ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

디지털위험 관리조직에 대한 신뢰가 위험지각과 위험관리에 미치는 영향: 전문가 조사를 중심으로☆

Effect of Trust Toward Digital Risk Management Organization on Risk Perception and Cognition of Risk Management: Focused on Expert Survey

김 원 제[1] 김 찬 원[2]
Won-je Kim Chan-won Kim

요 약

본 논문은 전문가들을 대상으로 디지털위험을 관리하는 조직에 대한 신뢰가 위험지각과 위험관리 인식에 미치는 영향을 규명하였다. 주요결과를 보면, 첫째, 전문가들이 디지털위험을 관리하는 조직인 정부, 관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰가 높을수록 위험지각은 상대적으로 낮아지는 것으로 나타났다. 둘째, 한국사회 내에 존재하는 다양한 영역의 전문가들이 디지털위험을 관리하는 조직에 대해 높은 신뢰를 가질수록 관련 위험에 대한 관리가 효율적으로 이루어지고 있다고 인식하는 것으로 나타났다. 셋째, 디지털위험에 대한 위험지각은 위험관리 인식에 통계적으로 유의한 영향을 미치지 못하였다. 이런 결과에 비추어볼 때, 한국사회 내 새로운 위험으로 부각되고 있는 디지털위험을 효과적으로 통제, 예방하기 위해서는 사회 내에 신뢰를 높이고, 신뢰에 기반 한 의사결정이 이루어져야 할 것이다.

☞ 주제어 : 디지털위험, 신뢰, 위험지각, 위험관리, 전문가

ABSTRACT

The purpose of this study was to examine the effect of trust toward digital risk management organization on risk perception and cognition of risk management focused on expert survey. The results were as follows. First, Trust toward digital risk management organization influenced negatively on risk perception. Second, Trust toward digital risk management organization influenced positively on cognition of risk management organization. Third, risk perception on digital risk influenced not significantly on cognition of risk management organization. Findings of this study requires an effort to increase trust of digital risk management organization and to develop trust-based decision-making on digital risk.

☞ keyword : digital risk, trust, risk perception, risk management, expert

1. 서 론

한국은 세계적으로 정보통신기술 및 인프라가 고도화된 국가이자 정보통신 관련 테스트베드(test bed)로서 주요 국가로부터 주목을 받고 있는 정보통신 강국이라고 할 수 있으나, 역설적으로 다양한 디지털위험(digital risk)에 노출되어 있는 국가이기도 하다. 현재 한국사회에서 나타나고 있는 다양한 유형의 디지털위험은 고도화된 정보통신기술 및 네트워크에 기반 한 새로운 위험(new risk)으로서 어느 누구도 그 위험을 쉽게 예측할 수 없을 뿐만 아니라 고도화된 정보통신기술 및 네트워크에 의해 사회적으로 구조화된 위험이라는 점에서 엄청난 충격과 혼란을 유발할 수 있다. 디지털위험은 위험자체를 인식하지 못할 정도로 매우 은밀하게 이루어지며, 개인에게 위험이 발생하고 있음에도 정작 본인은 그 사실을 제대로 알 수 없고, 설사 자신에게 위험이 발생하고 있음을 인지하더라도 관련 정보와 지식이 부족하여 적절하게 대처하기도 어렵다는 한계를 갖는다. 디지털위험은 개인적 위험임과 동시에 사회적, 국가적 위험이기도 하며, 개인과 사회, 국가 모두가 합심하여 대처 및 해결해야 하는 총체적

[1] College of Social Sciences, Sungkyunkwan University. Seoul, 110-745, Korea
[2] SSK Risk Communication Center, Sungkyunkwan University, Seoul, 110-745, Korea.
* Corresponding author (ares6357@naver.com)
[Received 2 June 2015, Reviewed 7 June 2015, Accepted 10 July 2015]
☆ 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2014S1A3A2044217).

위험이다. 이에 디지털위험에 효과적으로 대응하고 관리하기 위해서는 위험커뮤니케이션을 통한 효율적인 위험관리의 필요성이 중요해지고 있다.

위험커뮤니케이션은 위험에 대한 정보를 제공하거나 위험발생 가능성을 알려줌으로서 위험을 예방하거나 위험으로 인한 부정적 결과를 최소화하는 것을 기본 목적으로 한다[1]. 이에 위험커뮤니케이션은 우리사회 내에서 다양한 위험요인으로 존재하는 디지털위험을 효과적으로 대처, 관리할 수 있는 핵심 요소라고 할 수 있다. 디지털위험과 같은 새로운 위험이자 고도의 전문지식이 필요한 영역에서는 전문가의 역할이 중요해진다. 전문가는 새롭게 부각되는 위험에 대해 공중에게 알리고, 관련 위험을 어떻게 해석하고, 대처해야 하는지에 대한 정보와 지식을 제공해줄 수 있어야 한다. 이를 가능하게 하기 위해서는 우리사회 내에 위험커뮤니케이션이 확고하게 자리 잡아야 하며, 위험에 대해 효과적인 소통이 이루어질 수 있는 위험커뮤니케이션 환경이 구축되어 있어야 한다. 하지만 전문가들도 특정 위험을 지각하는데 있어서 일정한 편향성(bias)이 존재하며, 그 편향성은 특정 위험에 대한 전문가들 사이에서 갈등과 충돌을 유발하여 일반 공중으로 하여금 관련 위험을 인지하고 해석하는데 있어 상당한 혼란을 초래하기도 한다.

일반적으로 전문가들은 일반 공중과 비교할 때, 위험을 주관적이 아닌 객관적으로 판단하는 특성을 보이나, 자신들이 속한 위험분야에 대해서는 위험강도를 낮게 지각하는 반면에 사회적 이익은 높은 것으로 바라보는 경향이 있다. 즉, 전문가들은 자신이 속한 영역에 대해서는 풍부한 정보와 지식을 갖고 있고, 위험강도를 연간 사망률과 같은 객관적 지표나 데이터를 통해 파악하기 때문에 위험이 잘 알려져 있고, 통제할 수 있으며, 더 친숙하다고 믿는 경향이 있다는 것이다[2]. 따라서 전문가들은 자신과 관련된 위험 영역에 대해 보다 친숙함은 물론 위험을 잘 통제할 수 있다는 믿음과 신념을 갖고 있으며, 이러한 믿음과 신념은 전문가의 위험지각 형성에 일정한 영향을 미쳐 일반 공중에 비해 관련 영역에 대한 위험을 낮게 지각하는, 이른바 위험지각과 관련된 편향성이 존재한다고 볼 수 있다. 이런 측면에서 전문가들의 위험지각은 우리사회 내에 존재하는 다양한 위험을 어떻게 평가하고, 효율적으로 관리해나갈 것인가에 대해 직접적 혹은 간접적 영향을 미칠 수 있기 때문에 특정 위험영역에 속한 전문가들에 국한하기 보다는 전문적 지식을 갖춘 다양한 전문가 집단을 대상으로 우리사회 내에 존재하는 위험들을 효율적으로 평가, 관리할 수 있는 방안을 도출하는데 필요한 요인들을 탐색할 필요가 있다. 이에 본 연구는 한국사회 내의 구조적 측면에서 새로운 위험으로 떠오르고 있는 디지털위험에 대해 심리측정패러다임을 적용, 전문가들이 갖고 있는 편향성을 최소화하고 효율적 위험관리 방안을 도출하는데 필요한 시사점을 제공하고자 하였다.

2. 이론적 배경

2.1 새로운 위험으로서의 디지털위험

디지털위험은 디지털기술이 선도하는 사회의 네트워크적인 특징과 그 위에서 발생하는 위험으로서 사회공동체의 존립과 운영에 부정적 영향을 미치는 각종 위험[3]을 포함한다. 인터넷의 확산과 그로 인한 정치, 경제, 사회행동 등의 많은 부분들이 디지털공간으로 이동되면서 정보와 지식이 핵심자원인 디지털사회를 창출하였으나, 모든 기술발달이 댓가를 요구하고, 각 단계마다 기술이 해결했던 문제보다 더 큰 문제를 일으킬 수 있는 야누스적 모습을 가지고 있기 때문에 기술발전의 부수적 결과로서 다양한 위험이 창출되고 있는 것이다[4], 특히, 디지털위험은 고도로 연결된 네트워크 환경이 위험을 창출하고, 고도화된 네트워크의 복잡성과 상호연결성이 위험과 결합[5]되어 나타난다는 점에서 위험 자체를 예측하기가 불가능하고, 위험유발자를 쉽게 파악할 수 없으며, 한번 발생한 피해는 네트워크상에서 지속되는 특성을 보인다. 따라서 디지털위험은 우리사회에서 네트워크가 고도화될수록 위험 역시 고도화된다는 점에서 기술발전의 부수적 결과이자 디지털환경이라는 새로운 환경적 틀 속에서 비롯된 위험이라고 볼 수 있다.

오늘날 디지털위험은 사적 영역이나 공적 영역 모두에서 전문지식이 필요한 영역으로서 복잡하면서도 매우 역동적인, 즉 변화가 빠른 위험영역이라고 볼 수 있다. 이에 따라 디지털위험은 공중이 그 위험을 인지하고 대처하기에는 상당히 제한적인 영역이며, 오로지 관련 정보와 지식 제공을 통해 미연에 방지하거나 예방하는 것만이 디지털위험을 제어할 수 있는 핵심조건이 된다. 현재 한국사회에서 대두되는 주요 디지털위험은 크게 사이버폭력, 정보유출, 해킹, 개인감시 및 통제라고 할 수 있다. 먼저 사이버폭력은 사이버공간에서 온갖 형태의 폭력적인 표현과 행위를 의미하는 것으로, 모욕적인 언사나 욕설, 인신공격성 발언, 사이버스토킹, 사이버명예훼손, 성적인 묘사나 여성비하, 성차별적 욕설, 개인의 신상

정보 유포 등을 포함한다[6]. 이러한 사이버폭력은 각종 비난과 위협 등을 통해 상대방으로 하여금 목숨을 끊게 만들기도 한다는 점에서 그 심각성이 높다고 할 수 있다.

정보유출은 가장 빈번하게 발생하는 디지털위험으로 예를 들자면, 2014년 국내 신용카드사의 고객정보가 대량으로 유출, 대한민국 국민 2명 중 1명의 개인정보가 유출되는 큰 피해를 입기도 하였다. 정보유출과 밀접한 관련이 있는 해킹은 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 행위로서[7], 임의적으로 타인의 아이디(ID)나 패스워드(Password)를 도용 혹은 자료를 유출 또는 훼손시킴으로서 개인에게 심각한 정신적, 재산적 피해를 유발하는 전형적인 디지털위험 중 하나라고 할 수 있다. 그리고 개인감시 및 통제는 첨단 디지털기술에 의한 초소형 감시 및 도청기기들의 등장과 관련된 위험으로, 이들 기술 및 기기들에 의해 개개인에 대한 적극적인 신원 확인 및 소재파악이 가능해졌으며, 사적 목적을 위해 악용될 경우에 명예훼손이나 프라이버시 침해로 나타날 소지가 높다. 최근에는 새로운 디지털위험으로서 인포데믹스(infordemics)가 부각되고 있는데, 인포데믹스는 Information(정보)과 Epidemic(전염병)의 합성어로서, 추측이나 과장, 혹은 부정확한 정보가 인터넷 혹은 스마트폰을 통해 전염병처럼 빠르게 전파되어 개인의 명예훼손이나 사생활 침해, 나아가 경제, 정치, 안보 등에 악영향을 미치는 새로운 유형이다. 허위게시 글이나 확인되지 않은 정보, 과장된 정보, 그리고 가짜 연평도 위성사진 등이 대표적인 사례이다. 이와 같은 디지털위험은 고도의 네트워크에 기반을 두고 나타나는 위험으로서 이전과는 전혀 다른 새로운 유형의 위험이자 디지털기술이 고도화될수록 그 심각성도 높아지는 위험이라고 볼 수 있다. 전술한 위험들은 현재 한국사회 내에서 발생하고 있는 전형적인 디지털위험으로서, 디지털위험의 심각성을 조사한 연구에서 개인생활감시과 개인정보유출, 잘못된 정보유포 및 확산(인포데믹스), 사이버폭력(테러) 등은 한국사회에서 심각성이 매우 높은 디지털위험으로 보고된 바 있다[3]. 우리는 일상적인 삶과 사회발전의 동력으로서 디지털기술에 상당 부분 의존하고 있다. 하지만 디지털기술에 대한 일상성과 의존성이 오히려 디지털위험을 실제적으로 인식하고 받아들이는데 부정적 영향을 미치기도 한다. 이런 맥락에서 디지털위험은 우리가 일상적으로 노출될 수 있는 위험이자 예측불가능하고 효과적으로 통제하기가 거의 불가능한 고도의 위험이라고 볼 수 있는 것이다. 그러므로 디지털위험 발생가능성을 줄이고, 위험을 최소화하기 위해서는 일상적으로 준비상태가 필요할 수밖에 없으며, 디지털위험에 대처하고 관련 위험을 최소화하기 위한 준비상태로서 위험관리의 중요성이 부각된다.

준비된 상태로서의 위험관리는 결국 위험을 어떻게 관리할 것인가의 문제이다. 즉, 위해요인에 대해 인식하도록 하고, 그에 대하여 의사결정을 하도록 도와주며, 그에 따라 적절한 통제 혹은 완화전략들을 실천에 옮기도록 도와주는 활동[4]이 필요한 것이다. 다만, 디지털위험의 경우에 고도의 기술자체에서 파생되는 위험이므로 기술만을 통해 관련 위험을 해결하는 것만으로는 부족하다. 즉, 기술의 야누스적 특성을 고려할 때, 기술 자체가 고도화될수록 관련 위험 또한 고도화되는 특성을 보인다. 결국 디지털위험에 대한 위험관리는 기술적으로 해결하기보다는 디지털위험에 대한 위험성을 알리고, 안전문화 형성을 통해 개인과 사회의 인식 및 태도를 변화시켜야 효율적 예방이 가능하고 위험을 최소화할 수 있는 것이다.

2.2 위험관리 결정요인: 신뢰와 위험지각을 중심으로

현재의 시점에서 디지털위험에 대한 효과적 위험관리가 이루어지기 위해서는 디지털위험에 대한 개인 및 사회구성원들의 인식과 태도가 중요하며, 이를 가능하게 하는 기본적 요소가 바로 위험커뮤니케이션이다. 위험커뮤니케이션은 위험요인에 대해 인식을 공유하는 커뮤니케이션 과정으로서 위험주체들(정부, 연구자 등의 전문가집단, 언론, 일반시민) 간의 위험인지 및 위험행태, 위험관리, 위험수용 등에 대한 위험소통, 즉 상호작용을 기본 전제로 한다. 하지만 과학기술자들은 사회적 인식에 대해 관심이 약하고, 대중은 과학적 지식에 취약하며, 이로 인해 잦은 정보의 통제나 왜곡이 발생하고 결국 사회적 불신과 저항이라는 갈등양상으로 발전하곤 한다. 정보를 제공하는 경우에도 정보제공자의 목적을 위한 도구적 접근에 치중하고, 성실한 의사소통이 잘 이루어지지 않는다. 따라서 전반적인 커뮤니케이션의 실패로 나타나곤 한다. 이런 측면에서 커뮤니케이션 파워를 회복함으로서 모든 사람들이 정보에 자유롭게 접근하고, 의사결정과정이 투명하게 이루어질 수 있는 커뮤니케이션 환경,이 구축되어야 하는 것이다. 따라서 디지털위험을 최소화하고 예방하기 위해서는 기술적 접근뿐 아니라 원활한 위험소통을 위한 사회적 접근이 중요하고, 커뮤니케이션 회복을 통한 근본적인 대책과 사후처방이 필요하다

[8]. 결국 디지털위험에 대한 위험관리의 출발은 위험주체들 간의 위험커뮤니케이션을 통한 커뮤니케이션의 회복을 바탕으로 이루어져야 하는 것이다.

위험커뮤니케이션을 통한 위험관리의 기본전제는 신뢰(trust)이다. 이는 위험커뮤니케이션 자체가 위험주체 상호간의 신뢰를 바탕으로 열려 있는 커뮤니케이션을 기본 전제로 하고 있기 때문이다[9]. 1980년대 위험커뮤니케이션 연구는 공중과 전문가들을 연결시킴으로서 위험평가에 대한 공중과 전문가의 격차를 최소화하는데 초점을 두었으나, 1990년대 이후 위험커뮤니케이션 연구분야가 공중과 전문가의 격차를 줄이는데 부응하지 못하였고, 그 원인으로 신뢰에 대한 위험커뮤니케이션 연구분야의 관심부족이라는 비판이 부각되면서 신뢰는 위험관리 분야에서 매우 중요한 요소로 부상하고 있다[10]. 특히, 신뢰의 중요성은 사람들이 시간과 정보, 지식 등이 부족할 경우에 더욱 큰 영향을 발휘한다. 즉, 사람들은 특정 위험에 대해 판단할 수 있는 기준나 근거가 부족하거나 없을 경우에 대부분 신뢰에 의존하여 위험을 평가하는 경향이 있기 때문에 위험관리에 있어서 신뢰는 매우 중요한 영향요인으로 이해되고 있다. 기존의 연구들도 사람들이 특정 사고를 해석하고 평가하는데 있어 신뢰에 의존하는 경향이 많고, 운영 혹은 책임 기관(사람)에 대한 신뢰 여부가 위험을 지각하는데 중요한 영향을 미친다고 보고[11, 12, 13]하여 신뢰가 전반적인 위험관리와 밀접한 관련이 있음을 시사한다.

신뢰(trust)는 타인의 의도 혹은 행위에 대한 긍정적 기대에 기반 한 것으로 취약성을 수용하려는 의도가 포함된 심리적 상태를 의미한다[14, 15]. 이런 신뢰는 특정 위험과 관련된 주요 의사결정을 내리는 과정에서 정책을 수행하는 책임자들을 믿고, 의존하는 것을 포함한다[16]. 그러므로 특정 위험을 책임지고 관리하는 사람들에 대해 높은 신뢰를 가질 경우에 사람들은 관련 위험을 낮게 지각하는 경향을 보이는 것으로 보고된다[17, 18]. 이에 따라 신뢰는 위험지각을 효율적으로 제어하고 통제할 수 있는 요인으로서, 전반적으로 위험을 평가, 관리하고 그 수용성 여부를 결정하는 핵심요인으로 볼 수 있는 것이다. 하지만 신뢰는 단기간에 걸쳐 형성되는 것이 아니라 오랜 기간에 걸쳐 점진적으로 형성된다. 또한 단 한 번의 실수나 사고로 인해 그 동안 쌓아왔던 신뢰가 순식간에 무너지기도 한다. 한번 신뢰를 잃으면 이전의 수준으로 다시 돌아가기 힘들며, 때로는 이전의 수준으로 회복 자체가 불가능하다는 특성을 띤다[12, 18]. 따라서 위험커뮤니케이션을 통한 효과적인 위험관리가 이루어지기 위해서는 다른 상황에 놓여 있는 다양한 사람들에게 위험에 대한 이해를 높이고, 실제사실을 평가함은 물론 정확하고 객관적인 정보제공을 통해 위험주체 간에 상호 신뢰가 형성될 수 있도록 해야 하는 것이다.

일반 공중들과 비교하여 전문가들은 특정 위험에 대해 잠정적인 위해와 혜택, 과학적 지식 등 다양한 요인들을 고려하여 최종적으로 위험을 지각하고 평가한다[19]. 다만, 전문가들도 자신과 관련된 영역이 아닐 경우에는 관련 위험에 대한 종합적 해석을 내리는데 어려움을 겪기 때문에 위험을 책임지고 관리하는 전문가 집단에 대한 신뢰의 여부에 따라 전반적인 위험지각 및 위험관리 그리고 수용여부를 결정한다[16, 18, 20, 21]. 전술한 바와 같이, 대부분의 사람들은 특정 위험에 대한 지식이 부족한 상황에서 자신의 의사나 행동을 결정해야 하는 상황에 직면할 경우에 신뢰라는 자원을 통해 행동을 포함한 최종 의사결정을 내리는 경향이 있다. 전문가들 역시 어떤 위험을 판단하고 평가하는데 있어서 구체적인 평가자원이 없을 경우에는 해당 위험을 관리하는 조직들에 대한 신뢰 여부를 통해 위험을 지각하고, 관련 조직들의 위험관리가 효과적으로 이루어지고 있는지를 평가한다. 이런 측면에서 신뢰는 디지털위험에 대한 위험지각과 효율적인 위험관리에 대한 인식을 결정하는 중요한 요인으로 판단된다. 이상의 논의를 통해 디지털위험 역시 신뢰가 위험지각이나 위험관리에 중요한 영향을 미칠 것으로 판단되며, 다음과 같은 연구가설을 설정하였다.

연구가설 1. 전문가들의 정부, 관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰가 높을수록 디지털위험에 대한 위험지각은 낮아질 것이다.

연구가설 2. 전문가들의 정부, 관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰가 높을수록 디지털위험에 대한 위험관리 인식도 높아질 것이다.

한편, 위험지각은 어떤 사건이나 행위, 혹은 기술의 불확실성과 관련된 신호를 수집하고 해석하는 과정으로서, 위험은 인간의 감각에 의해 지각될 수 없으며, 실제 현상의 이미지를 통해 형성된다. 개인의 위험판단과 관련된 정신모델과 심리학적 메커니즘은 위험 자체가 사회적, 문화적 학습을 통해 내면화되며, 미디어나 주변 사람들, 혹은 또 다른 커뮤니케이션 과정을 통해 중재됨을 강조한다[22, 23]. 이에 따라 위험지각은 사람들마다 위험유형, 위험상황, 개인적 특성과 사회적 콘텍스트 등에 따라 다르게 나타나며, 지식이나 경험, 가치, 태도, 그리고 감

정 등과 관련된 요인들이 위험의 심각성이나 수용성에 대한 개인적 사고 및 판단에 영향을 미치는 것으로 보고된다[24]. 특정 위험대상에 대한 위험지각은 정보출처를 신뢰하지 못하거나 우리사회 내에 관련 위험에 대한 정보 혹은 피드백이 부족할 때 발생한다[1]. 즉, 위험소통이 제대로 이루어지지 않고 있기 때문에 위험관리가 효과적으로 이루어지고 있는가에 대한 판단 기준이 부족하고, 결과적으로 위험관리가 제대로 이루어지고 있는가에 대한 의무과 불신이 형성되는 것이다. 이에 따라 특정 위험에 대한 객관적인 정보제공과 그에 따른 피드백, 다시 말해서 위험소통은 개인들의 의사결정과정에 대한 참여를 촉진함으로서 위험에 관한 의사결정이나 정책결정이 적합하게 이루어지고 있는지를 평가하고, 상호 신뢰를 바탕으로 위험관리가 협의, 수정을 통해 효율적으로 이루어지고 있는가에 대한 인식 형성에 영향을 미치게 되는 것이다. 결국 특정위험에 대한 과학적이고 올바른 정보의 공유는 위험요소를 제거하는데 필요한 합리적 방안을 도출하기 위한 위험관리의 단계이자 해결방법을 사회적으로 이끌어내기 위한 위험관리 전략이라고 볼 수 있다[4]. 따라서 위험지각이 결과적으로 위험소통이 부족할 때 발생한다는 점을 기본전제로 한다면, 위험커뮤니케이션 차원에서 디지털위험에 대한 높은 위험지각은 위험관리에 부정적 영향을 미칠 것으로 판단되며, 이에 따라 다음과 같은 연구가설을 설정하였다.

연구가설 3. 전문가들의 디지털위험에 대한 위험지각은 위험관리 인식에 부정적 영향을 미칠 것이다.

3. 연구방법

3.1 조사대상

본 연구의 조사대상자는 디지털위험 관련 전문가들이 가질 수 있는 편향성을 고려하여 우리사회 내에서 비교적 전문지식을 갖추고 있다고 판단되는 집단을 추출하여 설문조사를 실시하였다. 전문가 집단의 추출은 위험커뮤니케이션 측면에서 고려되었는데, 위험커뮤니케이션 연구영역에서는 정부와 학계(교수 및 연구원), 언론, 시민단체, 기업 간의 투명한 위험소통을 통해 상의 및 협의하고, 나아가 참여를 통한 의사결정을 강조하고 있다. 이에 근거하여 본 연구에서는 전문가 집단으로서 정부소속 관리, 교수 및 연구원, 그리고 언론영역 소속 기자들을 전문가 집단으로 설정하였다. 다만, 전문적 지식을 고려하여 시민단체와 개인은 제외하였다. 이에 따라 온라인 전문조사 업체에 의뢰하여 설문조사를 실시, 최종적으로 212부의 자료를 분석에 활용하였다. 조사대상자의 주요 특성을 보면, 성별은 남성이 145명(68.4%), 여성 67명(31.6%), 전문가 분포는 정부소속 관리가 54명(25.5%), 교수 및 연구원 141명(68.4%), 언론인이 17명(8.0%)으로 나타났다.

3.2 측정도구

3.2.1 신뢰

본 연구에서 신뢰는 디지털위험 관리조직에 대한 신뢰를 의미하는 것으로, 디지털위험 관련 정보를 제공하는 것은 물론 관련 위험을 직·간접적으로 관리하는 정부, 디지털관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰를 측정하였다. 이런 분류는 Knight(2007)가 바이테크놀로지 위험관리조직으로 분류한 것에 근거하였으며, 신뢰 문항 역시 Knight(2007)가 사용한 문항을 통해 측정하였다[25]. 이 문항은 각각의 위험관리조직에 대해 신뢰를 개별적으로 측정하도록 되어 있으며, 본 연구에서도 정부, 디지털관련 과학자그룹(기술자 포함), 언론, 시민단체, 기업에 대한 신뢰를 개별적으로 측정하였다. 이에 따라 본 연구에서 신뢰 측정은 총 5문항을 통해 이루어졌으며, 각 문항은 5점 척도(1점: 전혀 신뢰하지 않음, 5점: 매우 신뢰함)로 측정, 점수가 높을수록 신뢰가 높은 것으로 해석한다.

3.2.2 위험지각

본 연구에서 위험지각 측정은 Song(2014)이 사용한 위험지각 척도를 이용하였다[26]. 이 척도는 특정 위험대상에 대해 사회적 측면과 개인적 측면(자신/가족)에서 위험지각을 측정하도록 구성되어 있으며, 총 2문항으로 구성되어 있다. 본 연구에서는 디지털위험으로서 인포테믹스, 사이버폭력, 정보유출, 해킹, 개인감시/통제에 대해 각각 위험지각을 측정하였으며, 위험지각을 측정하기 위해 사용된 총 문항은 10문항이었다. 각 문항은 11점 척도(0점: 전혀 위험하지 않음, 10점: 매우 위험함)로 측정하였고, 점수가 높을수록 해당 디지털위험에 대한 위험을 높게 지각하는 것으로 해석한다.

3.2.3 위험관리 인식

본 연구에서 위험관리는 송해룡과 조항민, 이윤경, 김원제(2012)에 근거하여 디지털위험과 관련하여 평소 위

험예방 활동과 위험발생 시 대응, 그리고 위험예방 활동에 대한 믿음과 신뢰로 규정하고 정부, 디지털관련 과학자그룹, 언론, 시민단체, 기업에 대한 위험관리 인식을 측정하였다[8]. 이에 본 연구에서 정부, 디지털관련 과학자그룹, 언론, 시민단체, 기업에 대해 개별적으로 3문항을 적용, 총 15문항을 통해 위험관리가 효율적으로 이루어지고 있는지에 대한 인식을 측정하였다. 각 문항은 5점 척도(1점: 전혀 동의하지 않음, 5점: 매우 동의함)로 측정, 점수가 높을수록 위험관리가 효율적으로 이루어지고 있는 것으로 해석한다.

4. 연구결과

4.1 기술통계 및 상관관계 분석

전문가들의 디지털위험 관리조직에 대한 신뢰, 디지털위험인 인포데믹스, 사이버폭력, 정보유출, 해킹, 개인감시 및 통제에 대한 위험지각, 그리고 디지털위험 관리조직에 대한 위험관리 인식에 대해 기술통계분석을 수행하였다. 신뢰를 살펴보면 전문가들은 디지털위험 관리조직에 있어 과학자그룹(M=2.85)에 대한 신뢰가 가장 높았던 반면에 기업(M=2.21)과 정부(M=2.24)에 대한 신뢰는 낮은 것으로 나타났다. 디지털위험에 대한 위험지각은 정보유출(M=8.36)이 가장 높았고, 그 다음으로 해킹(M=8.02), 개인감시 및 통제(M=7.94), 사이버폭력(M=7.82), 인포데믹스(M=7.04) 순이었으며, 위험관리는 과학자그룹(M=2.64), 시민단체(M=2.58), 언론(M=2.18), 기업(M=2.16), 정부(M=2.13) 순으로 나타났다.

(표 1) 기술통계 분석
(Table 1) Descriptive Statistics Analysis

	세부위험	M	SD	통합
신뢰	정부	2.24	.93	2.44(.67)
	과학자	2.85	.87	
	언론	2.28	.94	
	시민단체	2.62	.84	
	기업	2.21	.89	
위험지각	인포데믹스	7.04	1.95	7.84(1.50)
	사이버폭력	7.82	1.80	
	정보유출	8.36	1.62	
	해킹	8.02	1.71	
	개인감시/통제	7.94	1.73	
위험관리	정부	2.13	.83	2.34(.53)
	과학자	2.64	.68	
	언론	2.18	.72	
	시민단체	2.58	.70	
	기업	2.16	.77	

한편, 디지털위험 관리조직에 대한 신뢰와 디지털위험에 대한 위험지각, 그리고 위험관리 인식 간의 상관관계를 살펴보기 위하여 상관관계 분석을 수행하였다. 그 결과 신뢰는 위험지각(r=-.37, p<.01)과 부적 상관을 보였으며, 위험관리(r=.62, p<.01)와는 정적 상관을 보였고, 위험지각의 경우에는 위험관리(r=-.34, p<.01)와 부적 상관을 보인 것으로 확인되었다.

(표 2) 상관관계 분석
(Table 2) Correlation Analysis

	신뢰	위험지각	위험관리
신뢰	-		
위험지각	-.37**	-	
위험관리	.62**	-.34**	-

** p<.01

4.2 가설검증

4.2.1 모델적합도

본 연구에서 설정한 모형의 적합도를 확인하기 위해서 절대적합지수(Normed χ2, RMSEA, GFI)와 증분적합지수(IFI, TLI, CFI)를 활용하였다. 모형의 적합도가 충족되기 위해서는 일정한 요건을 갖추어야 하는데, Normed χ2는 3.00 이하, RMSEA는 .08 이하, GFI와 IFI, TLI, CFI는 .90 이상일 때, 적합기준을 충족한 것으로 보고, 모형의 타당도가 있는 것으로 평가한다[27]. 이러한 기준을 적용하여 디지털위험관리조직에 대한 신뢰와 위험지각, 그리고 위험관리 인식의 모형 적합도를 살펴본 결과, Normed χ2=2.16, RMSEA=.07, GFI=.90, IFI=.94, TLI=.92, CFI=.94로 나타나 모든 적합지수가 적합기준을 충족한 것으로 확인되었다. 따라서 본 연구에서 설정한 모형이 비교적 양호한 모델인 것으로 평가할 수 있다.

4.2.2 경로분석

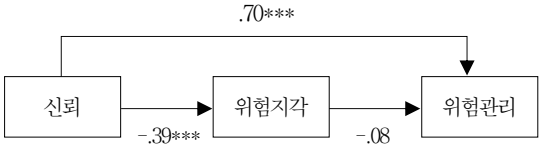
현재 한국사회에서 발생하고 있는 디지털위험과 관련하여 다양한 영역의 전문지식을 갖춘 전문가들을 대상으로 디지털위험을 관리하는 조직으로서 정부, 관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰가 디지털위험에 대한 위험지각, 그리고 이들 조직의 위험관리에 대한 인식에 미치는 영향을 경로분석을 통해 살펴보았다. 주요 결과를 보면, 우선 디지털위험을 관리하는 조직에 대

한 신뢰가 디지털위험에 대한 위험지각에 미치는 영향을 살펴본 결과, 신뢰는 위험지각에 대해 β=-.39(t=-4.87, p<.001)로 통계적으로 유의한 부적(-) 영향을 미치는 것으로 나타나 연구가설 1은 채택되었다. 따라서 전문가들의 디지털위험 관리조직에 대한 신뢰가 높을수록 디지털위험에 대한 위험지각은 감소하는 것으로 평가할 수 있다. 디지털위험을 관리하는 조직에 대한 신뢰가 위험관리에 미치는 영향을 살펴본 결과, 신뢰는 위험관리 인식에 대해 β=.70(t=5.77, p<.001)으로 통계적으로 유의한 정적(+) 영향을 미치는 것으로 나타나 연구가설 2 역시 채택되었다. 그러므로 전문가들의 디지털위험 관리조직에 대한 신뢰가 높을수록 위험관리가 효율적으로 이루어지고 있다는 인식도 높아지는 것으로 볼 수 있다. 마지막으로 디지털위험에 대한 위험지각이 위험관리에 미치는 영향을 살펴본 결과, 위험지각은 위험관리 인식에 대해 β=-.08(t=-1.23, p>.05)로 통계적으로 유위한 영향을 미치지 못한 것으로 확인되어 연구가설 3은 기각되었다.

(표 3) 경로분석 결과
(Table 3) Path analysis

	표준 경로 계수	표준 오차	t
신뢰 → 위험지각	-.39	.19	-4.87***
신뢰 → 위험관리	.70	.09	5.77***
위험지각 → 위험관리	-.08	.02	-1.23

*** p<.001



(그림 1) 경로모형
(Figure 1) Path model

5. 결 론

본 연구는 전문가들을 대상으로 한국사회에서 발생하고 있는 디지털위험과 관련, 디지털위험을 관리하는 조직에 대한 신뢰가 위험지각과 위험관리 인식에 미치는 영향을 규명하였다.

먼저 디지털위험을 관리하는 조직에 대한 신뢰가 위험지각에 미치는 영향을 살펴보았다. 그 결과 전문가들이 디지털위험을 관리하는 조직인 정부, 관련 과학자그룹, 언론, 시민단체, 기업에 대한 신뢰가 높을수록 위험지각은 상대적으로 낮아지는 것으로 나타나 연구가설 1은 지지되었다. 이러한 결과는 특정 위험을 책임지고 관리하는 사람들에 대한 신뢰가 높을수록 관련 위험을 낮게 지각한다고 보고한 선행연구들의 결과[17, 18]와 일치하는 것으로서 전문가의 디지털위험 관리조직에 대한 신뢰가 디지털위험에 대한 위험지각을 낮추는 결정요인임을 시사한다.

둘째, 디지털위험을 관리하는 조직에 대한 신뢰가 위험관리 인식에 미치는 영향을 살펴보았다. 그 결과, 전문가들이 디지털위험을 관리하는 조직에 대해 높은 신뢰를 가질수록 관련 위험에 대한 관리가 효율적으로 이루어지고 있다고 인식하는 경향이 있는 것으로 나타나 연구가설 2 역시 지지되었다. 이러한 결과는 위험을 책임지고 관리하는 조직에 대한 신뢰의 여부에 따라 위험관리 및 위험수용이 결정된다고 보고한 선행연구들[20, 21]의 결과를 뒷받침하는 것으로서 신뢰가 위험관리를 평가하는 핵심 요인임을 시사한다.

셋째, 디지털위험에 대한 위험지각이 위험관리 인식에 미치는 영향을 살펴본 결과, 위험지각은 위험관리 인식에 통계적으로 유의한 영향을 미치지 못하였다. 이런 결과는 위험지각이 위험소통의 부족이나 결여로 인해 발생하고, 효율적인 위험소통은 신뢰를 기반으로 위험관련 의사결정과정에 대한 참여를 촉진, 결과적으로 효율적인 위험관리가 이루어질 수 있도록 하는데 영향을 미친다는 점[4]을 고려한 것이었으나, 연구가설 3은 지지되지 않았다. 이에 대해서는 다양한 원인이 있겠으나, 우선은 본 연구에서 설정한 디지털위험(인포데믹스, 사이버폭력, 정보유출, 해킹, 개인감시/통제)에 대한 위험관리가 관리하고자 하는 대상에 따라 다르게 나타날 수 있으며, 일반적 수준에서 위험관리가 관리하는 대상에 대한 통제가능성[4]을 전제로 한다는 점을 고려할 때, 아직 우리사회에서 기술적으로나 문화적으로 관련 디지털위험을 효과적으로 관리하기가 쉽지 않다는 인식이 본 연구의 결과에 일정 부분 영향을 미친 것으로 사료된다. 이상의 결과가 의미하는 바는 전문가들 역시 디지털위험을 지각하고 위험관리가 효율적으로 이루어지고 있는가의 여부를 평가하는데 있어서 신뢰를 매우 중요한 자원으로 활용하고 있음을 시사하며, 디지털위험을 효과적으로 관리하고 통제하기 위해서는 무엇보다 신뢰에 기초한 위험커뮤니케이션이 효율적으로 이루어져야 함을 보여준다.

참 고 문 헌 (Reference)

[1] M. R. Greenberg, and K. Lowrie, “From the Very Public to the Less Known,” Risk Analysis, Vol.29, No.2, 2009, pp.157-158.

[2] Young-Ai Lee, and Na-Keung Lee, “Psychological Dimensions of Risk Perception for the Korean,” PMORP Workshop, 2005, pp.1-12. http://www.riss.kr/search/download/FullTextDownload.do?control_no=4812c62a746d512fffe0bdc3ef48d419&p_mat_type=1a0202e37d52c72d&p_submat_type=&fulltext_kind=&t_gubun=undefined&DDODFlag=&redirectURL=%2Fsearch%2Fdownload%2FFullTextDownload.do&loginFlag=0&url_type=&query=Psychological+Dimensions+of+Risk+Perception+for+the+Korean

[3] Hang-Min Cho, “Introduction of Digital Media and Consequent New Risk Types: Focus on the Analysis of User Risk Perception and Risk Features of Smart Phones as Convergence Media”, The Journal of Korea Contents, Vol.11, No.8, 2011, pp.353-364. http://www.dbpia.co.kr/Journal/ArticleDetail/1509670

[4] Bo-yun, Seo, “A Study on the Risk Communication in Digital Society”, Doctoral Dissertation, The Graduate School of Chung-Ang University.

[5] C. Roth and M. Siegrist, “Cyber Threat in the Field CIP: Trust and Perception”, CRN: Zurich, Univ. of Zurich, 2001.

[6] Dong-Kyoo Sung, Doo-hee Kim, Yoon-Suk Lee, and Seong-Won Lim, “A Study on the Cyber-Violence Induction Factors of Teenagers: Focused on Individual Inclination, Cyber Violence Damage Experience, and Moral Consciousness,” Journal of Cybercommunication Academic Society, No.19, 2006, pp.79-129. http://www.dbpia.co.kr/Journal/ArticleDetail/886168

[7] Cyber Bureau, 2015, http://www.netan.go.kr/prevention/sub2.jsp?mid=010201

[8] Hae-Ryong Song, Hang-Min Cho, Yoon-Kyung Lee, and Won-Je Kim, “A Study on the Conceptualization, Structural Analysis and Domain Establishment of Risk Communication,” Dispute Resolution Studies Review, Vol.10, No.1, 2012, pp.65-100.

[9] V. T. Covello, D. McCallum, and M. T. Pavolva, “Effective Risk Communication”, New York: London, 1989.

[10] Hae-Ryong Song, Won-Je Kim, and Chan-Won Kim, “A Study on Public’s Credibility, Risk Perception and Effectiveness of Nuclear Power Plant”, Korean Review of Crisis & Emergency Management, Vol.11, No.4, 2005, pp.123-140, http://www.earticle.net/Article.aspx?sn=247480

[11] T. C. Earle and M. Siegrist, “Morality Information, Performance Information, and the Distinction between Trust and Confidence”, Journal of Applied Social Psychology, Vol.36, 2006, pp.383-416. http://onlinelibrary.wiley.com/doi/10.1111/j.0021-9029.2006.00012.x/abstract;jsessionid=7331D2274E7B7F81ABE504CA08CE066E.f03t02?userIsAuthenticated=false&deniedAccessCustomisedMessage=false

[12] P. Slovic, “Perceived Risk, Trust and Democracy,” Risk Analysis, Vol.13, No.6, 1993, pp.675-682. http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.1993.tb01329.x/abstract

[13] V. H. M. Visshcers and M. Siegrist, “How a Nuclear Power Plant Accident Influence Acceptance of Nuclear Power: Results of Longitudinal Study Before and After the Fukushima Disaster”, Risk Analysis, Vol.33, 2013, pp.333-347. http://www.ncbi.nlm.nih.gov/pubmed/22762151

[14] T. C. Earle, “Trust in Risk Management: A Model-Based Review of Empirical Research,” Risk Analysis, Vol.30, No.4, 2010, pp.541-574. http://www.ncbi.nlm.nih.gov/pubmed/20522197

[15] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not so different after all: A Cross-Discipline View of Trust,” Academy of Management Review, Vol.23, 1998, pp.393-404. http://amr.aom.org/content/23/3/393.short

[16] M. Siegrist, and G. Cvetkovich, “Perception of Hazards: The Role of Social Trust and Knowledge,” Risk Analysis, Vol.20, 2000, pp.713-719. http://www.ncbi.nlm.nih.gov/pubmed/11110217

[17] M. Siegrist, “The Influence of Trust and Perception of Risk and Benefits on the Acceptance of Gene Technology,” Risk Analysis, Vol.20, 2000, pp.195-204. http://www.ncbi.nlm.nih.gov/pubmed/10859780

[18] Young-Ai Lee, and Hea-Sook Lim, “The Effects of Trust and World views on Risk Perception,” PMORP Workshop, 2005, pp.13-26.

[19] Hea-Sook Lim, and Young-Ai Lee, “The Public Perception of Risk from Gene Technology,” PMORP Workshop, 2005, pp.47-60.
http://www.riss.kr/search/download/FullTextDownload.do?control_no=ec2c5ada88498d25ffe0bdc3ef48d419&p_mat_type=1a0202e37d52c72d&p_submat_type=&fulltext_kind=&t_gubun=undefined&DDODFlag=&redirectURL=%2Fsearch%2Fdownload%2FFullTextDownload.do&loginFlag=0&url_type=&query=The+Public+Perception+of+Risk+from+Gene+Technology

[20] G. Cvetkovich, “The Attribution of Social Trust,” In G. Cvetkovich and R. Lofstedt (Eds.), Social Trust and the Management of Risk. London: Earthscan, 1999.

[21] M. Siegrist, G. T. Cvetkovich, and C. Roth, “Salient Value Similarity, Social Trust, and Risk/Benefit Perception,” Risk Analysis, Vol.20, No.3, 2000, pp.353-362.
http://onlinelibrary.wiley.com/doi/10.1111/0272-4332.203034/abstract

[22] M. G. Morgan, B. Fischhoff, A. Bostrom, and A. Atman, “Risk Communications: A Models Approach,” Cambridge, MA: Cambridge University Press, 2001.

[23] P. Slovic, “Perception of risk,” Science, Vol.236, 1987, pp.280-285.

[24] G. Wachinger, O. Renn, C. Begg, and C. Kuhlicke, “The Risk Perception Paradox: Implications for Governance and Communication of Natural Hazards,” Risk Analysis, Vol.33, No.6, 2013, pp.1049-1065.
http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2012.01942.x/abstract

[25] A. Knight, “Intervening Effects of Knowledge, Morality, Trust and Benefits on Support for Animal and Plant Biotechnology Applications,” Risk Analysis, Vol.27, No.6, 2007, pp.1553-1563.
http://www.ncbi.nlm.nih.gov/pubmed/18093052

[26] G. Song, “Understanding Public Perception of Benefits and Risk of Childhood Vaccinations in the United States,” Risk Analysis, Vol.34, No.3, 2014, pp.410-426.
http://www.ncbi.nlm.nih.gov/pubmed/24033739

[27] Hak-Sik Lee and Ji-Hoon Lim, “Structural Equation Model Analysis and Amos 20.0,” Seoul: JypHyuJae Publishing Co, 2013.

◐ 저 자 소 개 ◑

김 원 제 (Won-je Kim)
1993년 원광대학교 신문방송학과(정치학사)
1999년 중앙대학교 대학원 신문학과(언론학석사)
2005년 성균관대학교 대학원 신문방송학과(언론학박사)
2011～현재 성균관대학교 사회과학부 겸임교수
관심분야 : 위험커뮤니케이션, 디지털미디어 등
E-mail : wonje5@daum.net

김 찬 원 (Chan-won Kim)
1997년 광주대학교 법학과(법학사)
2000년 중앙대학교 대학원 신문방송학과(정치학석사)
2007년 중앙대학교 대학원 신문방송학과(언론학박사)
2013~현재 성균관대학교 SSK 위험커뮤니케이션 연구단 전임연구원 및 사회과학부 겸임교수
관심분야 : 위험커뮤니케이션, 위험심리, 미디어심리 등
E-mail : ares6357@naver.com