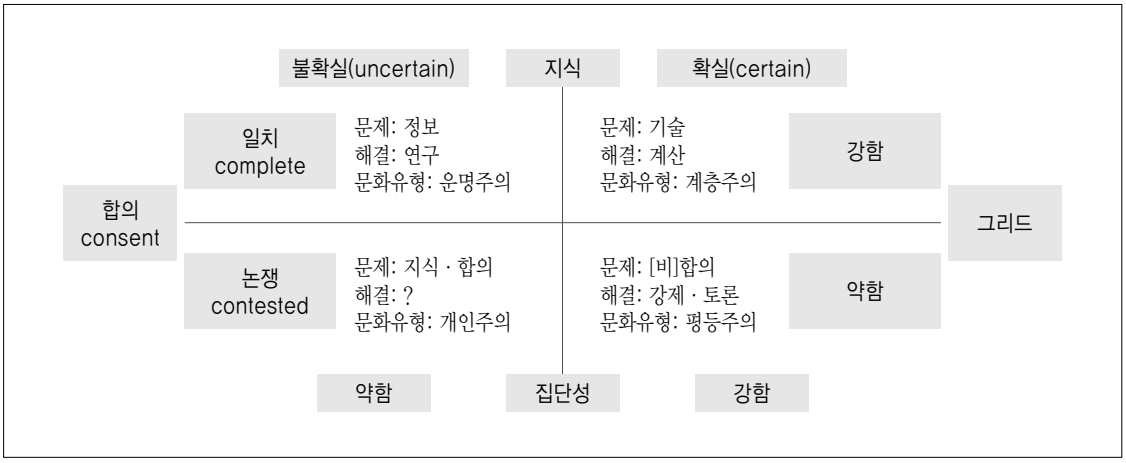
1. 위험기반의 정책대응 이론

연구의 배경은 Douglas, et al.(1982)의 위험기반의 문화유형, Wildavsky(1988)의 위험별 대응정책, Project Management Institute(2008, 이하 PMI)의 프로젝트 위험관리전략, May(1991)의 정책유형, 빅 데이터의 조작적 정의를 기초로 한다. 먼저 Douglas, et al.(1982)가 제시한 위험의 지식과 합의 정도에 따른 해결방안은 〈그림 1〉과 같다.

위험을 내포한 사회문제가 무엇이고 그 문제가 발행할 가능성은 얼마나 되며 위험을 해결하고 예방하는 비용은 얼마나 되는지 등에 대한 지식이 많으면 확실한 위험이고, 위험에 대한 지식이 적으면 불확실한 위험으로 구분하였다. 위험에 대한 합의의 정도는 내포한 사회문제를 밝히고 그것을 해결하기 위한 정

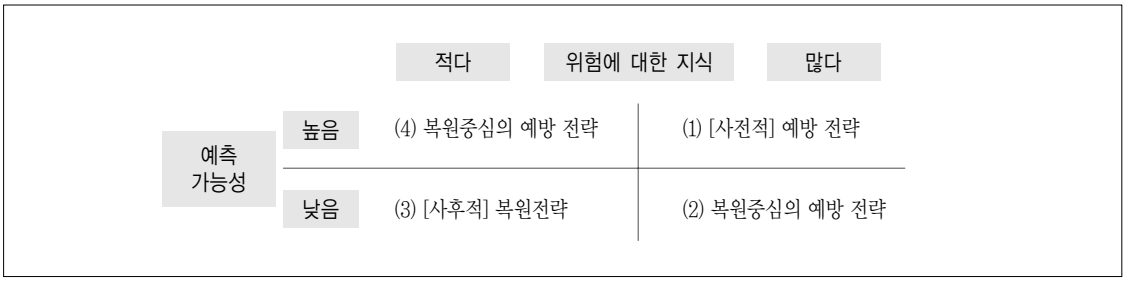
책을 결정하는 이해당사자간의 합의를 기준으로 구분하였다. 관련지식이 확실하고 합의가 이루어진 위험은 기술부문이며 정확한 계산에 의해 해결된다. 관련지식이 불확실하여도 문제에 대한 합의가 일치한 위험은 정보 부분이며 적극적인 연구를 통해 정보위험의 문제를 해결한다. 관련지식이 확실하나 논쟁 중인 위험은 합의의 문제이며 강제하거나 토론으로 해결한다. 관련지식도 불확실하고 논쟁적인 위험은 지식과 합의의 문제이며 적합한 해결책은 없다. Douglas, et al.(1982)는 위험의 특성을 이해하여 문화적으로 해결해야 한다고 제시하였다. 위험의 해결전략은 문화적 성향에 따라 시장기반의 개인주의와 관료기반의 계층주의로 해결하여야 한다고 제안하였다. 문화적 성향은 Douglas(1970)가 집단성과 그리드의 강약에 따라 '계층주의(Hierarchy), 운명주의(Fatalism), 평등주의(Egualitarianism), 개인주의(Individualism)' 네 가지로 구분하였다. 집단성의 강약은 소속감, 유대, 교류 등의 정도에 따라 구분하며 그리드의 강약은 계급, 종교, 나이, 성별 등에 대한 구속의 정도이다.

불확실성을 본질로 하는 위험에 대한 대응전략의 선택기준으로서 지식과 예측가능성 두 가지 요인을 고려하여 어떤 위험대응전략을 선택할 것인가를 논하면 〈그림 2〉와 같다(Wildavsky, 1988).



출처: Douglas(1970), Douglas & Wildavsky(1982) 재구성

〈그림 1〉 위험상황별 문화유형



출처: Wildavsky(1988)

〈그림 2〉 위험상황별 복원전략

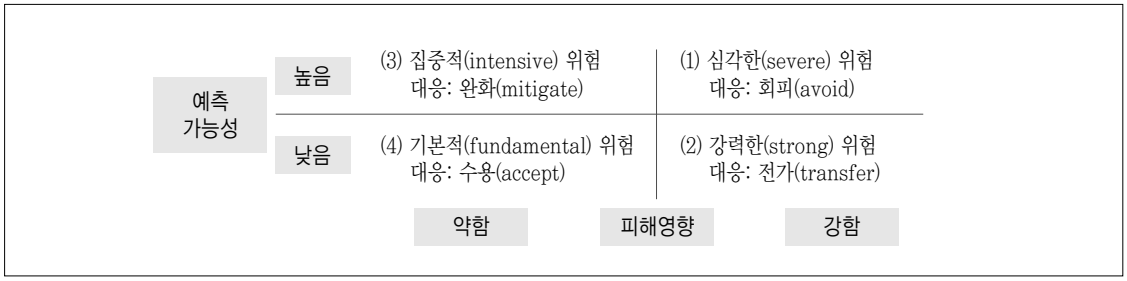
위험상황(1)은 특정 위험의 대응에 대한 지식이 충분하게 확보되어 있고, 구체적으로 어떤 위험이 발생할지 예측이 비교적 정확한 경우로 예방 전략이 월등한 전략이다. 위험상황(2)는 위험 대응방법에 대한 지식은 충분하지만 발생에 대한 예측이 용이하지 않은 경우를 나타내고 있다. 위험대응에 요구되는 지식이 많아 통제가능성이 높고 그만큼 복원중심의 예방 전략에 관심이 모아진다. 위험상황(3)은 위험에 처하여 무엇을 해야 할지 잘 모르고, 어떤 위험이 발생할지 예측도 불가능한 경우로 복원전략을 적용한다. 어떤 위험이 발생할 것인지에 대해 예측할 수 있지만 이에 대응하기 위한 지식, 즉 통제가능성이 낮은 위험상황(4)의 경우 역시 예방 전략을 선호한다. 하지만 대응방안에 대해서 충분한 지식이 없다는 점에서 복원전략에 근거한 예방 전략에 의존하는 것이 바람직하다.

PMI(2008)는 프로젝트에서 발생 가능한 위험을 빈도와 영향으로 측정, 네 가지로 구분하여 〈그림 3〉과 같이 대응 전략을 제안한다.

가능성이 높고 영향력이 강한 위험상황(1)은 이에 대한 피해가 크기 때문에 위험이 발생하지 않도록 정기적인 점검을 통해 사전에 위험을 예방하는 회피전략으로 대응한다. 가능성은 낮아도 한번 발생하면 피해가 큰 위험상황(2)은 사건발생 후에 수습하는 전가전략으로 대응하며 평소 업무기반의 검토를 통해 점검한다. 가능성은 높으나 영향력이 낮은 위험상황(3)은 위험으로 인한 피해는 약하나 발생가능성이 높기 때문에 기술기반의 점검을 통해 위험을 최소화하도록 복구중심의 완화전략으로 대응한다. 위험의 가능성도 낮고 피해의 영향도 약한 위험상황(4)는 개인적인 차원에서도 수습이 가능하기 때문에 위험이 발생하도록 방치하였다가 상황에 따라 비공식적으로 대응하는 수용전략으로 대응한다.

May(1991)는 정책설계를 사회문제가 지니는 위험의 성격에 따라 구분하였다. 국가의 정책 대응이 되는 사회문제는 공적위험과 사적위험의 성격을 지닌다. 공적위험은 기술함정, 혁신정책, 예산수립 등 대중의 관심이 적은 일반적인 사회문제이다. 공적 위험은 두 가지이다. 첫째, 발생빈도가 낮고 피해의 영향이 강한 자연재해, 오존파괴 등 위험이다. 둘째, 발생빈도가 높고 영향이 약한 가정용 라돈이나 식품오염 등의 위험이다. 공적위험은 정부가 주도하여 정책을 설계하는 경향을 띤다. 사적위험은 노사, 보건, 중독, 실업, 범죄, 마약 등 대중의 관심도가 높은 사회문제가 지니는 위험이다. 사적위험은 대중의 관여도가 높기 때문에 대중이 참여하여 정책을 설계하는 경향을 띤다. 위험의 발생빈도와 영향이 큰 사회문제는 국가가 적극적으로 대응해야 할 국방, 의료 등의 중요한 사회문제이다.

빅 데이터는 대용량, 고성능, 다양성의 특성을 지니며(Douglas, 2001), 현재의 기술로는 저장 · 관리 · 분석이 불가능한 규모의 데이터이다(Manyika,



출처: PMI(2008) 재구성

〈그림 3〉 위험상황별 대응전략

et al., 2011).[1] 이로 인해 빅 데이터의 활용은 개인정보의 유출위험으로 확산되고 있는 실정이다(디지털타임즈, 12/10/19). 빅 데이터를 활용하기 위해서는 초고속의 수집 · 발굴 · 분석이 가능한 차세대 기술 및 구조가 필요하다(Gantz, et al., 2011). 빅 데이터의 기술 및 구조 개발을 위해서는 빅 데이터의 특성과 위험에 대한 이해가 선행되어야 한다. 대용량의 의미는 빅 데이터를 발생시키는 사용자를 많이 보유한 SNS나 포털 등의 운명주의 문화유형에서 주로 나타난다. 고성능의 특성은 빅 데이터를 관리하는 성능이 빠르고 목적성을 가진 영리기업의 시스템에서 나타나며 평등주의 문화유형에서 주로 나타난다. 다양성의 특성은 빅 데이터로 만들어지는 결과물이 파일, 동영상, 이미지 등 여러 가지 형식을 보이고, 그 내용도 정규화되지 않는데 이러한 특성은 개인주의에서 나타난다. 이러한 빅 데이터의 기본적인 특성에서 발생하는 위험을 사용자로부터 비롯된 문화적 측면, 시스템이 갖는 위험적인 측면에서 재조명하여 이 연구의 분석틀에 적용한다.

2. 선행연구

위험을 정량적으로 분석한 초기 연구는 Crouch, et al.(1983)의 연구이다. 위험을 내포한 사건 또는 사고가 발생할 확률과 그것에 의해서 나타나는 결과의 강도와 영향력을 비용과 효용의 경제적인 함수관계로 설명하였다. 사회문제가 가지는 위험의 부정적인 문제와, 위험을 감수함으로 인해 얻는 효용가치의 상호 관계를 분석하여 대응 전략을 어떻게 수립해야 할지 제안하였으나 위험을 직접적으로 측정하지 않고 대안에 소요되는 비용으로 측정하는 데 그쳤다.

위험의 문제를 정책적 입장에서 연구한 대표적인 선행연구는 Slovic(1987)의 연구이다. 국가의 각종 정책 중 위험성을 지니는 활동과 그 활동에 필요한 기술에 내포된 문제에 대한 위험인식에 대한 연구이다. 여성유권자, 대학생, 정당회원(남성유권자), 기술전문가 간 위험관련 정보의 소통이 증가하고 그 함정에 대한 대중의 응답을 이해하여 정책결정의 기초를 마련하였다. 국가의 위험한 활동과 기술이 지닌 문제를 선정하여 심각성과 불확실성의 측면으로 구분하여 정책적 대응의 차이를 설명하였다.[2] 연구결과 대부분의 국가 위험은 기술에서 기인하는 것을 확인하였으나 설문조사 방식으로 위험을 진단한 것이 이 연구의 한계이다.

Deloach(2000)는 특정업무의 흐름에서 발생 가능한 위험을 발굴하여 분석하였다. 위험의 발생가능성과 영향으로 측정하여 위험을 정량화하여 기업의 통합적인 정보시스템 업무에 적용하였다. Slovic(1987)이 정성적, 설문적 조사를 통해 위험의 심각성과 불확실성으로 구분한 반면 Deloach(2000)는 위험을 경제적인 가치로 정량화하였다. 위험의 발굴과 정량화, 대응방안을 관리할 수 있는 조직과 체계를 함께 제안하였으나 설문조사에 의해 위험을 측정하였다는 단점이 있다.

Norrman, et al.(2004)은 특정업무의 흐름에서 발생 가능한 위험을 발굴하여 분석하였다. 위험의 발생가능성과 영향을 측정, 정량화하여 공급망 관리업무에 적용하였다. Slovic(1987)이 제안한 위험의 불확실한 위험을 위험의 발생가능성으로 인식하고, 심각한 위험을 위험의 영향으로 이해하여 우선순위를 적용하였다. Norrman, et al.(2004)은 위험을 업무별로 예상하고 관련 사고가 발생하였을 때 정상업무를 복구하기까지 필요한 시간을 위험의 영향으로 측정하였다. 위험의 피해 영향을 측정하는 데 있어

1) 빅 데이터 시대 정보화의 위험에 대한 대응정책을 논의하기위해서는 빅 데이터의 정의와 특성의 파악이 선행되어야 한다. 현재 학술적인 빅 데이터의 이론적인 연구는 미흡한 형편이며, 몇몇 선두 정보시스템 업체나 컨설팅 업체가 논의한 바는 기술적 특징에 불과하다.

2) Slovic(1987)은 대표적인 사회문제에 대해 대표적인 사회집단에 따라 내포한 위험을 정량화 하였다. 선별된 사회문제는 핵발전, 자동차, 권총, 흡연, 알콜중독, 경찰업무, 살충제, 외과수술, 화재, 대형건설, 산악등반, 전력문제, 피임, 식품방부제, 예방접종 등 31가지이다.

비용이 아니라 시간으로 측정하였다는 점에서 정량화의 한계가 있다.

국내 정보위험에 대한 정책적 대응을 논의한 연구는 정익재(2007)의 보안사고사례에 대한 분석이 있다. 정익재(2007)는 미국 연방정부의 보안사고의 위험을 정량화하여 구분하고 그에 따른 정책설계의 차이를 제언하였다. 정보위험에 대한 정책적 대응을 가장 위험의 발생빈도가 높고 위험으로 인한 영향력이 강한 위험상황 정보보안 문제를 정보사회의 위험이라는 시각을 통해서 접근하고, 이를 관리하기 위해 정책적으로 연구하였다. 1998년부터 2000년까지 미국의 연방정부기관에서 발생한 보안사고 가운데 연방정부 보안사고 대응기관 FedCIRC[3]에 보고된 총 1,306건의 사례를 위험기반으로 정량화하여 정책적 대응의 차이를 설명하였다. 그러나 미국의 사례를 기반으로 하였기 때문에 우리나라 실정에 직접적으로 적용하기에는 한계가 있다.

May, et al.(2009a; 2009b)은 정책결정에 미치는 영향을 경험적인 측면에서 분석하였다. 25년간 미국에서 일어난 공공위험의 문제가 된 테러 등의 사고에 대해 정책이 설계된 과정을 정량적으로 분석하였다. 위험의 성격에 따라 대중의 관심도는 어떠하였고, 국토안보부 등의 주요 집단이 정책을 주도하였는지 분석하였다. 발생빈도가 높고 피해가 적은 사적위험을 내포한 사회문제는 대중이 참여하여 정책을 설계하는 경향을 보였다. 발생빈도가 낮고 피해발생 시 영향이 큰 공적위험은 대중의 관심도가 낮아 정부가 주도하여 정책을 설계하는 경향을 보였다. 미국의 의제설정과정에서 위험을 대상으로 한 정책설계의 특징을 연구한 것으로써 위험을 정량적으로 측정하는 데 미흡하였다.

한창희(2011)는 개인정보 유출의 피해를 국가 입장에서 경제적으로 피해규모를 계량화하였다. 일본 네트워크 보안협회 등 해외 유수 연구들의 방법론과 새로운 접근법들을 참고하였다(Ponemon, 2010). 개인정보 유출사고의 피해실태를 파악하기 위한 정보의 수집과 이의 정량적 분석의 개념적 틀을 제시하였다. 정보보안 사고에 대한 피해의 규모를 정책적 지표로서 의미 있는 피해액을 측정하여 개인정보 유출 피해를 막기 위한 다양한 정책기획의 기반자료를 제시하였다. 사고에 대한 피해를 정책적 지표로 측정하는 방법론을 제시하였으나 위험의 발생 가능성을 배제하여 위험의 특성을 구분하는 데 미흡하였다.

선행연구에 비해 이 연구가 가지는 차별성은 다음과 같다. 첫째, 정보보안의 위험 중 국내의 피해 사례가 가장 심각한 개인정보침해사례를 기반으로 실증적인 사례 연구를 수행하겠다. 둘째, 지난 10년간의 정보보호 위험에 대한 사고 사례를 기반으로 위험의 사고건수를 측정하여 발생가능성에 적용하겠다. 셋째, 실제로 발생할지 모르는 위험에 대한 영향을 법률에 근거하여 비용을 사전에 계산하겠다. 넷째, 정보위험의 대상이 되는 집단의 문화적 유형과 빅 데이터의 특성에 따라 달라지는 대응 정책을 분석하겠다. 다섯째, 동일한 유형의 사고가 발생한 사례 및 이에 대한 법적 조치를 확인하여 사례분석의 결과와 대조하여 연구결과를 진단하겠다.

Ⅲ. 연구의 설계 및 분석틀

1. 연구의 설계

연구질문은 정보통신기술의 위험상황에 따라 달라지는 '문화유형, 대응전략, 빅 데이터의 특징' 세 가지의 특성이 어떻게 달라지고 이에 대한 대응정책의 수립은 어떠한 차이가 있는지에 초점을 둔다. 위험의 발생가능성과 영향에 따라 대응방안수립에 어떠한 영향을 미쳤는지 정책적으로 분석할 것이다. 위험의 내용이나 결과보다는 대응전략이 형성되는 과정을

3) The Federal Incident Response Capability

위주로 다음과 같은 연구질문을 토대로 사례분석을 수행하겠다.

연구질문 1. 발생가능성과 영향에 따라 정보위험은 어떠한 특성을 보이는가?

1.1 발생가능성에 상호 영향을 주는 위험은 어떠한 것이 있는가?

1.2 위험의 영향 평가에서 법규제는 어떠한 역할을 하는가?

연구질문 2. 위험상황에 따라 해결전략은 어떻게 달라지는가?

2.1 위험상황에 따라 관련 집단은 어떠한 문화유형을 보이는가?

2.2 위험상황에 따라 대응전략은 정책적으로 어떠한 차이를 보이는가?

연구질문 3. 위험상황에 따라 정보기술은 어떠한 차이를 가지는가?

3.1 위험상황에 따라 정보위험이 가지는 데이터는 어떠한 특징을 보이는가?

3.2 위험상황에 따라 빅 데이터 환경과 기술의 영향은 어떠한 차이를 보이는가?

연구대상은 지난 10년간 발생한 개인정보침해 사례이다. 정보보호의 실태에 대한 자료는 한국인터넷진흥원(이하 KISA)이 제공하는 통계자료를 기초로 한다. KISA는 '개인정보보호실태, 기업정보보호실태, 스팸의 수신량, 해킹/바이러스, 개인정보침해' 분야의 정보보호 통계를 관리하고 있다. 개인의 정보보호 실태는 2006년 이후 설문조사 수준으로 정보보호에 대한 개인적인 의식을 조사하여 제공되고 있다. 기업의 정보보호 실태는 개인정보보호와 마찬가지로 설문조사에 의한 기업의 정보 보호에 대한 의식조사의 결과로 2007년 이후부터 제공되고 있다. 스팸의 수신량은 2003년 이후부터 민원신고에 의한 통계자료를 관리하고 있으나 2003년 1인당 매일 받는 스팸의 수신량이 평균 30건이었던 반면 최근 2012년 1건 수준으로 그 피해는 감소하고 있다. 2003년부터 관리해온 해킹 사고는 2005년 최대 3만 3천건 수준으로 증가했다가 최근 2012년에는 1만 8천건으로 감소하여 상대적으로 피해가 줄어들고 있는 형편이다. 바이러스 사고는 2003년 이후 2004년에 10만 7천건까지 증가했다가 이후 정부의 강력한 바이러스 소프트웨어 보급으로 인해 2005년부터는 이전의 20% 수준으로 감소하였다. 반면 개인정보침해 사고는 2003년 1만 7천건에서 최근 2012년에는 15만 5천건으로 증가하여 그 피해가 급속히 증가하고 있는 실정이다. 이 논문에서는 그 피해가 가장 큰 개인정보침해 사례를 대상으로 사고가 지닌 위험을 정량화하여 정책적인 대응을 논의하겠다.

연구방법은 특정사례를 선정하여 서로 특성이 다른 사례를 구조적으로 분리하고 분리된 각 사례를 서로 비교하는 방식의 기술적인 사례분석이다(George, et al., 2005). 전체 사례는 개인정보침해에 대한 정보보호위험의 문제를 대상으로 한다. 연구의 대상이 되는 사례를 특성에 따라 구분하고 그 특성에 따라 일관된 기준으로 각 사례를 비교한다. 개인정보침해 사고는 KISA에서 사고신고로 분리하는 15가지 체계로 나누어 분석한다. 각 사고에 대한 위험의 정량화는 발생가능성과 영향으로 나눈다. 개인정보침해 사고에 해당하는 위험의 발생가능성은 과거 10년간의 신고사례건수로 정량화하여 향후 발생가능성에 적용한다. 개인정보침해 사고로부터 발생하는 위험의 영향은 사고가 실제로 발생하기 전에는 측정하기 불가능하다. 따라서 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 법)에서 정한 형량과 벌금에 근거하여 위험이 발생할 경우 피해로 발생하는 영향의 최소치로 계산한다. 이렇게 구분된 사례는 분석틀이 제시하는 위험의 특성에 따라 '대상집단이 지니는 문화유형, 위험상황별 대응방안, 대상 시스템이 가지는 빅 데이터 특성' 세 요소별로 사례

를 분석하여 정보화가 지니는 위험에 대한 대응 정책의 수립방안을 논의하겠다.

2. 분석틀

정책의 대상이 되는 사회문제는 정치적 상황의 영향을 받는다(Cobb, et al., 1976). 특히 언론의 집중보도를 받는 천재지변 등의 사회문제는 내포한 위험의 특성에 따라 정책설계가 달라진다(Cobb, et al., 1983). 위험은 주로 기술적 문제에서 발생하고 위험을 내포한 집단의 문화적 차이에 따라 해결방안을 정책적으로 접근하여야 한다(Douglas, et al., 1982). 위험은 발생가능성과 발생 시 피해의 영향으로 정량화하여 구분한다(Slovic, 1987). 위험이 지니는 발생가능성과 영향의 특성에 따라 위험에 대한 대응 전략은 달라진다(PMI, 2008). 또한, 위험을 해결하기 위한 정책은 위험과 관련된 집단의 특성에 따라 정책설계가 달라진다(May, 1991). 정책은 위험을 대응하는 비용을 최소화하는 방향으로 설계된다(한창희, 2011). 이 논문의 분석틀은 위험의 가능성과 영향에 따라 사회문제를 구분하고 이에 따라 달라지는 '대상 집단의 문화유형, 위험의 대응정책, 정보통신기술의 빅 데이터 특징' 세 가지 분석요소에 따라 정책설계가 어떻게 차이를 두고 달라지는지 〈그림 4〉와 같이 분석하겠다.

위험의 상황을 구분하는 기준은 발생가능성과 영향이다. 첫째, 발생가능성은 위험의 '그리드, 빈도, 합의'의 특성을 포함한다. 위험 집단의 그리드수준은 종교, 성별, 나이 등 위험의 대상이 되는 구성원이 벗어나기 어려운 구속이나 제약의 수준을 나타낸다(Douglas, et al., 1982). 위험의 발생빈도는 위험과 관련된 사건의 발생빈도와 그 가능성 대한 지표

분석요소: 1. 문화유형, 2.대응정책, 3. 빅 데이터 특징

출처: Douglas, et al.(1982), Wildavsky(1988), May(1991), PMI(2008) 재구성

〈그림 4〉 분석틀: 정보통신기술의 위험상황별 정책설계

이다(Slovic, 1987). 위험에 대한 합의 정도는 집단의 의견 일치와, 합의 실패 후 논쟁적인 대립에 관한 문제이다(Wildavsky, 1988). 발생빈도가 크고, 합의정도가 일치하고 그리드의 구속이 강할수록 위험의 가능성은 높다고 본다. 둘째, 위험의 영향은 위험의 '집단성, 복구비용, 관련지식'을 포함한다. 집단성은 위험과 관련한 조직의 소속감, 유대감, 집단 내 교류의 수준을 의미한다(Douglas, et al., 1982). 위험의 복구비용은 위험과 관련한 사건이 일어났을 때 해당사건이 발생하기 이전으로 복구시키는 노력과 비용을 의미한다(Slovic, 1987; Deloach, 2000; Norrman, et al., 2004). 위험에 대한 관련지식은 위험을 예상, 점검하고 대응하기 위해 필요한 지식의 수준을 의미한다(Wildavsky, 1988). 복구비용이 높고, 관련지식이 많으며 집단성이 높을수록 위험의 영향은 강하다고 본다.

위험은 발생가능성과 영향에 따라 '심각한 위험, 강력한 위험, 집중적 위험, 기본적 위험' 네 가지로 구분된다(PMI, 2009). 각 위험은 '문화유형, 대응정책, 빅 데이터 특징'으로 그 차이를 알아볼 수 있다(Douglas, et al., 1982; PMI, 2009). 이 논문에서는 기존연구에서 제시된 '위험별 문화유형에 따른 대응전략의 차이'를 설명하고, 위험이 정보통신기술에서는 어떠한 특징을 가지는지 사례를 분석하여 빅 데이터 관점에서 설명하고자 한다.

첫째, 가능성이 높으며 영향력이 큰 '심각한 위험'이다. 심각한 위험에 관련된 구성원의 특성은 집단성이 높고 그리드의 구속이 강한 계층적 집단으로 국가가 대표적인 사례이다(Douglas, et al., 1982). 정해진 절차에 의해 위험을 정기적으로 철저히 검사하고, 사전에 발생을 회피할 수 있도록 예방 위주의 대응전략을 수립한다(PMI, 2009). 심각한 위험을 내포한 정보시스템은 '대용량, 고성능, 다양성' 빅 데이터 특성(분석틀에서는 vvv라 표기함)을 모두 지닌다.

둘째, 가능성은 낮으나 영향력이 큰 '강력한 위험'이다. 그리드의 구속력은 낮으나 조직의 집단성이 큰 평등주의의 문화유형을 지니며 특정한 목적을 위해 구성된 영리기업이나 전문가 집단 등이 사례이다(Douglas, et al., 1982; May, 1991). 업무와 조직을 위주로 위험을 사전에 식별하고 우선순위를 정하며, 위험 발생 시 보험이나 인증 등의 대안으로 전가하는 대응전략을 적용한다(PMI, 2009). 강력한 위험에 관련한 조직은 영리기업 등의 특정한 목적을 위해 구성된 조직으로서 고성능의 특성을 지닌 시스템을 이용하여 데이터를 생성 · 관리한다.

셋째, 발생가능성은 높으나 위험의 영향이 적은 '집중적 위험'이다. 관련 구성원은 그리드의 구속력은 높으나 조직의 집단성은 약한 운명주의 성격을 지니며 포털, 커뮤니티, 클럽모임 등이 그 사례이다(Douglas, et al., 1982; May, 1991). 집중적 위험은 위험이 발생하는 문제가 집중되어 있으므로 기술적 구현으로 사전에 점검하고, 위험을 사전에 진단하여 피해를 최소화하는 완화 전략을 적용한다(PMI, 2009). 집중적 위험에 관련된 포털 등의 집단은 광범위한 활용을 위해 대용량의 특성을 지닌다.

넷째, 발생가능성도 낮고 위험의 영향도 약한 개인들의 '기본적 위험'이다. 그리드의 구속력이 낮고 구성원의 집단성이 약한 개인주의의 성격을 지닌다(Douglas, et al., 1982). 기본적 위험은 심각하지는 않으나 문제가 다양하기 때문에 상황에 따라 비공식적으로 점검하고, 위험이 발생한 후 사후에 복구하는 수용의 대응전략을 적용한다(PMI, 2009). 기본적 위험이 지니는 정보는 개인의 취향과 목적에 따라 데이터의 형식이 다양하다.

위험의 영향과 발생빈도가 큰 사회문제는 공적위험의 성격을 지닌다. 공적위험은 정부가 주도하여 예방 위주의 대응정책으로 관리한다(Wildavsky, 1988). 공적위험은 자연재해, 기술함정, 예산수립, 혁신정책 등 광범위한 사회문제를 포함하고 있다(May, 1991). 위험의 영향과 빈도가 낮은 사회문제는 사적 위험의 성격을 지닌다. 사적 위험은 민간의

특정단체를 대상으로 하는 위험으로 사고 발생 후 복구하는 대응전략으로 관리한다(Wildavsky, 1988). 사적 위험은 범죄, 마약, 보건, 노사문제 등 특정한 조직과 관련된 사회문제이다(May, 1991).

Ⅳ. 사례분석

1. 사례개요

KISA는 법에 근거하여 개인정보침해의 신고유형을 15가지로 정의하여 이에 대한 상담현황을 관리하였다. 개인정보침해 신고유형별 근거법과 벌칙은 〈표 1〉과 같다.

개인정보침해사례는 매해 증가하여 지난 10년간 8배까지 증가하였다. 2003년부터 2010년까지 침해사례는 평균 10% 정도 증가한 반면, 최근 2011년에는 전년도에 비해 200% 이상 침해사례가 증가하는 현상을 보였다. 2012년 9월 현재 개인정보침해의 신고사례는 이미 작년치를 넘어서고 있다. 침해사례가 증가한 유형은 8가지(C01, C02, C03, C04, C05, C06, C10, C14)이다. 이 중 '주민등록번호 등 타인정보의 훼손 · 침해 · 도용'(C14)의 문제가 전체 침해의 50.92%를 차지할 만큼 피해가 심각하다. 2012년엔 '이용자의 동의 없는 개인정보 수집'(C01)는 전년도의 두 배, '개인정보 수집 시 고지 또는 명시 의무 불이행'(C02)은 전년도의 7배 이상 증가하고 있다. 침해사례가 감소한 유형은 등 7가지(C07, C08, C09,C11, C12, C13, C15)이다. '법정대리인의 동의 없는 아동의 개인정보 수집'(C13)은 정부가 인터넷 침해신고문제를 관리하기 시작한 2003년에 비해 40분의 1로 감소한 모범적인 사례이다. '동의철회 · 열람 또는 정정 요구 불응'(C11)의 문제는 2004년 한

〈표 1〉 개인정보침해의 신고유형 및 근거법조항[4]

유형	개인정보침해 내용	근거법조항	벌칙조항(벌금[5])
C01	이용자의 동의 없는 개인정보 수집	22조1항	64(1),71(5)
C02	개인정보 수집 시 고지 또는 명시 의무 불이행	22조2항	64(1),76(3)
C03	과도한 개인정보 수집	23조2항	71(5),76(3),76(1)
C04	고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공	24조2항	64(1),71(5),76(1)
C05	개인정보 취급자에 의한 훼손 · 침해 또는 누설	28조2항	64(1),71(5)
C06	개인정보 처리 위탁 시 고지의무 불이행	25조1항	64(1),71(5)
C07	영업의 양수 등의 통지의무 불이행	26조1항	76(2)
C08	개인정보관리책임자 미지정	27조1항	76(2)
C09	기술적 · 관리적 조치 미비로 인한 개인정보누출 등	28조1항	64(10),71(5),73(1),76(3)
C10	수집 · 제공받은 목적 달성 후 개인정보 미파기	29조	76(3)
C11	동의 · 철회 · 열람 · 정정의 요구 불응	30조1,2,5항	71(5)
C12	동의 · 철회 · 열람 · 정정을 수집보다 쉽게할 조치 미이행	30조6항	76(3)
C13	법정대리인의 동의 없는 아동의 개인정보 수집	31조1항	64(1),71(5)
C14	주민등록번호 등 타인 정보의 훼손 · 침해 · 도용	49조2항	71(5),72(3),73(1)
C15	정보통신망법 적용대상 이외의 개인정보침해		없음[6]

4) KISA(한국인터넷진흥원). http://www.kisa.or.kr/.
5) 해당 법규 위반 시 부과되는 벌금으로 천만원단위로 계산
6) 법조항에 해당하지 않는 사고피해의 규모는 개별적 소송으로 정한다.

〈표 2〉 개인정보침해 신고유형별 통계분석

유형 / 년도		증가형 (58%)								감소형 (42%)							총계
		C01	C02	C03	C04	C05	C06	C10	C14	C07	C08	C09	C11	C12	C13	C15	
2003		260	10	38	337	172	8	122	8,058	9	88	82	795	229	1,195	6,374	17,777
2004		564	27	43	784	235	2	107	9,163	5	42	212	2,312	569	736	2,768	17,569
2005		1,140	15	33	915	187	4	151	9,810	7	25	390	771	287	71	4,400	18,206
2006		2,565	27	61	917	206	5	266	10,835	11	23	632	923	484	23	6,355	23,333
2007		1,166	7	51	1,001	123	2	146	9,086	14	10	522	865	461	14	12,497	25,965
2008		1,129	6	87	1,037	125	6	294	10,148	9	26	1,321	949	503	27	24,104	39,771
2009		1,075	15	115	1,171	158	6	294	6,303	6	10	819	680	603	19	23,893	35,167
2010		1,267	75	146	1,202	158	25	323	10,137	22	21	1,551	826	630	35	38,414	54,832
2011		1,623	53	379	1,499	278	36	488	67,094	64	38	10,958	662	800	71	38,172	122,215
2012		3,020	368	711	1,922	770	117	731	116,263	33	44	3,278	613	568	40	10,886	139,364
총계		13,809	603	1,664	10,785	2,412	211	2,922	256,897	180	327	19,765	9,396	5,134	2,231	167,863	494,199
비율(%)		2.83	0.12	0.33	2.21	0.49	0.04	0.60	50.92	0.04	0.07	4.06	1.95	1.06	0.46	34.83	100.00
발생	內	C01, C02, C03, C04, C05, C06, C10 (6.6%)								C07, C08, C11, C12, C13 (3.6%)							(10.2%)
	外	C14 (50.9%)								C09, C15 (38.9%)							(89.8%)

기간: 2003.01 ~ 2012.11

출처: 인터넷통계정보검색시스템[7]

때 증가하였다가 감소하였다. 지난 10년간 개인정보침해 신고유형별 통계결과는 〈표 2〉와 같다.

최근 문제가 커진 '기술적 · 관리적 조치 미비로 인한 개인정보누출 등'(C09)의 사고는 2011년 전년도보다 10배까지 증가하였다가 2012년에서야 2010년 이전 수준으로 감소하였다. 개인정보침해의 위험을 발생위치로 구분하여 보면 집단 외부의 공격으로 인해 발생한 사고가 89.8%로 매년 증가하고 있는 실정이다.

2. 사례분석

개인정보침해 사례를 기반으로 정보통신기술이 지닌 위험을 분석하기 위해 발생가능성과 영향으로 구분하여 사고의 심각성을 측정하였다. 발생가능성은 각 유형별로 신고가 발생한 건수를 기반으로 측정하여 향후 동일한 위험이 발생할 가능성의 예측이 가능하다(Slovic, 1987). 영향은 유형별로 해당하는 벌칙조항에 명시된 벌금으로 경제적인 피해 규모를 측정하여 동일 위험 발생 시 피해가 예상되는 경제적인 규모를 계산한다(한창희, 2011). 각 신고유형은 해당 위험의 발생빈도와 영향이 높고 낮음에 따라 〈그림 5〉와 같이 '심각한 위험, 강력한 위험, 중심적 위험, 기본적 위험' 네 가지로 구분된다.

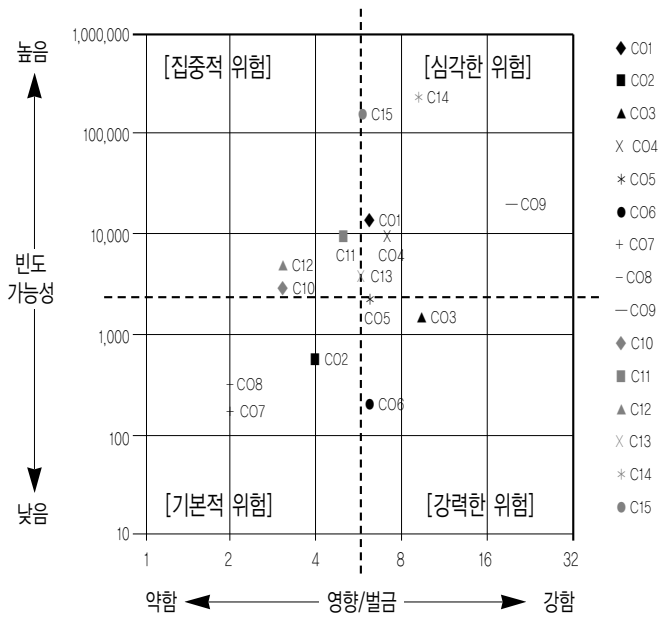
1) 심각한 위험의 회피사례(C09, C14, C15)

(1) 높은 빈도 · 강한영향의 심각한 위험

위험의 발생가능성이 높고 피해의 영향력이 큰 상황은 심각한 위험이다. 개인정보침해의 사례분석에서는 과거 발생건수가 많고 이로 인해 부과된 법조항

7) http://isis.kisa.or.kr/

유형	가능성 빈도[9]	영향 벌금[10]
C01	13,809	6
C02	603	4
C03	1,664	9
C04	10,785	7
C05	2,412	6
C06	211	6
C07	180	2
C08	327	2
C09	19,765	19
C10	2,922	3
C11	9,396	5
C12	5,134	3
C13	2,231	6
C14	256,897	9
C15	167,863	5.8[11]



〈그림 5〉 개인정보침해의 가능성과 영향에 따른 위험분석[8]

의 벌금이 큰 위험 C09, C14, C15 유형이다. C09는 '기술적 · 관리적 조치 미비로 인한 개인정보누출 등'으로 발생하는 위험이다(법 제28조1항). C09의 발생건수는 2만여건으로 타 사고에 비해 적은 편이나 개인정보누출로 인한 피해의 영향은 매우 크다. 개인정보보호법에서는 피해발생 시 64조의 1억원, 71조의 5천만원, 73조의 1천만원, 76조의 3천만원 등 문제의 경중에 따라 가장 많은 벌금을 부과한다. C14는 '주민등록번호 등 타인 정보의 훼손 · 침해 · 도용'이다(법 제49조2항). 지난 10년간 신고발생건수는 25만건으로 전체 사고의 과반수를 차지할 만큼 발생가능성이 크다. C14의 피해발생시 영향을 법적 비용으로 산정하며 71조의 5천만원, 72조의 3천만원 73조의 1천만원이다. 개인정보를 보유한 조직의 악의 여부와 관리 소홀의 수준에 따라 벌금을 부과한다. C15는 '정보통신망법 적용대상 이외의 개인정보 침해'이다. 10년간 누적신고가 17만건을 차지할 만큼 법에서 다루지 않는 다양한 위험이 존재한다. 전체 사고의 35%가 법 이외의 문제로 개인정보침해와 관련된 위험의 불확실성은 매우 높으며 관련지식의 수준 또한 낮다. C15는 법에서 정한 바가 없으므로 타 사고유형 벌금의 평균을 적용하여 위험의 최소 정

8) X축, 영향: 사고발생현황의 상대적인위치를 보기위해 영향의 측정값을 Log값으로 변환하여 표기
Y축, 빈도: 사고발생현황의 상대적인위치를 보기위해 사고발생건수의 측정값을 Log값으로 변환하여 표기
9) 2003년부터 2012년 9월까지 사고별 신고건수의 합계
10) 법의 벌칙조항에서 정하는 벌금 위험이 발생하였을 때 법적부담금으로 정한다(단위: 1천만원).
11) 법조항에 해당하지 않는 사고피해는 다른 사고 값의 평균으로 법적부담금을 정한다.

도를 측정 · 관리한다. 2011년 넥슨코리아의 개인정보유출 사고로 방송통신위원회(이하 방통위)는 7억원의 과징금을 부과하였으며, 2012년 KT의 개인정보유출은 10억원 상당의 피해를 일으켜 실제 사고가 발생한 경우 관련 피해의 영향이 크다.

(2) 계층주의집단의 위험회피정책

심각한 위험의 대상이 되는 집단은 그리드의 구속이 강하고 집단성이 높은 계층주의 문화형식을 보인다. 그리드는 성별, 나이, 종교, 국적, 언어 등 구성원이 한번 특성을 지니면 좀처럼 바뀌지 않는다. 집단성은 집단 내 교류, 협력, 소통 등의 유대관계의 높고 낮음을 나타낸다. 단일민족으로 구성된 강한 그리드와 인터넷이 발달한 좁은 한반도에서 한글 콘텐츠로 소통하는 강한 집단성을 지닌 대한민국은 전형적인 계층주의 집단이다. 계층주의 문화유형을 지닌 집단에 발생한 위험은 정부가 주도하여 관료 기반의 공적 위험을 관리하여야 한다. 공적 위험의 성격이 강한 심각한 위험의 대응은 사전에 정기적으로 점검하여 사고를 미연에 방지하는 적극적인 회피전략이 적합하다. 사례분석에서 확인한 C09, C14, C15 유형의 사고는 심각한 위험을 내포하기 때문에 국가 등의 강력한 권한을 지닌 계층주의 집단이 주도하여 정책적으로 위험의 예방 전략을 수립하고 적용하는 것이 적당하다. 최근 기업의 개인정보 유출사고가 빈번해지고 그 피해가 심각해지자 개인정보취급을 의무화하는 인터넷실명제를 폐지하여 사고위험을 사전에 차단하기 위해 대응을 준비하는 정부정책은 심각한 위험에 대한 예방위주의 회피전략 사례로 볼 수 있다(참여연대, 11/08/10; 지디넷, 12/08/23).

(3) 빅 데이터 기반 위험사례

심각한 위험의 사례인 C09, C14, C15 유형은 발생빈도가 높으며 사고 발생 시 그 피해의 규모도 크다. 특히 C09의 경우 기술 · 관리 조치 미비로 인한 개인정보누출 사고라기보다는 빅 데이터 환경의 도래로, 관련 조직이 앞서가는 기술을 제대로 통제하지 못하여 발생하는 문제로 보인다. 빅 데이터의 대표적인 환경은 저렴한 하드웨어와 통신비용, 사용자의 무제한적인 참여와 자료공유, 센서 기계 등의 자동 로그 생성 등이다. 이러한 발전된 환경에서 빠르게(고성능) 늘어나는(대용량) 다양한(다양성) 데이터는 빅 데이터의 생성을 촉진시킨다. 급격히 성장하는 빅 데이터는 소유권이 타인에게 있고, 의도한 바와 다르게 비정형적으로 생성되기 때문에 특정 조직이 관리하기에는 예방비용도 크고 기술적으로 해결할 문제도 복잡하다. 이러한 빅 데이터화로 인하여 발생하는 개인정보침해의 문제는 현재 KISA, 방통위 등이 중요한 정보화 부분의 정책문제로 해결하기 위한 핵심 의제로 다루고 있다.

2) 강력한 위험의 전가사례(C03, C06)

(1) 낮은 빈도 · 강한영향의 강력한 위험

위험 발생가능성이 낮고 피해로 인한 영향이 높은 상황은 강력한 위험이다. 개인정보침해의 사례분석에서는 과거 발생건수는 적으나 이로 인해 부과된 법조항의 벌금이 큰 위험 C03, C06 유형이다. 지난 10년간 C03의 발생건수는 1,600건, C06은 200건으로 발생빈도는 매우 낮은 편이다. C03은 '과도한 개인정보 수집'으로 발생하는 위험이다(법 제23조 2항). 이에 해당하는 피해비용을 계산하면 C03은 71조 5천만원, 76조 3천만원, 76조 1천만원등 그 영향이 크다. C06은 '개인정보 처리 위탁 시 고지의무 불이행'으로 발생하는 위험이다(법 제25조 1항). C06의 경우도 1천만원(법 제64조), 5천만원(법 제71조)으로 피해영향이 크다. C03과 C06 모두 기업의 개인정보 남용을 위해 고의에 의해 발생하는 사고이다. 따라서 발생가능성은 낮으나 이로 인한 고객의 피해가 크기 때문에 정부는 적극적으로 규제한다.

(2) 평등주의집단의 위험전가정책

강력한 위험의 대상이 되는 집단은 평등주의 문화

유형을 보인다. 평등주의는 성별, 나이 등의 구속력은 낮으나 소통, 거래 등의 집단성은 높은 집단이다. 평등주의는 노력에 의해 같은 관심사를 가진 영리기업이나 전문집단의 특성을 나타낸다. 평등주의 성격의 집단은 강력한 위험을 방지하기 위해서는 사전에 많은 비용이 투입되는데, 평등주의의 그리드는 낮기 때문에 합의점에 일치하기 쉽지 않다. 따라서 위험이 발생한 이후에 보상이나 지원을 받는 보험, 인증 등의 전가정책이 적합하다. 정보통신기술의 가장 대표적인 전가정책은 감리, ISO27001 등 인증이다. 2008년 옥션의 1800여만명의 회원정보의 유출 이후 ISMS, ISO 등 보안인증획득을 통해 위험의 전가 전략은 더욱 확산되었다.

(3) 고성능 기반 위험사례

강력한 위험의 성격을 지닌 개인정보침해 대상은 고성능 시스템이다. 광대역의 이동통신 환경에서 고성능스마트폰 사용이 범용화 되자 개인의 로그, 콘텐츠, 정보 등 다양한 데이터가 실시간으로 자동 저장된다. 특정한 목적을 위해 구성된 기업 등은 정규화되고 의도된 데이터를 정제하여 고성능 시스템에 저장, 관리한다. 이때 생성된 데이터는 소유권이 해당 기업에 있어 다양한 마케팅이나 이벤트에 사용한다. 따라서 실시간 생성, 이동, 적재, 분석 등의 다양한 처리를 빠르게 수행할 수 있도록 고성능의 기능을 지닌다. 빅 데이터 구축기술, 생성환경 등이 발전할수록 기업 등의 고성능 시스템이 보유한 개인정보의 민감성과 양은 증가하고 유출 시 피해도 심각해지고 있다.

3) 집중적 위험의 완화사례(C11, C12)

(1) 높은 빈도 · 약한영향의 집중적 위험

사고가 발생하였을 때 그 피해는 약하나 발생빈도가 빈번한 상황은 집중적 위험이다. 개인정보침해사례에서 발생한 대표적인 집중적 위험은 C11, C12 유형이다. C11 유형은 '개인정보의 동의 · 철회 · 열람 · 정정의 요구에 불응' 한 경우이다(법 제30조 1,2,5항). C11의 사고 발생 시 법에서 규정하는 벌금은 5천만원이다(법 제71조). C12 유형은 '개인정보의 동의 · 철회 · 열람 · 정정을 수집보다 쉽게 해야할 조치 미이행' 이다(법 제30조6항). C12유형의 사고에 대한 벌금은 3천만원이다(법 제76조). C11, C12 유형사고의 누적발생회수는 각각 9만여건, 5만여건으로 매해 감소되고 있다.

(2) 운명주의집단의 위험완화정책

집중적 위험의 특징을 가지는 조직은 운명주의 문화유형을 지닌다. 운명주의 집단의 특성은 그리드가 높고 집단성이 낮다. 운명주의 집단은 그리드의 특성이 커서 성별, 종교 등 타고난 구성원의 특성으로 좀처럼 바뀌지 않는 제약성을 지닌다. 그러나 집단성은 약하기 때문에 구성원간의 소통, 거래 등 유대관계는 낮다. 이러한 운명주의 집단은 그리드의 특성에 의해 구성되는 커뮤니티나 포털 등이 해당한다. 집중적 위험의 대표 사례인 C11, C12 사고의 경우 모두 '개인정보의 동의 · 철회 · 열람 · 정정' 에 대한 문제로, 운명주의 성격을 지닌 포털 등이 주로 발생하는 사고이다. 이러한 위험은 사고 빈도는 잦아도 발생을 방지하는 비용이 낮은 집중적 위험인데, C11, C12의 경우 사고를 일으키는 몇몇 포털이나 커뮤니티 기업만 통제하면 되므로 역시 위험을 사전에 최소화하기 위한 비용이 적다고 볼 수 있다. 해당 기업은 C11, C12 등의 문제를 사전에 방지하기 위해, 회원가입과 회원정보 수정 부분에 프로그램 개발 등 시스템을 수정하여 기술적인 통제방법을 적용한다.

(3) 대용량 기반 위험사례

C11, C12 등 개인정보의 동의 · 철회 · 열람 · 정정에 대한 위험을 지닌 주요 업체는 구글, 네이버 등의 검색이나 포털이다. 구글은 기업의 법적, 지리적 차이로 인해 국내법 규제에 불응하여 몇 년째 한국 규제에 불응하고 있는 실정이다. 구글의 인터넷실명제

등의 거부는 대용량 고객정보 유출의 위험을 사전에 방지할 수 있었기 때문에 결과론적으로는 현명한 기업방침이었다고 평가할 수 있으나 구글, 다음 등 개인의 위치정보를 무단으로 수집한 검색, 포털 기업들의 위반사례는 증가하고 있다(경향신문, 11/05/03). 이러한 잦은 사고에도 불구하고 정부의 솜방망이 처벌로 인해 피해는 줄어들지 않고 있다. 실례로 방통위는 애플이 위치정보 앱 종료 후에도 정보를 서버로 전송한 점이 사용자의 동의를 얻지 않고 위치정보를 수집 · 이용해서는 안 된다는 위치정보보호법(제15조 1항)을 위반했다고 판단했지만 과태료 300만원을 부과하는데 그쳤다(서울경제, 11/08/03).

4) 기본적 위험의 수용사례(C07, C08)

(1) 낮은 빈도 · 약한 영향의 기본적 위험

사고의 발생가능성도 낮고 사고 발생 시 피해도 적은 상황은 기본적 위험이다. 개인정보침해 사례에서 기본적 위험의 유형은 C07, C08이다. C07은 개인정보에 대한 영업적인 양수 등의 통지의무를 불이행하였을 때 발생하는 사고이다(법 제26조 1항). C08은 기업이 개인정보관리에 대한 책임자를 지정하지 않아 발생하는 피해에 대한 위험이다(법 제27조 1항). 두 유형 모두 신고발생건수가 10년간 이삼백건으로 낮은 수준이다. 이로 인해 발생한 사고의 경우 법에서 정하는 벌금도 2천만원으로 경미하다(법 제76조). 기본적 위험은 위험사고 발생 시 사회적으로 미치는 영향도 약하고 대중의 관심도 낮다.

(2) 개인주의집단의 위험수용정책

기본적 위험과 관련된 주요 집단은 그리드의 구속이 낮고 집단성도 약한 개인주의 문화유형의 특성을 지닌다. 인구, 성별, 국적 등 타고난 그리드의 제약도 없고 거래, 소통 등 구성원간 집단성도 약한 전형적인 개인들에 해당한다. 개인정보침해 사고의 경우 최진실 사건 등 공인의 피해가 큰 경우도 있으나 대부분은 개인을 대상으로 하여 피해의 영향은 미미한 편이다(SBS뉴스, 08/10/08). 또한 피해 발생 시 개인이 민사소송 등을 통해 해결하는 등 기본적 위험이 발생 가능하도록 방치하는 수용정책을 적용하는 실정이다.

이 연구의 분석대상인 개인정보침해사례에서 기본적 위험의 성격을 가지는 위험은 C07, C08이다. C07의 경우 개인정보에 대한 영업적 양수에 대한 문제인데, 주로 텔레마케팅의 수단으로 악용된다. C07처럼 텔레마케팅에 이용되었다는 근거를 개인이 밝히기는 매우 어렵기 때문에 사고발생건수가 적고 그 법적 제제도 어려운 실정이다. 반면 C08은 기업의 개인정보관리책임자를 지정하지 않았을 때 발생하는 위험인데, 조직원 하나가 기업전체를 통제할 수 있는지 효율성에서부터 문제가 있다. 기본적 위험에 해당하는 개인정보보호를 위해서는 개인정보 관리책임자 한 명이 아니라 기술, 문화, 법규, 규범 등을 포함한 체계적인 대응이 필요하다. 기본적 위험은 다양한 반면 체계적인 대응은 거대한 비용을 수반하므로 사실상 관련사고 발생 시 방치할 수밖에 없는 수용적 대응이 적용된다.

(3) 다양성 기반 위험사례

개인정보의 영업적인 양수에 대한 규제는 2008년 강화되면서 신용정보업 일부 양도 및 양수의 경우에도 금융위 인가를 받도록 요건을 강화하였다(뉴스핌, 08/07/23). 그러나 인수합병 및 신규브랜드 창출을 통해 기업들은 법의 통제를 벗어나서 여전히 개인정보를 영업적으로 거래하고 있다. 이로 인해 기업이 보유한 개인정보의 크기와 다양성은 날로 커지고 있다. 특히 통신사와 신용카드사의 제휴 등 전 국민의 개인정보는 각 기업들이 덩어리로 보유, 활용하고 있다 해도 과언이 아닐 것이다. 일반적으로 신용카드 한 장에 가입하면 250개 기업에 개인정보가 공개된다고 한다(머니투데이, 12/03/27). 법에서는 제3자에게 제공 동의하지 않아도 회원가입 가능해야 하지만 적발 시 내는 과징금보다 이로 인한 이득이 크기

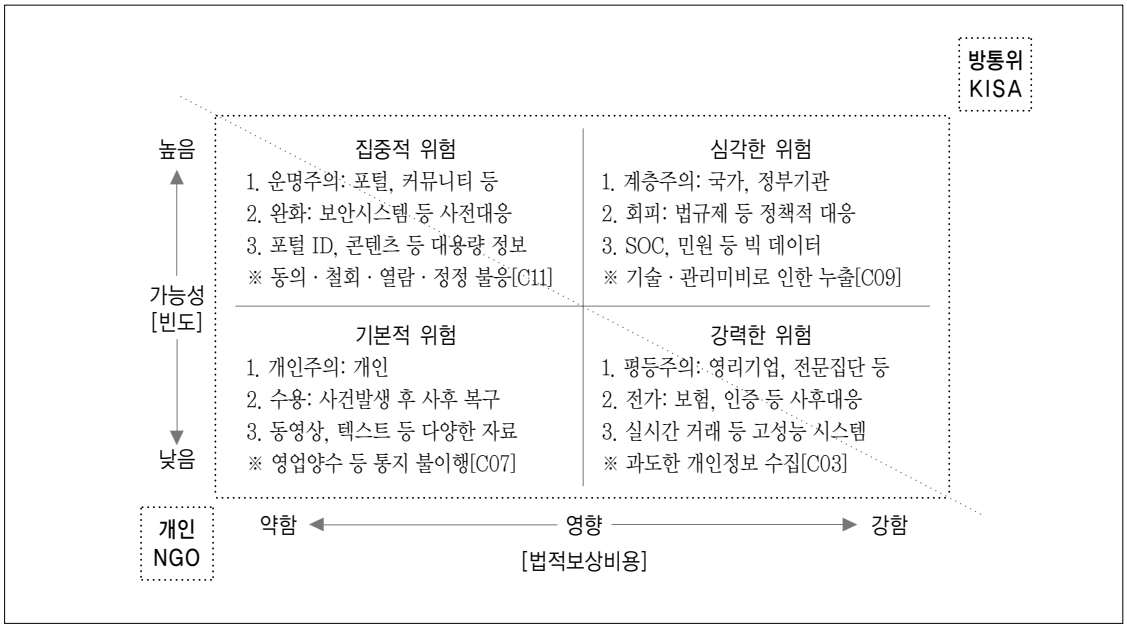
때문에 지키는 카드사는 없는 실정이다. 제휴, 마케팅, 설문조사 등 개인정보의 빅 데이터화는 영리기업에는 더할 나위 없이 좋은 기회인 것이다. 반면 정부입장에서는 다양해지는 개인정보의 유형에 따라 범죄방법과 개인정보침해도 지능화되어 그 위험대응은 더욱 어려워지고 있는 실정이다.

3. 분석결과

개인정보유출에 대한 정보통신기술의 위험은 네 가지 큰 상황으로 구분된다. 각 상황은 위험의 발생가능성의 크기와 피해영향의 정도에 따라 구분했다. 구분된 위험상황은 시간이 지나도 같은 유형의 특성을 지니고 있었다. 위험과 관련된 집단은 특유의 문화유형을 지니고 있었으며 이에 따라 위험의 대응정책을 적용하였다. 또한 각 위험상황은 관련 집단의 문화유형에 따라 정보통신기술에 나타나는 빅 데이터 성격에도 차이를 보였다. 개인정보침해의 사례분석결과 위험상황별 대응사례는 〈그림 6〉과 같다.

분석결과 1. 발생가능성과 영향에 따라 정보통신기술의 위험은 '심각한 위험, 강력한 위험, 집중적 위험, 기본적 위험'으로 구분된다. 1.1 개인정보침해 사례분석결과 개인정보누출사고(C09)는 개인정보 훼손 · 침해 · 도용(C14) 등 다양한 사고(C15)로 확산되는 것을 확인하였다. 전체사고의 80% 이상을 차지하는 C14, C15를 대응하기 위해서는 먼저 C09사고를 선결해야 할 것이다. 1.2 위험의 영향을 평가할 때 법에서 강한 규제가 강할수록 피해비용도 큰 것으로 확인할 수 있었다. 실례로 C09사고로 인한 법적 최대 벌금은 10억이었고 사고 발생 시 부과된 판례는 7억원이었다.

분석결과 2. 위험상황에 따라 해결전략은 각 관련 집단이 갖는 문화의 유형에 따라 대응정책을 적용하였다. 2.1 위험상황별 관련조직의 문화유형은 '심각한 위험-국가 등 계층주의', '강력한 위험-기업, 전문집단 등 평등주의', '집중적 위험-포털, 커뮤니티



분석요소: 1. 문화유형, 2. 대응정책, 3. 빅 데이터특징
※ 위험사례

〈그림 6〉 개인정보침해의 위험상황별 대응정책

등 운명주의', '기본적 위험-개인'이다. 2.2 개인정보침해의 사례분석결과 관련 집단이 갖는 문화유형에 따라 대응전략은 비용대비 효율을 최대화할 수 있는 정책을 적용하였다. C09 등 개인정보 누출 및 침해 위험을 지닌 심각한 위험은 국가적 차원에서 사전에 예방하는 회피전략을 적용하였다. C03 등 과도한 개인정보수집으로 인해 발생하는 개인정보침해는 대상기업을 적발하여 과징금을 부과하고 보험, 인증 등을 획득하는 복구중심의 전가전략을 적용하였다. C11 등 동의, 철회와 관련된 집중적 위험은 개인정보를 수집단계에서 사전에 방지할 수 있도록 포털 등의 회원가입 프로그램에 적용하는 기술적인 완화전략을 적용한다. C07 영업권 양수 등 기본적 위험은 유형도 다양하고 사실상 예방하기 힘들기 때문에 사고발생 후 복구하는 수용정책으로 대응할 수밖에 없는 실정이다.

분석결과 3. 위험상황에 따라 정보통신기술은 관련 집단의 문화적 특성에 따라 차이를 보였다. 정보통신기술의 발전 및 사회적인 데이터 공유의 문화 확산에 따라 개인정보의 빅 데이터 현상은 가속되었고 이로 인한 위험도 함께 증가하였다. 심각한 위험은 국가수준의 대용량, 고성능, 다양성의 빅 데이터의 모든 특징을 보유하였으며 싸이월드의 3천5백만 고객정보 누출 등 이로 인한 피해도 심각하다. 강력한 위험이 갖는 정보통신기술의 특징은 영리기업이나 전문 집단이 보유하는 고성능 시스템이다. 이들 기업이 보유하는 개인정보는 실시간 자동화 기능을 지닌 고성능 시스템에 의해 빅 데이터화 되고 피해 발생의 규모도 커지고 있다. 집중적 위험이 가지는 기술적 특징은 커뮤니티, 블로그, 포털 등이 갖는 대용량 정보이다. 인터넷의 '공유, 참여, 개방' 문화의 확산에 따라 해당조직이 보유하는 개인정보는 대용량의 빅 데이터 성격을 지니게 된다. 기본적 위험의 대상은 개인으로서 이들이 보유하는 자료는 동영상, 문서, 로그 등 그 형식도 다양하고 소유권, 저작권 등 법적 권리도 다양하였다.

Ⅴ. 결 론

정보사회의 위험을 기술뿐만 아니라 문화유형을 이해하고 정책적인 시각으로 접근하기 위하여 사례분석을 수행하였다. 특히 국내뿐만 아니라 세계적으로 피해 사례가 급증하고 있는 개인정보침해사례를 대상으로 분석하였다는데 의의가 있다. 사례분석의 결과는 다음과 같다. 첫째, 위험대응에 대한 차별적인 적용이 필요하다. 위험은 기본적으로 불확실성에서 출발한다. 개인정보침해의 문제는 특히 현재 중요한 사회문제이자 주요 정책현안이다. 이러한 정보통신기술의 보안에 대한 정책과제 해결을 위해서는 발생가능성과 영향에 따라 달라지는 위험에 대한 이해가 필요하다. 둘째, 위험대응을 위해서는 관련 집단의 문화이해가 필요하다. 위험상황별 관련 조직의 그리드와 집단성에 따라 달리하는 문화적 특성을 이해하고 위험에 대응해야 효과적이다. 우리나라 경우 국가, 기업, 포털, 개인 등 집단의 특성에 따라, 또한 국내기업인지 해외기업인지 적용법의 기준에 따라 개인정보침해 사고의 대응이 달라지는 것을 확인할 수 있었다. 셋째, 빅 데이터 현상으로 인한 정보통신기술 위험의 변화이다. 위험상황에 따라 대상 개인정보가 갖는 기술적 특성이 달랐다. 빅 데이터의 '대용량, 고성능, 다양성' 특징이 개인정보에도 확장되면서 이로 인한 위험은 더욱 빈번히 발생하고 그 영향도 커지는 것을 확인할 수 있었다.

사례분석의 결과 시사점은 다음과 같다. 첫째, 위험상황별 문화유형과 빅 데이터의 특성을 이해하여 대응정책을 수립 · 적용할 정부의 전담조직이 필요하다. 빅 데이터 시대 정보화가 가지는 위험상황별 특성은 분석틀의 특성과 거의 일치했다. 그러나 사례에서 정보화 위험의 대응 및 정책수립은 사고가 발생한 후 복구하는 형식의 대응전략 위주였다. 위험기반의 정책수립에서는 심각한 위험은 사전에 위험을 예측하고 대응전략을 수립 · 적용하여야 하는데 방통위, KISA 등 정부기관이 주체가 되기는 하였지만 그 대

응은 여전히 사후 복구 중심이었다. 이는 정보통신기술이 가지는 예측 불가능성과 가변성의 문제도 있겠지만, 이를 전담으로 담당하는 상설 조직이 없는 것도 문제이다. 따라서 빅 데이터의 기회를 활용하고 이로 인한 정보위험을 전담할 정부 내 상설조직의 설립이 필요하다고 본다. 둘째, 위험대응을 위해서는 정보화가 가지는 문화적 특성과 데이터의 특성을 함께 이해하여 '기술, 규범, 법, 시장' 측면에 예방과 복구를 위한 체계적 대응정책이 필요할 것이다(Lessig, 1999). 정보보안의 위험은 더 이상 기술로만 해결할 수 없다. 인터넷이나 SNS 사용에 있어서 자료의 사용권 보호, 상호 비방 방지를 위한 규제, 댓글이나 참조 표기에 대한 표준 양식 등의 각종 규범이 필요하다. 뿐만 아니라 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 등 다양한 법규제가 필요하다. 마지막으로 정보화로부터 발생하는 기회와 위험이 공존할 수 있는 시장구조가 필요하다. 인터넷실명제의 발효는 국내 네티즌들이 구글 이메일과 페이스북을 사용하게 되는 계기를 만들었다. 이에 따라 구글 등에 동반된 유튜브나 트위터 등이 국내의 인터넷 시장을 선도하게 되었다. 이와 같이 인터넷실명제 등의 과도한 규제는 오히려 국가의 경쟁력을 약화시키고, 국내 고객을 오히려 해외로 빠져나가게 만들 수도 있다. 빅 데이터 시대의 정보통신기술이 지닌 위험에 대한 대응 정책은 시장의 상황을 고려하여 균형 있게 설계되어야 할 것이다.

빅 데이터 시대의 도래는 확실히 여러 기업과 각종 사회의 새로운 기회를 줄 것이다. 이러한 빅 데이터의 기회는 국가가 개입하지 않아도 민간에서 자발적으로 발굴하고 활성화할 것이다. 그러나 빅 데이터 현상으로 인한 개인정보의 누출 등 정보통신기술로부터 발생하는 피해와 훼손은 이미 국가적인 재난의 문제가 되어 중요한 정책으로 다루어야 할 시기이다. 정보통신기술로 부터 발생하는 위험의 영향은 법률에서 정하는 과태료뿐만 아니라 기업의 이미지나 다른 비정량적 요소를 반영하여 결과치를 보정하는 등 정교화하여 대응 정책의 수립에 반영할 필요가 있다. 그러나 이러한 정책의 반영은 단기간에 이룰 수 있는 문제가 아니라 조직적이고 장기적인 정부의 노력이 필요하다. 얼마 전 행정안전부는 '빅 데이터 공통기반 업무 설계와 구축 계획 등을 수립할 예정'이라고 밝혔다(디지털타임즈, 12/10/22). 빅 데이터 공통기반 시스템은 정부 기관들에서 보유하고 있는 데이터들을 연계해 분석을 목표로 한다고 발표한 것이다. 이제 정부는 관리자의 입장이 아닌 실행자의 입장에서 전 국민을 위협하는 개인정보침해 등의 정보화의 문제를 빅 데이터 관점에서 구축·활용하여 정책적으로 관리하여야 할 것이다. 빅 데이터 시대 정보통신기술의 위험에 대한 대응 정책의 수립에 있어서 이 논문은 문화와 기술의 측면에서 균형 있는 정책설계의 방향을 모색하는데 도움이 되리라 기대한다. 또한 빅 데이터 시대 정보위험에 대한 대응 정책의 수립에 있어서 '정당성'의 가치와 '공고화'의 절차를 확보하기 위해서는 과거 정보통신부와 같은 전담 조직과 의사결정 체계가 필요하다고 주장하는 바이다(김영평, 1991).

이 연구는 정보통신기술이 지닌 위험을 다양한 관점에서 분석하지 않고 개인정보유출사고의 사례만 대상으로 하여 분석하였다는데 한계가 있다. 또한 사고의 영향을 법률에 정한 과태료로 산정하여 실질적인 피해비용의 측정에 미흡했다. 향후에는 사고가 발생한 기업이나 기관의 특성을 반영하여 비정량적인 척도를 고려하고 실제 사고가 발생하여 피해가 미친 영향을 심층적으로 분석한다면 정책설계에 활용이 가능한 실증적인 연구가 될 것이다. 그리고 45만여 건이나 되는 사례를 단순히 기술하는 것에 그칠 것이 아니라 통계분석 기법을 활용해 분석한다면 각 사고 간의 영향력 등을 파악하여 근본 원인이 되는 문제를 발굴하여 집중적인 정책 대상을 발굴하는 등 정책설계에 많은 도움이 되리라 기대한다.

■참고문헌

김영평 (1991). 「불확실성과 정책의 정당성」. 서울: 고려대학교출판부.

소영진 · 김영평 · 최병선 · 정윤수 · 정익재 (2001). 「한국 원자력 기술의 체감안전성에 관한 비교연구」. 대전: 한국원자력연구소.

정익재 (2007). "정보보안 취약성 분석과 정책적 대응논리." 「한국정책학회보」, 16(2): 211-238.

한창희 · 채승완 · 유병준 · 안대환 · 박채 (2011). "기업의 개인정보유출로 인한 경제적 피해규모 산출방법." 「한국전자거래학회지」, 16(4): 16-30.

경향신문 (2011). "떨고있는 포털업계… '개인 위치정보 수집' 구글 · 다음 압수수색." 5월 3일.

뉴스핌 (2008). "마케팅전화 거부 · 개인정보 동의 철회권 도입." 7월 23일.

디지털타임즈 (2012). "빅 데이터 활용이 개인정보 유출로 이어지지 않도록 법제화 노력 이어져야." 10월 19일.

디지털타임즈 (2012). "빅 데이터 공통기반 시스템 만든다." 10월 22일.

머니투데이 (2012). "카드한장 가입했는데…"개인정보 250곳에 뿌려진다": 개인정보 제3자 제공 동의하지 않아도 회원가입 가능해야 하지만 지키는 카드사 없어." 3월 27일.

서울경제 (2011). ""글로벌 기업 눈치" 솜방망이 처벌 논란." 8월 3일.

서울경제 (2012). "[KT 고객정보 유출] 해킹 · 악성코드 아닌 가입자 정보 조회하듯 한건씩 빼내." 7월 30일.

지디넷 (2012). "헌재 '위헌'…인터넷 실명제 폐지 된다." 8월 23일.

참여연대 (2011). "개인정보 해킹, 인터넷실명제폐지가 대안이다." 8월 10일.

SBS뉴스 (2008). ""' 최진실 괴담 ' 유포자 괘씸" 개인정보 유출 테러." 10월 8일.

Beck, Ulrich (1998). *The Politics of Risk Society.* Oxford: Polity Press.

Cobb & Elder (1983). *Participationin American Politics.* Baltimore: Johns Hopkins Univ. Press.

Cobb, Roger & Ross J. K. & Ross Macc H. (1976). "Agenda Building as a Comparative Political Process." *American Political Science Review*, 70: 126-135.

Crouch, Edmund & Richar Wilson (1983). *Risk/Benefit Analysis.* Cambridge, MA.: Ballinger Publishing Co.

Deloach, J. W. (2000). *Enterprise-wide Risk Management. Strategies for Linking Risk and Opportunities.* London: Financial Times/Prentice-Hall.

Douglas, Laney (2001). "3D Data Management: Controlling Data Volume, Velocity and Variety." Meta group (now Gartner). http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. (Retrieved on August 12, 2012).

Douglas, Mary & Aaron Wildavsky (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers.* Berkeley, CA: University of California Press.

Gantz, John & Reinsel, David (2011). "Extracting Value from Chaos." IDC IVIEW June.

Gonzalez, Jose J. & Agata Sawicka (2002). "A framework for human factors in Information security." Proceeding soft he WSEAS International Conference on Information Security (ICIS' 02), Riode Janeiro, Brazil.

George, Alexander L. & Andrew Bennett (2005). *The Method of Structured, Focused Comparison in Case studies and theory development in the social sciences.* Cambridge, MA and London, England: MIT Press.

Lessig, Lawrence (1999). *Code and Other Laws of Cyberspace.* New York: Basic books.

Manyika, James & Chui, Michael (2011). "Big data: The next frontier for innovation, competition, and productivity." McKinsey Global Institute. http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_inn

ovation. (Retrieved on May 1, 2012).
May, P. J. (1991). "Reconsidering Policy Design: Policies and Publics." *Journal of Public Policy*, 11(2): 187-206.
May, P. J. & Joshua Sapotichne, & Samuel Workman (2009a). "Widespread Policy Disruption: Terrorism, Public Risks, and Homeland Security." *Policy Studies Journal*, 37(2): 171-194.
May, P. J. & Joshua Sapotichne & Samuel Workman (2009b). "Widespread Policy Disruption and Interest Mobilization." *Policy Studies Journal*, 37(4): 779-801.
Norrman, A. & Jansson, U. (2004). "Ericsson's proactive risk management approach after a serious sub-supplier accident." *International Journal of Physical Distribution and Logistics Management*, 34(5): 434-456.
Ponemon Institute (2010). "Fifth Annual US Cost of Data Breach, January 2010." http://msisac.cisecurity.org/resources/reports/documents/symantec_ponemon_data_breach_costs_report2010.pdf. (Retrieved on October 10, 2012).
Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge(PMBOK®Guide)*. Carolina: PMI.
Slovic, Paul (1987). "Perception of Risk." *Science*, 236: 236-285.
Wildavsky, Aaron (1988). *Searching for Safety*. New Brunswick, NJ.: Transaction Publisher.