개인정보 유출의 통제가능성 인지가 정서 및 행동의지에 미치는 영향: 외부해킹과 내부유출 비교를 중심으로

위초롱(주저자)
㈜씨에이에스
(wclong91@naver.com)
권순동(교신저자)
충북대학교 경영정보학과 교수
(sdkwon@cbnu.ac.kr)

지금까지 경영정보나 정보보호 분야의 연구는 보안기술이나 정책 등 인간의 합리성을 중시하는 이성적 측면에 초점이 맞춰졌다. 따라서 개인정보 유출 등의 사고나 서비스 실패로 인해 고객들이 느끼는 실망감이나 배신감과 같은 정서적 측면의 연구는 합리성에 밀려 주목을 받지 못했다. 이렇다 보니 개인정보 유출 사고에 대한 기업 대응은 고객의 마음을 충족시키지 못하고, 서비스 회복에 효과적이지 못했다. 따라서 본 연구에서는 그동안 심리학 및 마케팅 분야에서 연구된 인지→정서→의지의 이론을 개인정보 유출 상황에 적용하여 유출원인의 인지에 따른 정서적 반응과 그로 인한 행동의지의 영향관계를 규명하였다. 본 연구의 모형은 개인정보 유출사고의 사전 통제가능성 인지가 정서에 영향을 미치고 나아가 행동의지에 영향을 미친다는 것이다. 그리고 내부유출 및 외부해킹의 원인소재에 따라 이러한 영향은 달라진다는 것이다.
본 연구를 위해 개인정보 유출 경험이 있는 사람들을 대상으로 설문조사를 실시하였다. 설문조사에서는 개인정보 유출의 원인을 외부해킹과 내부유출로 구분하여 가상의 시나리오를 제시하였고, 각 시나리오에 따라 통제가능성 인지, 정서, 행동의지에 대해 응답하도록 하였다. 최종적으로 460개의 데이터가 수집되었고, 연구모형을 검증하기 위해 Smart-PLS 2.0 통계 분석도구를 이용하였다.
본 연구모형을 데이터 분석을 통해 검증한 결과는 다음과 같다. 첫째, 개인정보 유출사고에 대한 사전 통제가능성 인지 수준이 높을수록 실망감과 배신감의 정서를 더 많이 유발하고, 이렇게 유발된 정서는 경쟁사로의 서비스 전환과 부정적 구전의 행동의지를 더 높게 유발한다는 것이다. 둘째, 외부해킹에 의해 개인정보가 유출될 경우에는 통제가능성 인지로 인해 실망감이 유발되고 이것은 부정적 구전의도에 영향을 미친다는 것이다. 셋째, 내부자에 의해 개인정보가 유출될 경우에는 통제가능성 인지를 통해 배신감이 유발되고 서비스 전환 의도가 높아진다는 것이다.
본 연구의 의의는 학술적 측면과 경영관리적 측면에서 살펴볼 수 있다. 먼저, 학술적 의의는 지금까지 보안 및 개인정보 보호 관련 연구들이 인지→행동의지의 관계에 초점을 두어 설명하였던 것에 비해, 본 연구에서는 인지→정서→의지의 심리 이론을 개인정보 유출 상황에 적용하여 종전보다 설명력을 더 높였다는 점이다. 즉, 종전의 이성적 측면을 강조한 보안 분야의 연구에 배신감과 실망감의 정서적 측면을 추가함으로써 설명력과 행동의 예측력을 높였다는 점이다.
경영관리적 의의는 기존 연구에서 다루지 않았던 외부해킹 및 내부유출의 원인소재에 초점을 두어 차이를 규명함으로써 기업의 사고 대응책을 원인소재에 따라 차별화해야 함을 제시하였다는 점이다. 그리고 개인정보유출로 인한 고객의 부정적 행동이 외부해킹의 경우에는 실망감으로 인한 것이고, 내부유출의 경우에는 배신감에 의한 점을 규명함으로써 기업의 사후대책의 효과성을 높이는데 기여하였다는 점이다.
외부해킹에 의해 개인정보 유출 사고가 발생하면, 기업은 실망감을 낮추는데 초점을 맞출 필요가 있다. 예를 들어, 기업은 예방을 위한 각고의 노력을 해왔으나, 현실적으로 완벽한 예방은 어려운 일이고 유감스럽게도 사고가 발생했다는 식의 메시지 전달을 통해 고객의 기대를 낮추는 동시에 고객의 이해를 구할 필요가 있다. 아울러, 현재 기업에서 하고 있는 보안 활동을 명시하고, 앞으로 이를 어떻게 더 발전시킬 것인지를 보여주는, 즉, As-is와 To-be 계획에 관한 재발 방지 대책을 제시할 필요가 있다.
내부유출로 개인정보 유출 사고가 발생하면, 기업은 배신감을 낮추는데 초점을 맞출 필요가 있다. 예를 들어, 배신감을 치유하고 회복하기 위해 기업은 우선으로 겸허히 잘못을 인정하고 진정성 있는 사과를 해야 할 것이다. 또한, 시기적절하고 공정한 피해보상을 통해 공정성 회복 노력을 기울여야 할 것이다. 아울러, 기업 내부적으로는 윤리교육을 실시하고, 유출과 관련된 내부자를 엄정히 처벌하는 내적 인적 쇄신을 취할 필요가 있다.

주제어: 외부해킹, 내부유출, 통제가능성, 실망감, 배신감, 인지·정서·의지

최초투고일: 2017. 8. 16 게재확정일: 2017. 9. 14

Ⅰ. 서 론

전통적으로 경영정보나 정보보호 분야의 연구는 보안기술이나 정책 등 인간의 합리성을 중시하는 이성적 측면에 초점을 맞추어왔다. 따라서 개인정보 유출 등의 사고나 서비스 실패로 인해 고객들이 느끼는 실망감이나 배신감과 같은 정서적 측면의 연구는 거의 전무한 실정이다. 특히 배신감에 대한 연구는 경영학을 비롯한 여러 학문분야에서 아직까지 심층적으로 이루어지지 않고 있다. 이렇다 보니 개인정보 유출 사고에 대한 기업 대응은 고객의 마음을 충족시키지 못하고, 신뢰 회복을 더디게 만들고 있다. 개인정보 유출로 유발된 실망감이나 배신감은 서비스 이용 중지나 타사로의 전환, 또는 부정적 구전 등의 행동으로 연결될 수 있다. 따라서 개인정보 유출 사고와 같은 사건발생이 정서에 미치는 영향에 대한 정확한 이해와 그에 적합한 대응행동은 고객의 부정적 행동을 줄이고 신뢰를 회복하는데 매우 중요한 요인이라고 볼 수 있다.

본 연구는 개인정보 유출 원인별 통제가능성 인지에 따른 정서 유발과 그로 인한 행동의지의 전개과정을 규명하는데 초점을 맞추었다. 개인정보 유출사고에 대한 사전 통제가능성 인지는 실망감이나 배신감 등의 정서적 유발을 불러일으키고, 이것은 타사로의 서비스 전환이나 부정적 구전 행동에 영향을 미칠 수 있다는 것이다. 개인정보 유출 사고는 조직 내부자의 실수 또는 고의에 의해 발생할 수 있고, 조직 외부 전문가의 해킹에 의해 발생할 수도 있다. 본 연구에서는 이러한 내부유출과 외부해킹의 사고 원인에 대한 인지에 따라 정서유발이 다르고 결과적으로 행동도 다르게 나타난다는 것을 규명하였다. 본 연구는 개인정보 유출 사고에 대한 기업의 대응책 수립 및 추진에 매우 중요한 의미를 지닌다고 본다.

Ⅱ. 이론적 배경

2.1 개인정보 유출

최근 스마트기기의 보급과 사용이 늘면서 실시간으로 생성된 대용량 디지털 정보를 분석하여 새로운 부가가치를 창출하는 빅데이터(big data)가 주목받고 있다(산업연구원, 2014). 기업은 이렇게 수집된 개인정보를 활용해 시장기회를 포착하고 새로운 비즈니스 모델을 창출한다. 이 과정에서 개인정보유출과 프라이버시 침해의 문제가 발생할 수 있는데(배재권, 2016), 지난 1년간 자신의 개인정보가 침해된 경험의 이유로 46.7%가 개인정보 유출을 뽑았다(개인정보보호위원회, 2015). 개인정보 유출의 원인은 크게 외부해킹과 내부유출로 나눌 수 있다. 기업 및 기관이 당하는 보안 사고를 분석한 결과, 외부 해킹에 의한 유출은 전체 사고의 9.7%이고, 사고 한 건당 49만 3000달러의 비용이 소요되는 것으로 나타났다. 반면에, 내부유출은 전체 사고의 21.8%를 차지하며, 사고 한 건당 77만 6000달러의 비용이 발생한다고 조사되었다(Ponemon Institute, 2016). 이렇듯 통상적으로 내부자에 의한 개인정보유출일 때, 피해의 규모와 심각성이 더욱 크다. 이에 정부는 '징벌적 손해배상제'를 도입하였고, 기업은 내부 유출 예방 솔루션을 도입하여 내부자 유출을 막고자 노력하고 있다(한국정보보호산업협회, 2015).

〈Table 1〉 Personal Information Leakage from Korea

Cause	Year	Company	Scale (unit: million)
External Hacking	2014	KT	1,200
	2014	Neungyule	105
	2016	Interpark	1,030
Internal Leakage	2014	KB, Lotte, Nonghyupcard	10,400
	2014	Lottemart	250
	2015	Samsung, Shinhan, Hyundai card	740

2.1.1 개인정보 유출의 개념 및 현황

개인정보 유출은 "법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보 처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것"을 말한다(표준 개인정보 보호지침 제25조). 다시 말해 고객의 동의 없이 고객의 개인정보가 유출되는 것이다. 현재 개인정보 유출은 지속적으로 발생하고 있으며, 그 규모가 점점 대형화되는 추세이다. 세계적으로 2015년 1회 1,000만 건 이상의 개인정보가 유출된 대형 보안사고가 9차례 발생했으며, 이 때 유출된 개인정보는 4억 2,900만 건으로 전년 대비 23% 증가했다(Symantec Corporation, 2016). 국내에서도 상황은 마찬가지이다. 2014년 발생한 신용카드 3사의 개인정보 유출로 총 1억 400만 건의 개인정보가 유출되었다. 이는 우리나라 경제활동인구 중 약 58%의 개인정보가 유출된 것으로(산업연구원, 2014), 이는 세계 3위에 해당하는 대규모의 유출 사고였다. 〈Table 1〉은 2014년 이후 국내에서 발생한 개인정보 유출 중 일부를 유출 원인별로 구분한 것이다. 유출 원인은 크게 2가지, 즉 외부해킹과 내부유출로 구분할 수 있다. 외부해킹은 외부자(해커)가 홈페이지, 이메일 등을 대상으로 하여, 해킹 등의 방법으로 개인정보를 탈취하여 유출시키는 것을 말하고, 내부유출은 기업의 내부자(개인정보 취급자, 개인정보 처리자, 협력업체 직원 등)가 자신의 경제적 이익 취득 등을 목적으로 개인정보를 외부로 유출시키는 것을 말한다.

2.1.2 개인정보 유출 관련 선행연구

개인정보 유출이 지속적으로 발생하면서 개인정보 보호에 대한 관심이 높아지고 있고, 이에 대한 다양한 연구가 진행되고 있다. 이러한 연구들은 주로 개인의 인식 및 행동에 초점을 두고 있다. 장익진과 최병구(2014)는 인지된 위험과 효능감에 의해 그룹을 분류하고, 각 그룹별 개인정보 유출예방과 관련된 보호동기, 정보탐색, 예방활동의 차이를 규명하였다. 윤일한과 권순동(2015)은 금융정보보안 컴플라이언스와 관련주체의 위기대응, 금융정보보안 신뢰의 영향관계를 실증하였다. 여기서는 금융신뢰회복을 위한 각 관련 주체의 행동에 대해 사전대응과 사후대응, 개인정보 유출자의 관점으로 나누어 연구하였다. 임규목과 부경희(2015)는 개인정보 유출 시 커뮤니케이션 전략과 수용자의 보복욕구 및 행동의 인과관계를 탐색하였다. 이외에도 보호기술 및 관리에 초점을 둔 연구, 경제적 비용이나 법적·제도적 장치에 초점을 둔 연구 등이 진행되었다. 이처럼 개인정보 유출 관련 선행연구들은 인식 및 행동에 초점을 맞추었다. 그러나 아쉽게도 인간의 감정이나 정서에 초점은 맞춘 연구는 거의 진행되지 않았다. 뿐만 아니라 개인정보 유출의 원인에 따른 영향을 다

룬 연구도 거의 진행되지 않았다. 따라서 본 연구에서는 개인정보 유출의 원인과 그로 인한 정서유발에 초점을 맞추어 연구를 수행하였다.

2.2 인지, 정서, 의지

본 연구에서는 개인정보 유출 상황에서 개인의 심리에 대한 적절한 이해와 조직의 효과적인 대처법을 도출하기 위해 그동안 주로 심리학에서 연구되어 온 인지(cognition), 정서(affection), 의지(conation)의 세 차원(tripartite model)에서 접근하였다. 심리치료 및 심리상담기법에서 널리 사용되고 있는 인지·정서·행동치료(Rational Emotive Behavioral Therapy)이론에서는 인간의 신념이 정서와 행동에 영향을 미친다고 보고 있다(Ellis, 1994). 신경생리학에서는 인지에 의해 정서가 유발되고 정서에 의해 의지가 형성된다고 보고 있다(Damasio, 2000). 마케팅 분야에서는 인지, 정서, 의지의 세 조합을 통해 인간의 행동이 나타난다고 보고 있고(Rosenberg and Hovland, 1960), 소비자 행동 분야에서는 태도(attitude)가 인지, 정서, 의지의 세 요소로 구성되는데(Fishbein and Ajzen, 1975), 인지 → 정서 → 의지의 단계를 따라 충성도가 형성된다고 보고 있다(Oliver, 1999). 최근에는 정보시스템 분야에서도 지·정·의(知情意) 관점에서 IT 도입에 따른 조직변화를 설명하고 관리하려는 연구가 나타나고 있다(강용식·권순동, 2016). 철학에서는 사회적 정의나 개인의 행복이 인지(이성), 정서(격정), 의지(욕망)의 세 부분의 능력 발휘와 조화를 통해 실현될 수 있다고 보고 있다(Kant, 1790; 최민홍, 1986). 여기서 인지는 합리적으로 헤아리고 숙고하는 이성적 능력을 말하고, 정서는 기쁨-슬픔, 차분-불안, 행복-불행 등과 같이 특정 대상이나 생각에 대한 감정적이거나 일반적인 반응을 말하며, 의지는 원하는 행동을 시작하기 위해 목표를 설정하거나 할 수 있다고 느끼는 자아효능감 뿐만 아니라 시작된 행동을 방해하는 유혹이 있으면 욕구나 정서를 조절하여 극복하는 실행제어(action control)나 지속하기 위한 결의나 인내를 발휘하는 것을 의미한다(Kant, 1790; 박도영, 2000).

본 연구에서는 개인정보유출의 사전 통제가능성의 인지가 실망감 및 배신감의 정서적 반응을 일으키고 이는 다시 타사 서비스로의 전환 의도나 부정적 구전과 같은 행동의지가 유발되는 과정을 정서적 차원에 초점을 두고 분석하였고, 또한, 이러한 과정이 내부유출과 외부해킹의 유출 원인에 따라 어떻게 달라지는가를 규명하였다.

2.3 귀인이론과 통제가능성

귀인이론(attribution theory)은 어떤 사건의 원인과 의미를 이해하고자 하는 시도로(Ajzen and Fishbein, 1983), 이 이론의 핵심은 사람이 어떤 사건이나 결과가 왜 일어났는지를 규명하는데 있다. 이러한 인과적 추론은 이후의 행위에 영향을 준다(Weiner, 1980). 귀인이론을 발전시킨 Weiner (1980)는 귀인을 원인의 소재(locus of cause), 안정성(stability), 통제가능성(controllability)의 세 가지 차원으로 분류하여 설명하였다. 첫째, 원인의 소재는 사건의 원인이 내부(고객)에 있는지 혹은 외부(기업)에 있는지에 대한 것이다(Folkes, 1984). 즉, 사건의 책임이 누구에게 있는지를 묻는 것이다. 둘째, 안정성은 사건의 원인이 영구적인지 혹은 일시적인지에 대한 것이다. 즉, 사건의 재발 가능성에 대해 평가하는 것이다. 셋째, 통제가능성은 사건의 원인을 통제하는 것이 가능했는지 혹은 불가능했는

지에 대한 것이다. 즉, 사건의 발생을 사전에 방지할 수 있었는지 여부를 의미한다.

그동안 기업의 위기나 서비스 실패 상황에서 귀인이론을 적용한 연구들이 진행되었다. 원유석(2005)은 서비스 회복노력이 고객만족에 미치는 영향을 안정성과 통제가능성이 조절하는 것을 검증하였다. 이상경과 이명천(2006)은 원인의 소재와 안정성이 사과의 수용의도에 유의한 영향을 미치는 것을 밝혔다. 유호범 등(2013)은 서비스 실패의 통제가능성이 회복 후 만족에 부정적인 영향을 미친다고 하였다. 이러한 선행연구들은 서비스 실패의 통제가능성 및 안정성과 행위의도 간의 관련성을 규명하였지만 실망감이나 배신감과 같은 정서적 요인에 대해서는 고려하지 않았다. 본 연구에서는 귀인이론의 내용 중에서 원인의 소재와 통제가능성이 인간의 정서에 미치는 영향에 초점을 두었다.

Ⅲ. 연구 방법

3.1 연구모형

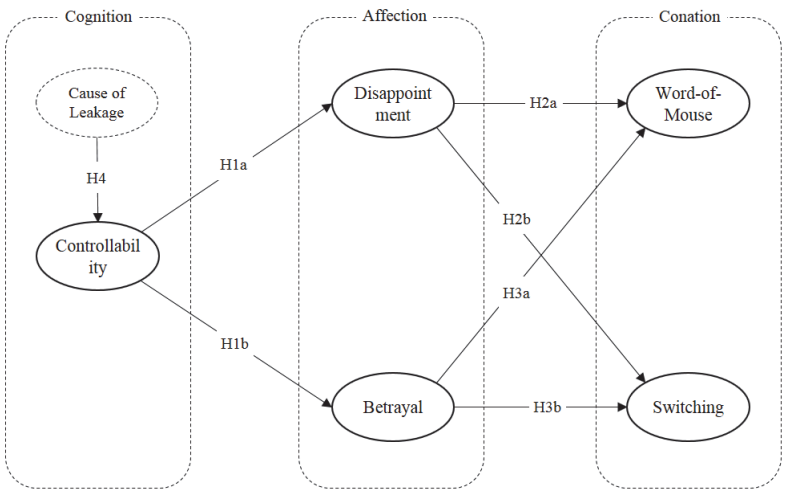
개인정보 유출 관련 선행연구에서 통제가능성과 행동의지 간의 관계를 설명하는데 초점을 두었다. 본 연구에서는 그동안 심리학 분야에서 주로 연구된 인지, 정서, 의지의 세 차원을 고려하였다. 따라서 개인정보 유출 관련 선행연구에 인간의 정서적 요인을 추가하여, 상황 및 원인 인지에 따른 정서적 반응과 그로 인한 행동의지를 규명하는데 초점을 두었다(Weiner, 1980). 고객이 어떤 사건의 결과로서 행동의지를 갖고 있다고 했을 때, 그 동인(動因)을 불러일으킨 정서적 원인을 정확히 파악하고 적절한 조치를 취할 때, 기업의 사고대처 및 신뢰회복 노력이 효과적일 수 있기 때문이다.

본 연구모형은 개인정보 유출사고의 사전 통제가능성 인지가 정서에 영향을 미치고 나아가 행동의지에 영향을 미친다는 것이다. 그리고 내부유출 및 외부해킹의 사고원인의 소재에 따라 이러한 영향은 달라진다는 것이다(Figure 1). 이를 설명하면, 개인정보 유출사고에 대한 사전 통제가능성 인지가 높을수록 실망감 및 배신감의 정서가 유발되고(Folkes, *et al.*, 1987), 이렇게 유발된 정서는 경쟁사로의 서비스 전환 및 부정적 구전과 같은 행동의지를 유발한다는 것이다. 그리고 이러한 인지, 정서, 의지의 영향 관계는 원인의 소재에 따라 달라지는데, 개인정보 유출사고 원인의 소재가 조직 외부의 해킹에 있다고 인지할 경우에는 배신감보다는 실망감이 유발되고, 이를 통해 부정적 구전의도가 높아지지만, 원인의 소재가 조직 내부에 있다고 인식할 경우에는 실망감보다는 배신감이 유발되고, 이로 인해 경쟁사로의 서비스 전환 의도가 높아진다는 것이다.

3.2 연구가설

3.2.1 인지(통제가능성)와 정서(실망감, 배신감)의 관계

통제가능성(controllability)은 해당 기업이 개인정보 유출을 사전에 통제하는 것이 가능했는지에 대한 고객의 인지이다(Hess, 2008). 이러한 통제가능성 인지에 따라 유발되는 고객의 정서는 다를 수 있다(Folkes *et al.*, 1987). 고객은 통제 불가능한 이유로 인한 개인정보 유출에 대해서는 상대적으로 관대한 경향을 보이지만(Folkes, 1984), 개인정보 유출을 사전에 통제하는 것이 가능했는데도 불구하



〈Figure 1〉 Research Model

고 부정적 결과가 발생했을 때에는 상대적으로 불만과 분노가 높아질 수 있다(문신희, 2013; Folkes *et al.*, 1987). 이처럼 고객이 당초 기대한 서비스가 유지되지 않고 서비스 실패가 발생할 경우, 이에 대한 인지의 결과로서 실망감이나 배신감과 같은 정서가 유발될 수 있다.

실망감과 배신감은 화(anger)의 수준에 있어서 분명히 구별되는 정서이다(공옥례 · 이형재, 2009; Bell, 1985; Koehler and Gershoff, 2003). 실망감(disappointment)은 긍정적인 결과를 기대했으나 실제 긍정적인 결과를 얻지 못하는 기대불일치의 상황에서 유발되는 정서인데 비해(Bell, 1985), 배신감(betrayal)은 기대불일치 보다 더 강하고 극단적인 정서 상태로, 서비스 제공자를 신뢰하고 위임하였으나 최소한의 믿음마저 져버렸거나 고객의 허용영역(zone of tolerance)을 초과하는 부정적 결과가 획득되었을 때 유발되는 정서이다(Koehler and Gershoff, 2003). 실망감과 배신감은 감정의 정도와 유발되는 상황에 있어서 차이가 있다. 감정의 정도에서 있어서 배신감은 실망감보다 더 강한 인지적, 정서적 상태를 보인다(공옥례 · 이형재, 2009; Oliver, 1999). 유발되는 상황에 있어서 배신감은 결과가 부정적일 때 나타나지만, 실망감은 긍정적일 때도 나타날 수 있다. 실망감의 예로, 60점을 맞으면 통과하는 시험에서 65점을 맞아 시험에 통과하는 긍정적인 결과를 얻었다 하더라도, 자신이 당초에 기대한 점수가 80점이었다면 통과한 65점의 점수에 대해서도 실망감을 느낄 수 있다.

본 연구에서는 개인정보 유출 사건이 발생했을 경우에 그러한 유출 사건이 발생하지 않도록 사전에 통제할 수 있었다고 인지할수록 실망감과 배신감이 높아진다고 보아 다음과 같이 인지가 정서에 미치는 영향 가설을 도출하였다.

H1a: 통제가능성은 실망감에 정의 영향을 미칠 것이다.

H1b: 통제가능성은 배신감에 정의 영향을 미칠 것이다.

3.2.2 정서(실망감, 배신감)와 의지(구전, 전환)의 관계

정서는 행동의지에 영향을 미칠 수 있다(Oliver, 1999; Damasio, 2000). 고객이 당초 기대한 긍정적 결과를 획득하지 못하거나 최소한의 믿음마저 지켜지지 않았다고 느낄 때, 고객은 행동 욕구나 의지를 갖게 된다. 고객이 실망감을 느끼면 서비스를 다른 사람에게 추천하지 않거나 또는 부정적 구전 활동을 벌일 수 있다. 이에 비해 배신감을 느끼면 서비스 이용을 중지하거나, 경쟁기업으로 전환하거나, 또는 공정성 회복을 위해 행동할 수 있다(윤일한・권순동, 2015; Frijda *et al.*, 1989). 본 연구에서는 개인정보 유출로 인한 실망감과 배신감으로 인해 발휘되는 행동의지 가운데에 구전의도와 전환 의도에 초점을 맞추었다. 구전(word-of-mouth)은 상업적인 이해관계가 없는 사람들이 특정 제품이나 서비스 또는 그 제공자에 관해 긍정적이거나 부정적인 정보를 비공식적으로 그리고 자발적으로 전달하는 의사소통 행위나 과정을 의미한다(Huefner and Hunt, 2000). 본 연구에서는 개인정보 유출이라는 부정적 사건에 초점을 맞추고 있기 때문에 구전이라 함은 해당 기업에 대한 부정적인 평가를 다른 사람에게 전하는 부정적 구전을 의미한다(김대원・윤영민, 2015). 전환(switching)은 유지의 반대 개념으로 고객이 현재 제공자가 제공하는 제품 및 서비스의 이용을 중단하고 다른 제공자가 제공하는 것으로 대체 이용하는 것을 의미한다. 즉, 전환은 제품 및 서비스 제공자와의 관계를 중단하고 새로운 제공자로 변경・교체하는 행위를 의미한다(Zeithaml *et al.*, 1996). 본 연구에서는 구전과 전환의 개념을 구전을 퍼뜨리거나 타 회사로 전환하고자 하는 행동의지를 의미하는 것으로 정의하였다.

마케팅 분야의 선행연구에 따르면 서비스 실패로 인해 유발된 실망감과 배신감의 정서가 구전 및 전환의 행동의지에 미치는 영향은 서로 다르다. 실망감과 배신감이 구전과 전환에 둘 다 영향을 미친다는 연구가 있고(Zeelenberg and Pieters, 2004; 문신희・김정희, 2014), 실망감은 구전에만 영향을 미치고, 배신감은 전환에만 영향을 미친다는 연구도 있으며(공옥례・이형재, 2009), 배신감에 대한 개별적 연구에서 배신감은 구전에 영향을 미치지 않는다는 연구도 있다(Feinberg *et al.*, 2002). 본 연구에서는 개인정보 유출로 인해 느끼게 되는 배신감과 실망감은 구전에도 영향을 미치고 전환에도 영향을 미친다는 가설을 도출하였다. 왜냐하면 개인정보 유출 사건은 마케팅 분야의 선행연구에서 다루어온 서비스 실패의 사건보다 개인에게 미치는 범위와 영향력이 클 수 있기 때문이다.

H2a: 실망감은 구전에 정의 영향을 미칠 것이다.
H2b: 실망감은 전환에 정의 영향을 미칠 것이다.

H3a: 배신감은 구전에 정의 영향을 미칠 것이다.
H3b: 배신감은 전환에 정의 영향을 미칠 것이다.

3.2.3 개인정보 유출 원인에 따른 차이

개인정보 유출의 원인은 크게 외부해킹과 내부유출로 나눌 수 있다. 외부해킹으로 인한 개인정보 유출은 외부의 침입자, 즉 해커(hacker)가 회사의 특정 시스템을 공격하여 고객의 개인정보가 유출되는 것이다. 이는 평소 기업이 시스템의 취약점을 잘 관리하지 못했기 때문에 발생한 것으로, 해당 기업에 과실 책임이 있는 것으로 본다(개인정보보호법 제29조). 내부유출로 인한 개인정보 유출은 회사의 내

부자, 즉 내부 임직원이나 협력업체 직원이 고객의 개인정보를 유출하는 것이다. 두 경우 모두 해당 기업의 책임으로 발생한 사고이지만, 그 책임의 경중에는 차이가 있다고 할 수 있다. 통상적으로, 유출의 원인이 외부해킹보다 내부유출일 때 해당 기업의 책임이 더 크다고 본다. 법에서도 '징벌적 손해배상제'를 적용하여, 내부 유출로 인한 개인정보 유출 시, 고객이 더 큰 손해배상을 청구할 수 있도록 하고 있다(개인정보보호법 제39조 제3항). 위기관리 분야의 연구에 따르면(이상경 · 이명천, 2006), 기업의 위기를 초래한 원인에 따라, 고객의 위기 커뮤니케이션 수용도가 다르다. 외부적 요인으로 발생한 위기와 내부적 과실로 발생한 위기에 따라서 고객이 기업에 대해 갖는 부정적 이미지와 태도가 차이를 보인다(이상경 · 이명천, 2006). 이렇듯 기업의 책임 정도는 고객의 감정과 행위에 영향을 줄 수 있다(Weiner, 1985). 그러나 아직까지 개인정보 유출 관련 연구에서 유출의 원인을 중심으로 살펴본 연구는 없다. 따라서 본 연구에서 개인정보 유출 원인에 따른 고객의 정서와 행동의지를 살펴보고자 다음과 같은 가설을 설정하였다.

H4: 개인정보 유출 원인에 따라 통제가능성 인지가 정서와 행위의도에 미치는 영향이 다를 것이다.

3.3 설문의 구성 및 데이터 수집

본 연구에서는 인지적 측면에서의 통제가능성, 정서적 측면에서의 실망감과 배신감, 의지적 측면에서의 구전과 전환을 다음과 같이 정의하였다. 첫째, 통제가능성은 개인정보 유출을 사전에 통제하는 것이 가능했는지에 대한 고객의 인지로 정의하였다. 둘째, 실망감은 기대와 달리 긍정적인 결과를 얻지 못함으로 인한 기대불일치의 상황에서 유발되는 정서적 상태로 정의하였다. 셋째, 배신감은 최소한의 믿음마저 져버리는 부정적 결과의 획득으로 인해 유발되는 정서적 상태로 정의하였다. 넷째, 구전과 전환은 구전을 퍼뜨리거나 타 회사로 전환하고자 하는 행동의지로 정의하였다. 각각의 변수에 대한 개념적 정의와 선행연구를 바탕으로 〈Table 2〉와 같이 설문문항을 개발하였다. 설문문항은 전혀 그렇지 않다(1), 그렇지 않다(2), 보통이다(3), 그렇다(4), 매우 그렇다(5)의 Likert 5점 척도로 측정하였다.

본 연구를 위해 개인정보 유출 경험이 있는 사람들을 대상으로 설문조사를 실시하였다. 설문조사는 2016년 9월 22일부터 28일까지로 일주일간 실시하였다. 본 설문에서는 개인정보 유출의 원인을 외부해킹과 내부유출로 구분하여 가상의 시나리오를 제시하였고, 각 시나리오에 따라 통제가능성 인지, 정서, 행동의지를 응답하도록 하였다. 최종적으로 230명이 외부해킹과 내부유출 각각에 대해 응답하여 (즉, 1인이 2회 응답하여) 460개의 데이터를 수집하였다. 한편, 동일인이 두 항목에 모두 응답하기 때문에 설문의 배치순서에 따라서 결과가 영향을 받을 수 있다. 따라서 본 설문에 앞서 내부유출과 외부해킹 순서로 예비조사를 하였고, 또한 외부해킹과 내부유출 순서로 예비조사를 실시하였다. 그리고 서로 다른 순서에 따른 예비조사를 비교 검토한 결과, 유의한 차이가 없음을 확인하여 설문을 진행하였다. 본 연구에 사용된 설문문항은 외부해킹, 내부유출 순이다.

〈Table 2〉 Survey items

Construct		Survey items
Cognition	Controllability (CON)	If the company had managed it in advance, personal information leakage would not have occurred.
		It would have been possible for the company to control the leakage of personal information in advance.
		I think that it is the responsibility of leakage of personal information to a company which is not managed thoroughly normally.
Affection	Disappointment (DIS)	I was disappointed with the company that leaked personal information.
		The companies that leaked personal information were not as good as I expected.
		Companies that leaked personal information were disappointing compared to other companies.
	Betrayal (BET)	There is a sense of betrayal to companies that leak personal information.
		I felt that I was deceived by the company that leaked personal information.
		It is difficult to trust companies that have leaked personal information.
Conation	Word-of-Mouse (WOM)	I will spread a bad reputation about the companies that have leaked personal information.
		I will blame companies that have leaked personal information to my friends.
		When my friends use a company that has a leak of personal information, I will tell my friends do not use its service.
	Switching (SWI)	I will use less of the companies that have leaked personal information.
		When a company has a leak of personal information, I will change my service to another company.
		I will no longer be using a company that has had its personal information leaks.

Ⅳ. 연구결과 분석

4.1 표본의 특성

설문에 응답한 표본의 특성은 〈Table 3〉과 같다. 성별은 남자가 54.8%, 여자가 45.2%로 나타났고, 연령대는 20대가 71.3%로 가장 높게 나타났다. 개인정보를 제공한 웹 사이트의 수는 5개 이상이라고 응답한 비율이 전체의 97.4%로 나타났다.

4.2 신뢰성 및 타당성 분석

본 연구모형을 검증하기 앞서 측정문항과 구성개념에 대해 신뢰성과 집중타당성과 판별타당성을 Smart-PLS 2.0 통계 패키지로 검증하였다. 〈Table 4〉와 같이, 각 구성개념의 Cronbach's Alpha 값이 0.7 이상으로 나타나서 신뢰성이 있는 것으로 나타났다. 각 구성개념의 복합신뢰도(CR)는 모두 0.7 이상이고, 평균분산추출값(AVE)은 0.5 이상으로 나타나 집중타당성이 있는 것으로 나타났다(Fornell and

〈Table 3〉 Profile of Data Sample

Category	Items	Frequency	Ratio(%)
Gender	Male	126	54.8
	Female	104	45.2
Age	Under 20	8	3.5
	20s	164	71.3
	30s	31	13.5
	40s	18	7.8
	Over 50	9	3.9
Number of web sites providing personal information	Under 5	6	2.6
	6~10	36	15.7
	10~15	53	23.0
	16~20	64	27.8
	Over 20	71	30.9
Total		230	100

〈Table 4〉 Reliability and Validity Test

Scale Items	Factor Loading	AVE	CR	Cronbach's Alpha
CON1	0.918	0.727	0.888	0.810
CON2	0.922			
CON3	0.847			
DIS1	0.892	0.725	0.888	0.810
DIS2	0.885			
DIS3	0.870			
BET1	0.868	0.804	0.925	0.877
BET2	0.866			
BET3	0.819			
WOM1	0.774	0.778	0.913	0.858
WOM2	0.882			
WOM3	0.896			
SWI1	0.909	0.837	0.939	0.903
SWI2	0.934			
SWI3	0.902			

Larcker, 1981). 판별타당성은 구성개념 간의 상관계수의 대각선 축에 표시되는 AVE의 제곱근 값이 다른 구성개념 간의 상관계수 값보다 큰가의 여부로 검증하였다. 〈Table 5〉에서와 같이, AVE의 제곱근 값 중 가장 작은 값(0.851)이 가장 큰 상관계수 값(0.565)보다 높게 나타나 판별타당성이 있는 것으로 확인되었다.

〈Table 5〉 Discriminant Validity Test

Construct	1	2	3	4	5
1.CON	0.852				
2.DIS	0.460	0.851			
3.BET	0.415	0.504	0.896		
4.WOM	0.393	0.555	0.511	0.882	
5.SWI	0.203	0.433	0.527	0.565	0.915

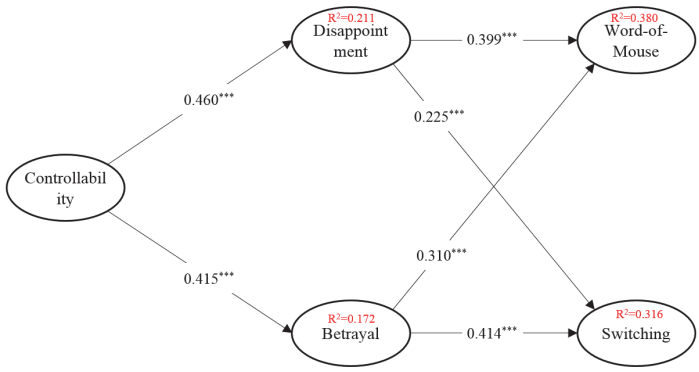
4.3 가설검증

4.3.1 전체 데이터를 이용한 경로분석

PLS 분석에서는 경로모형의 적합도 검정(Goodness-of-Fit, GoF)을 필요로 한다.[1] 모형 적합도는 10%, 25%, 36%을 기준으로 각각 낮음(small), 중간(medium), 높음(large)으로 판단한다(Wetzels, 2009). 내부유출과 외부해킹의 전체 데이터 460개를 이용한 연구모형의 GoF 계산 결과는 45.7%로서 높은 적합도를 보였다.

다음으로 경로계수의 유의성을 검증하였다. 개인정보 유출사고의 사전 통제가능성 인지가 정서에 영향을 미치고 나아가 행동의지에 영향을 미친다는 가설1에서 가설3까지는 전체 데이터분석을 통해 검증

1) GoF = $\sqrt{\overline{AVE} * \overline{R^2}}$



*p < 0.05(t≥1.96), **p < 0.01(t≥2.58),***p < 0.001(t≥3.30)

〈Figure 2〉 Path Analysis of Research Model

하였다. 그리고 내부유출 및 외부해킹의 사고원인의 소재에 따라 이러한 영향은 달라진다는 가설4는 외부해킹과 내부유출 집단비교를 통해 검증하였다.

먼저 가설1부터 가설3까지의 검증을 위해 460개의 전체 데이터를 이용하여 구조모형에 대한 경로계수를 구하고, PLS에서 제공하는 부스트랩(bootstrap)을 이용하여 경로계수의 t값을 산출하였다. 〈Figure 2〉는 이러한 분석결과를 그림으로 표현한 것이다. 분석결과, 각 가설의 경로계수 t값이 모두 3.3보다 큰 것으로 나타나 유의수준 0.1%에서 가설1a에서 가설3b에 이르는 6개의 가설 모두가 채택되었다. 〈Table 6〉은 이러한 결과를 표로 정리한 것이다. 따라서 개인정보유출의 사전 통제가능성의 인지가 실망감 및 배신감의 정서적 반응을 일으키고 이는 다시 타사 서비스로의 전환 의도나 부정적 구전과 같은 행동의지가 유발된다는 것이 증명되었다.

개인정보 유출 관련 선행연구들에서는 사람을 인과적 추론에 의해 행동하는 이성적 정보처리자로 간주하고 통제가능성의 인지적 측면과 행동 간의 관계를 규명하였다. 이러한 지금까지의 선행연구 관점을 적용하여 본 연구모형을 분석해 보았다. 이를 위해 연구모형에서 실망감 및 배신감의 정서적 변수를 제외하고, 선행연구에서와 마찬가지로 통제가능성 인지와 구전 및 전환 의도만을 포함한 전통적 연구모형을 분석해 보았다. 그 결과 선행연구 기반의 전통적 연구모형의 적합도(GoF)는 28.3%로 나타났다. 이는 실망감과 배신감의 정서적 측면을 고려한 본 연구모형의 적합도 45.7%에 비해 매우 낮은 수치이다. 따라서 정서적 측면을 제외한 선행연구보다는 인지, 정서, 행동의지를 모두 고려한 본 연구의 모형이 적합도 및 설명력이 더 우수한 것으로 입증되었다.

〈Table 6〉 Hypothesis Test(H1a~H3b)

Path		Coefficient	t-values	Results
H1a	CON→DIS	0.460	11.192***	Accepted
H1b	CON→BET	0.415	10.337***	Accepted
H2a	DIS→WOM	0.399	8.678***	Accepted
H2b	DIS→SWI	0.225	5.083***	Accepted
H3a	BET→WOM	0.310	6.840***	Accepted
H3b	BET→SWI	0.414	8.859***	Accepted

4.3.2 외부해킹과 내부유출의 비교 분석

4.3.2.1 외부해킹과 내부유출의 평균 비교

개인정보 유출원인을 외부해킹과 내부유출로 구분하여 각 연구변수별 평균값을 〈Table 7〉과 같이 비교해보았다. 그 결과, 내부유출이 외부해킹보다 모든 측면에서 높게 나타났다. 인지적 측면에서 볼 때, 개인정보 유출사고를 미연에 방지할 수 있었는가 하는 통제가능성은 내부유출(4.39)이 외부해킹(3.88)보다 높게 나타나 사람들은 내부유출의 통제가능성을 더 높게 인지하였다. 정서적 측면에서 볼 때, 실망감과 배신감은 내부유출(3.97, 3.82)이 외부해킹(3.03, 2.97)보다 높게 나타났다. 행동의지 측면에서 볼 때, 구전의도와 전환 의도는 내부유출(3.65, 3.50)이 외부해킹(3.09, 3.10)보다 높게 나타나 내부자에 의해 개인정보가 유출되었을 경우에 그러한 부정적 사건의 내용을 사람들에게 더 많이 퍼뜨리고자 하고, 또한 다른 기업으로 서비스 이용을 전환하려는 의도가 높았다.

〈Table 7〉 Comparing Means between External and Internal Leakage

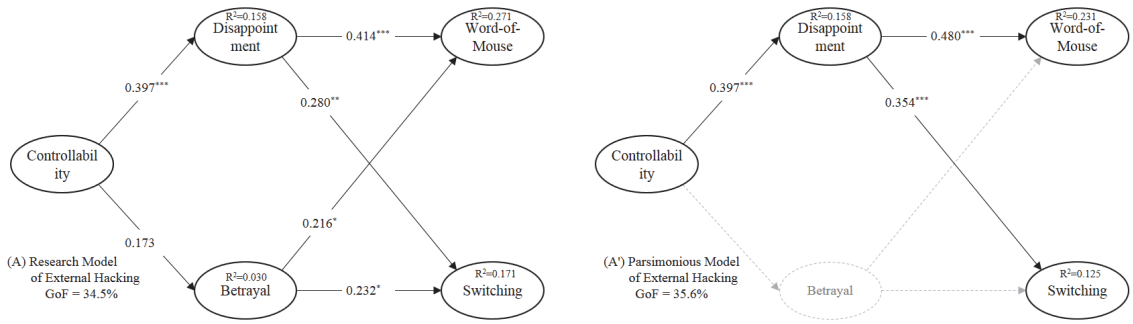
Construct		External Hacking	Internal Leakage	t-value
Cognition	Controllability	3.88	4.39	9.985***
Affection	Disappointment	3.03	3.97	19.672***
	Betrayal	2.97	3.82	20.379***
Conation	Word-of-Mouth	3.09	3.65	11.008***
	Switching	3.10	3.50	8.854***

4.3.2.2 외부해킹과 내부유출의 경로 비교 분석

다음으로 외부해킹과 내부유출의 유출 원인별로 통제가능성 인지가 정서와 행동의지에 미치는 영향을 분석하였다. 모형의 분석 및 해석은 Smart-PLS와 간명모형(parsimonious model) 특성을 이용하였다.

좋은 연구모형은 간명한(parsimonious) 특성을 지닌다. 연구모형의 간명성은 어떤 모형을 만들거나 검증할 때 변수를 최소한으로 하면서 의미 있게 설명하는 것이 좋다는 것이다. 따라서 간명성도 높고 설명력도 높은 것이 이상적일 수 있다. 그러나 모형의 간명성과 설명력 간에는 상충관계가 존재한다. 어떤 현상을 설명하는데 사용되는 변수가 적을수록 간명성은 높아지지만 설명력은 떨어지기 때문이다. 따라서 설명력을 손상시키지 않으면서 간명성을 충족하는 현명한 선택이 필요하다.

본 연구에서는 간명모형을 도출하기 위해 통계적으로 가장 중요하지 않다고 생각되는 변수를 하나씩 차례로 제거해나가는 후진제거법(backward selection)을 사용하였다. 간명성은 변수의 개수의 감소 정도로 평가하고, 설명력은 공통성(communality)의 평균과 설명력(R^2)의 평균의 곱에 대한 제곱근 값으로 산정하는 모형 적합도(GoF)로 평가하였다. 분석결과, 외부해킹에서는 배신감이 제거된 간명모형이 도출되었고, 내부유출에서는 실망감이 제거된 간명모형이 도출되었다. 즉, 외부해킹에서는 배신감 변수 제거시 모형적합도가 34.5%에서 35.6%로 증가하였고, 내부유출에서는 실망감 변수 제거시 모형적합도가 45.4%에서 49.2%로 증가하였다. 그리고 외부해킹과 내부유출에 따른 영향력의 차이를 결합경로계수와 t값 비교를 통해 검증하였다. 이와 같이 간명모형 분석과 결합경로계수 비교를 통해 개인정보 유출 원인에 따라 통제가능성 인지가 정서와 행위의도에 미치는 영향이 다르다는 가설4가 유의하게 나타나 채택하였다. 이러한 분석과정 및 결과해석을 외부해킹과 내부유출로 구분하여 자세히 살펴보면 다음과 같다.



〈Figure 3〉 Comparing Research Model and Parsimonious Model in External Hacking

(1) 외부해킹에 의한 개인정보 유출 상황에서의 모형분석

① 간명모형 분석

〈Figure 3〉의 (A)는 개인정보 유출이 외부해킹에 의해 이루어지는 상황에서, 본 연구모형을 분석한 결과이다. 본 연구모형에서 모형 적합도(GoF)는 34.5%로 나타났고, 실망감, 구전의도, 전환 의도는 각각 설명력(R^2)의 최소 기준값(Falk and Miller, 1992)인 10%를 넘었지만, 배신감은 3%로 기준값 이하로 나타났다. 다음으로 본 연구모형에서 간명모형을 도출했다. 간명모형은 후진제거법에 의해 설명력이 가장 낮은 배신감을 모형에서 제거하여 만들었고, 〈Figure 3〉의 (A′)는 간명모형의 분석결과이다. 간명모형에서 모형 적합도는 35.6%로 나타나 본 연구모형보다 모형 적합도가 향상되었다. 각 변수의 설명력 또한 실망감, 구전의도, 전환 의도 모두가 기준값 이상으로 나타났다.

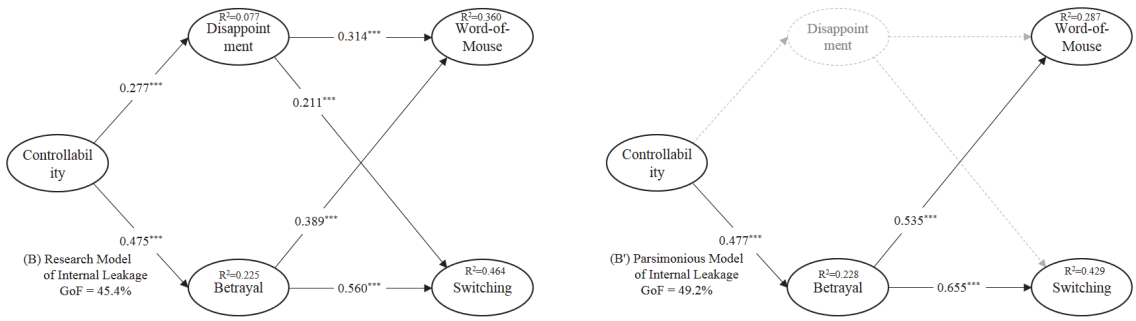
② 결합경로계수 비교 분석

〈Table 8〉 Combined Path Analysis of External Hacking

Path	Combined Coefficient	t-value
CON → DIS → WOM	**0.165**	**4.997*** **
CON → DIS → SWI	**0.111**	**3.562*** **
CON → BET → WOM	0.037	2.121*
CON → BET → SWI	0.040	2.031*

〈Table 8〉은 외부해킹에 의한 개인정보 유출 상황에서, 독립변수가 매개변수를 통해 종속변수에 미치는 영향의 상대적 크기를 결합경로계수를[2] 통해 비교한 것이다. 통제가능성 → 실망감 → 구전의도의 결합경로계수는 0.165로 가장 높고, 통제가능성 → 실망감 → 전환 의도의 결합경로계수는 0.111로 두 번째로 높았다. 그러나 통제가능성 → 배신감 → 구전의도의 결합경로계수와, 통제가능성 → 배신감 → 전

2) 결합경로계수 $= P_1 * P_2$
결합경로계수의 t값 $= (P_1 * P_2) / \sqrt{P_1^2 S_2^2 + P_2^2 S_1^2 + S_1^2 S_2^2}$
여기서, P_1은 독립변수에서 매개변수로 가는 경로계수, P_2는 매개변수에서 종속변수로 가는 경로계수, S_1과 S_2는 P_1과 P_2의 표준편차를 의미함



〈Figure 4〉 Comparing Research Model and Parsimonious Model in Internal Leakage

환 의도의 결합경로계수는 각각 0.037, 0.04로 영향력이 매우 낮았다. 이로써 외부해킹에 있어서 매개효과의 설명력은 실망감은 강하지만 배신감은 약한 것을 확인하였다. 즉, 외부해킹의 경우, 통제가능성 인식은 실망감을 통해 구전의도(0.165)로, 또는 전환 의도(0.111)로 영향을 미치는 반면, 배신감을 통해 구전의도(0.037)나 전환 의도(0.04)로 상대적으로 매우 약하게 영향을 미치는 것을 확인하였다.

③ 외부해킹에 의한 개인정보 유출 상황에서 간명모형 및 결합경로 분석 결과 종합

간명모형 분석을 통해 당초의 연구모형에서 배신감 변수를 제외하는 것이 더 바람직하다는 것을 확인하였고, 결합경로계수 비교 분석을 통해 통제가능성 → 실망감 → 구전의도의 경로가 가장 설명력이 높다는 것을 확인하였다. 따라서 이 두 분석을 종합하여 중요한 측면을 부각시켜 설명하면, 외부해킹에 의한 개인정보 유출 상황에서는 통제가능성 인지를 통해 실망감이 유발되고 나아가 부정적 구전의도가 높아진다고 말할 수 있다. 따라서 기업은 외부해킹에 의해 개인정보 유출 사고가 발생할 경우에 부정적 구전행동이 주로 실망감에서 비롯되기 때문에 실망감을 낮추기 위한 대응전략에 초점을 맞출 필요가 있다.

(2) 내부자에 의한 개인정보 유출 상황에서의 모형분석

① 간명모형 분석

〈Figure 4〉의 (B)는 개인정보 유출이 내부자에 의해 이루어지는 상황에서, 본 연구모형을 분석한 결과이다. 본 연구모형에서 모형 적합도(GoF)는 45.4%로 나타났고, 배신감, 구전의도, 전환 의도는 각각 설명력(R^2)의 최소 기준값인 10%를 넘었지만, 실망감은 7.7%로 기준값 이하로 나타났다. 다음으로 본 연구모형에서 간명모형을 도출했다. 간명모형은 후진제거법에 의해 설명력이 가장 낮은 실망감을 모형에서 제거하여 만들었고, 〈Figure 4〉의 (B′)는 간명모형의 분석결과이다. 간명모형에서 모형 적합도는 49.2%로 나타나 당초 연구모형보다 모형 적합도가 향상되었다. 각 변수의 설명력 또한 배신감, 구전의도, 전환 의도 모두가 기준값 이상으로 나타났다.

② 결합경로계수 비교 분석

〈Table 9〉는 내부자에 의한 개인정보 유출 상황

에서, 독립변수가 매개변수를 통해 종속변수에 미치는 영향의 상대적 크기를 결합경로계수를 통해 비교한 것이다. 통제가능성 → 배신감 → 전환 의도의 결합경로계수가 0.266으로 가장 높고, 통제가능성 → 배신감 → 구전의도의 결합경로계수는 0.185로 두 번째로 높게 나타났다. 그러나 통제가능성 → 실망감 → 구전의도의 결합경로계수와, 통제가능성 → 실망감 → 전환 의도의 결합경로계수는 각각 0.087, 0.059로 상대적으로 낮게 나타났다. 이로써 내부유출에 있어서 매개효과의 설명력은 배신감은 강하지만 실망감은 약한 것을 알 수 있다. 즉, 내부유출의 경우, 통제가능성 인식은 배신감을 통해 전환 의도(0.266)나 구전의도(0.185)로 강하게 영향을 미치는 반면, 실망감을 통해 구전의도(0.087)나 전환 의도(0.059)로 상대적으로 약하게 영향을 미치는 것을 확인하였다.

〈Table 9〉 Combined Path Analysis of Internal Leakage

Path	Combined Coefficient	t-value
CON → DIS → WOM	0.087	3.314***
CON → DIS → SWI	0.059	2.915**
CON → BET → SWI	**0.266**	**3.813*** **
CON → BET → WOM	**0.185**	**2.946****

③ 내부자에 의한 개인정보 유출 상황에서 간명모형 및 결합경로 분석 결과 종합

간명모형 분석을 통해 당초의 연구모형에서 실망감 변수를 제외하는 것이 더 바람직하다는 것을 확인하였고, 결합경로계수 비교 분석을 통해 통제가능성 → 배신감 → 전환 의도의 경로가 가장 설명력이 높다는 것을 확인하였다. 이 두 분석을 요약하면, 내부자에 의한 개인정보 유출 상황에서는 통제가능성 인지를 통해 배신감이 유발되고 나아가 전환 의도가 높아지는 것이다. 따라서 기업은 내부자에 의해 개인정보 유출 사고가 발생할 경우에 전환 의도가 주로 배신감에서 비롯되기 때문에 배신감을 낮추고 신뢰를 회복하기 위한 대응전략을 수립할 필요가 있다.

4.4 가설 검증결과의 논의

본 연구의 결과를 다음 네 가지 측면으로 구분하여 논의해 보았다.

첫째, 460개의 전체 데이터를 이용한 경로분석에서 개인정보 유출사고에 대한 사전 통제가능성 인지가 높을수록 실망감 및 배신감의 정서가 유발되고, 이렇게 유발된 정서는 경쟁사로의 서비스 전환 및 부정적 구전과 같은 행동의지를 유발한다는 것을 입증하였다. 지금까지 경영정보 및 보안 분야에서는 인지 → 의지의 영향관계에 초점을 두어 개인정보 유출 인지에 따른 고객의 행동을 설명하고자 노력하였다. 그러나 본 연구에서는 심리학과 마케팅 분야에서 적용되고 있는 인지 → 정서 → 의지의 영향 관계를 개인정보 유출 상황에 적용하여 설명하였다. 이를 위해 이성적 측면을 강조한 보안 분야의 연구에 배신감과 실망감의 정서적 측면을 보완하여 설명하였다. 이러한 결과는 개인정보 유출에 따른 고객 행동의 예측력을 높이고 나아가 기업의 사후대책의 효과성을 높이는데 기여할 것으로 예상된다.

둘째, 내부유출과 외부해킹의 원인별로 구분하여 수준을 변수의 평균값으로 비교한 결과, 인지·정서·의지의 부정적 수준이 내부유출 상황에서 더 높음을 확인하였다. 내부유출 사고의 경우 통제가능성, 실망감 및 배신감, 부정적 구전 및 서비스 전환 의도를 높게 갖는 것을 확인하였다. 이러한 내부유출의 심각성 수준과 선행연구에서 보여준 피해규모

의 심각성을(Ponemon Institute, 2016) 연결해 보면, 기업은 내부유출로 인한 사고 방지를 위해 정보보호 준수 의지와 효과적인 정책수립 및 집행이 필요하다고 볼 수 있다.

셋째, 외부해킹 상황에 응답한 230개의 데이터를 분석한 결과, 외부해킹 상황에서는 통제가능성 인지로 인해 실망감이 유발되고 이것은 구전의도에 영향을 미치는 것을 확인하였다. 외부해킹에서는 고객이탈과 같은 극단적 행동보다는 불만표출을 목적으로 부정적 구전을 주변 사람들에게 전달함으로써 기업 명성이나 브랜드 이미지를 낮추려는 노력을 한다고 볼 수 있다. 따라서 외부해킹에 의한 개인정보 유출로 실망감이 유발되었을 경우에 기업은 배신감 상황에서의 조치와는 차별화된 조치를 취할 필요가 있다.

실망감 관련 선행연구에 따르면(박명호 · 장영혜 2014; 윤일한 · 권순동, 2015), 기업에 대한 고객의 기대 수준이 과도하게 높을 경우에는 기대가 적절하고 현실적일 수 있도록 그 수준을 관리할 필요가 있다. 예를 들어, 고객의 관심을 유도하기 위한 과장광고 등에 유의해야 하고, 서비스가 절대적으로 안전하다는 일방적 커뮤니케이션은 지양할 필요가 있다. 대신에 외부해킹에 의한 서비스 실패의 상황적 불가피성을 알리는 커뮤니케이션을 개발할 필요가 있다(윤일한 · 권순동, 2015). 이처럼 외부해킹에 의한 부정적 구전이 발생할 경우에 기업은 그 원인이 실망감에서 비롯된 것을 인식하고 이러한 실망감을 회복하기 위한 노력을 기울일 필요가 있다.

넷째, 내부유출 상황에 응답한 230개의 데이터를 분석한 결과, 내부유출 상황에서는 통제가능성 인지를 통해 배신감이 유발되고 나아가 전환 의도가 높아지는 것을 검증하였다. 내부자에 의한 개인정보 유출 사고는 고객이탈이라는 매우 심각한 위기를 초래하기 때문에 기업에게 더 높은 경각심이 요구된다. 본 연구에서 경쟁사로의 고객이탈은 배신감에서 비롯된다는 것을 확인하였다. 따라서 기업은 내부자에 의해 개인정보 유출 사고가 발생하였을 경우에는 배신감을 달래고 서비스를 회복하기 위한 노력을 강구해야 한다.

서비스 회복에 관한 선행연구에 따르면(Gronoroos, 1998; 윤일한 · 권순동, 2015; 임목규, 2016), 서비스 실패 상황에서 면피성 미봉책을 제시하거나, 규정이 없다고 하여 고객의 기대에 벗어난 대응을 할 경우 배신감은 감소되지 않고 더욱 깊어질 수 있다. 사후 조치가 미흡하고 적절한 보상이 없으면 피해를 입은 고객은 모든 수단을 동원해 공정성을 회복하는 노력을 할 것이다. 따라서 기업은 시의적절한 응답, 사과, 할인, 금전적 보상 등을 공정하게 해줌으로써 배신감을 낮추는 노력을 강구해야 할 것이다.

Ⅴ. 결 론

5.1 연구결과의 요약

본 연구에서는 그동안 심리학 및 마케팅 분야에서 연구된 인지 → 정서 → 의지의 이론을 개인정보 유출 상황에 적용하여 유출원인의 인지에 따른 정서적 반응과 그로 인한 행동의지의 영향관계를 규명하였다. 본 연구의 모형은 개인정보 유출사고의 사전 통제가능성 인지가 정서에 영향을 미치고 나아가 행동의지에 영향을 미친다는 것이다. 그리고 내부유출 및 외부해킹의 원인소재에 따라 이러한 영향은 달라진다는 것이다.

본 연구모형을 데이터 분석을 통해 검증한 결과는 다음과 같다. 첫째, 개인정보 유출사고에 대한 사전

통제가능성 인지가 높을수록 실망감 및 배신감의 정서가 더 높게 유발되고, 이렇게 유발된 정서는 경쟁사로의 서비스 전환 및 부정적 구전과 같은 행동의지를 더 높게 유발한다는 것이다. 둘째, 외부해킹에 의해 개인정보가 유출될 경우에는 통제가능성 인지로 인해 실망감이 유발되고 이것은 부정적 구전의도에 영향을 미친다는 것이다. 셋째, 내부자에 의해 개인정보가 유출될 경우에는 통제가능성 인지를 통해 배신감이 유발되고 서비스 전환 의도가 높아지는 것이다.

5.2 연구결과의 시사점

본 연구의 의의는 학술적 측면과 경영관리적 측면에서 살펴볼 수 있다. 먼저, 학술적 의의는 지금까지 보안 및 개인정보보호 관련 연구들이 인지→행동의지의 관계에 초점을 두어 설명하였던 것에 비해, 본 연구에서는 인지→정서→의지의 심리 이론을 개인정보 유출 상황에 적용하여 종전보다 설명력을 더 높였다는 점이다. 즉, 종전의 이성적 측면을 강조한 보안 분야의 연구에 배신감과 실망감의 정서적 측면을 추가함으로써 설명력과 행동의 예측력을 높였다는 점이다.

경영관리적 의의는 기존 연구에서 다루지 않았던 외부해킹 및 내부유출의 원인소재에 초점을 두어 차이를 규명함으로써 기업의 사고 대응책을 원인소재에 따라 차별화해야 함을 제시하였다는 점이다. 그리고 개인정보유출로 인한 고객의 부정적 행동이 외부해킹의 경우에는 실망감으로 인한 것이고, 내부유출의 경우에는 배신감에 의한 점을 규명함으로써 기업의 사후대책의 효과성을 높이는데 기여하였다는 점이다. 본 연구 결과를 통해서 기업이 개인정보 유출 이후에 취할 수 있는 대응책을 유출 원인에 따라 제안하면 다음과 같다.

외부해킹에 의해 개인정보 유출 사고가 발생하면, 기업은 실망감을 낮추는데 초점을 맞출 필요가 있다. 예를 들어, 기업은 예방을 위한 각고의 노력을 해왔으나, 현실적으로 완벽한 예방은 어려운 일이고 유감스럽게도 사고가 발생했다는 식의 메시지 전달을 통해 고객의 기대를 낮추는 동시에 고객의 이해를 구할 필요가 있다. 아울러, 현재 기업에서 하고 있는 보안 활동을 명시하고, 앞으로 이를 어떻게 더 발전시킬 것인지를 보여주는, 즉, As-is와 To-be 계획에 관한 재발 방지 대책을 제시할 필요가 있다.

내부유출로 개인정보 유출 사고가 발생하면, 기업은 배신감을 낮추는데 초점을 맞출 필요가 있다. 예를 들어, 배신감을 치유하고 회복하기 위해 기업은 우선으로 겸허히 잘못을 인정하고 진정성 있는 사과를 해야 할 것이다. 또한, 시기적절하고 공정한 피해보상을 통해 공정성 회복 노력을 기울여야 할 것이다. 아울러, 기업 내부적으로는 윤리교육을 실시하고, 유출과 관련된 내부자를 엄정히 처벌하는 내적 인적 쇄신을 취할 필요가 있다.

5.3 연구의 한계 및 향후 과제

본 연구의 한계와 향후 연구에 대한 제언은 다음과 같다. 첫째, 본 연구에서는 개인정보 유출원인에 따라 배신감, 실망감 등의 정서유발이 어떻게 달라지고, 그로 인해 행동의지에 어떤 차이를 보이는지를 규명하였다. 그러나 부정적 행동을 감소시키기 위해 배신감 및 실망감을 구체적으로 어떻게 다루어야 하는지에 대한 실증적 연구를 제시하지 못했다는 한계점이 있다. 본 연구는 단지 선행연구를 참조하여 그 가능성만을 제시하는데 그치고 있다. 따라서 개인정보 유출로 인해 배신감 및 실망감이 유발된

상황에서 서비스 회복을 위해 필요한 구체적 조치가 무엇인지에 대한 실증 연구를 향후 연구로 제안하는 바이다.

둘째, 본 연구는 기업의 개인정보 유출 상황을 가정한 시나리오 연구라는 한계점이 있다. 가상의 시나리오에 따른 응답을 바탕으로 데이터를 분석하고 연구결과를 제시하였기 때문에 본 연구결과는 실제 개인정보 유출사건이 발생했을 상황에서의 연구결과와 차이가 있을 수 있다. 따라서 이와 같은 점을 보완하여 실제 사건이 발생한 직후, 그 사건의 피해자를 대상으로 하는 실증 연구를 향후 연구로 제안하는 바이다.

참고문헌

강용식 · 권순동(2016), "스마트워크 환경하의 업무성과에 영향을 미치는 요인에 관한 연구," **Journal of Information Technology Applications & Management**, 23(1), 61-77.

개인정보보호위원회(2015), **개인정보보호 연차보고서**.

공옥례 · 이형재(2009), "고객의 부정적 행동과 불만족을 유발하는 감정들의 비교연구," **서비스경영학회지**, 10(1), 271-298.

김대원 · 윤영민(2015), "SNS 에서 형성된 신뢰가 위기 시 방어막이 될 수 있는가," **한국언론학보**, 59(2), 196-225.

문신희(2013), **서비스 실패 상황에서 관계품질과 관계혜택이 지각된 배신감, 관계단절 행동에 미치는 영향: 공기업을 중심으로**, 제주대학교 대학원 석사학위논문.

문신희 · 김정희(2014), "서비스 실패 상황에서 관계품질과 관계혜택이 배신감과 관계단절행동에 미치는 영향: 공기업을 중심으로," **경영교육연구**, 29, 158-190.

박도영(2000), **학구적 知 · 情 · 意와 성취도의 인과구조 분석**, 한국교원대학교 대학원 박사학위논문.

박명호 · 장영혜(2014), "브랜드위기에 따른 브랜드실망감의 파급효과" **소비문화연구**, 17(1), 25-47.

배재권(2016), "빅데이터 환경에서 개인정보유출 위협이 정보보호행위에 미치는 영향에 관한 연구," **e-비즈니스연구**, 17(3), 191-208.

산업연구원(2014), **개인정보 보호와 빅데이터 기술의 산업화**.

원유석(2005), "서비스 실패의 안정성, 통제성이 서비스 회복 패러독스에 미치는 영향에 관한 연구-귀인이론(attribution theory)을 중심으로," **서비스경영학회지**, 6(1), 27-55.

유호범 · 지희진 · 강기두(2013), "서비스 실패의 심각성과 통제성이 회복만족에 미치는 영향," **대한경영학회지**, 26(4), 829-850.

윤일한 · 권순동(2015), "정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구," **Information System Review**, 17(1) 141-169.

이상경 · 이명천(2006), "기업위기에서 기업 이미지가 사과의 수용, 책임 귀인, 반복성 판단에 미치는 영향: 삼성, 현대 자동차 CEO 위기를 중심으로," **홍보학연구**, 10(2), 197-231.

임규목 · 부경희(2015), "개인정보유출에 대한 기업의 위기커뮤니케이션 전략이 수용자의 반응에 미치는 영향," **홍보학연구**, 19(3), 70-94.

장익진 · 최병구(2014), "위험지각과 효능감에 따른 인터넷 사용자의 개인정보 유출예방행위 분석," **한국전자거래학회지**, 19(3), 65-89.

최민홍 역(1986) 플라톤저, **국가론**, 성창출판사.

한국정보보호산업협회(2015), **2015년 국내 정보보호산업 실태조사**.

Ajzen, I. and Fishbein, M.(1983), "Relevance and Availability in the Attribution Process," In J. Jaspars, F. D. Fincham, and M. Hewstone (Eds.), *Attribution Theory and Research: Conceptual Development and Social Dimensions*,

(63-89), London & New York: Academic.

Bell, D. E.(1985), "Disappointment in Decision Making Under Uncertainty," *Operations Research*, 33(1), 1-27.

Damasio, A. R.(2000), "A Second Chance for Emotion," in: Lane, R. D., ed., *Cognitive Neuroscience of Emotion*, Oxford, 12-23.

Ellis, A.(1994), *Reason and Emotion in Psychotherapy*, Birch Lane Press Book.

Falk, R. F. and Miller, N. B.(1992), *A Primer for Soft Modeling*, University of Akron Press.

Feinberg, F. M., Krishna, A., and Zhang, Z. J.(2002), "Do We Care what Others Get? A Behaviorist Approach to Targeted Promotions," *Journal of Marketing Research*, 39(3), 277-291.

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading*, MA: Addison-Wesley.

Folkes, V. S.(1984), "Consumer Reactions to Product Failure: An Attributional Approach," *Journal of Consumer Research*, 10(4), 398-409.

Folkes, V. S., Koletsky, S., and Graham, J. L.(1987), "A Field Study of Causal Inferences and Consumer Reaction: The View from the Airport," *Journal of Consumer Research*, 13 (4), 534-539.

Fornell, C. and Larcker, D. F.(1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research,* 18(1), 39-50.

Frijda, N. H., Kuipers, P. and Ter Schure, E.(1989), "Relations among Emotion, Appraisal, and Emotional Action Readiness," *Journal of Personality and Social Psychology*, 57(2), 212-228.

Huefner, J. and Hunt, H. K.(2000), "Consumer Retaliation as a Response to Dissatisfaction," *Journal of Consumer Satisfaction, Dissatisfaction & Complaining Behavior*, 13, 61-82.

Hess Jr, R. L.(2008), "The Impact of Firm Reputation and Failure Severity on Customers' Responses to Service Failures," *Journal of Services Marketing*, 22(5), 385-398.

Kant Immanuel(1790), *Kritik der Urteilskraft(판단력 비판)*, Berlin und Libau.

Koehler, J. J. and Gershoff, A. D.(2003), "Betrayal Aversion: When Agents of Protection Become Agents of Harm," *Organizational Behavior and Human Decision Processes*, 90(2), 244-261.

Oliver, R. L. (1999), "Whence Consumer Loyalty?" *Journal of Marketing*, 63(4), 33-44.

Ponemon Institute(2016), *Ponemon Cost of Data Breach Study: Global Analysis.*

Rosenberg, M. J. and Hovland, C.I.(1960), "Cognitive, Affective, and Behavioral Components of Attitudes," in Rosenberg, M. J., Hovland, C. I., McGuire, W.J. (eds.), *Attitude Organization and Change,* Yale University Press, New Haven, 1-14.

Symantec Corporation(2016), *Internet Security Threat Report.*

Weiner, B.(1980), "The Role of Affect in Rational (attributional) Approaches to Human Motivation," *Educational Researcher*, 9(7), 4-11.

Weiner, B.(1985), "An Attributional Theory of Achievement Motivation and Emotion," *Psychological Review*, 92(4), 548-573.

Wetzels, M., Odekerken-Schröder, G., and Van Oppen, C.(2009), "Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *MIS*

Quarterly, 177-195.

Zeithaml, V. A., Berry, L. L. and Parasuraman, A. (1996), "*The Behavioral Consequences of Service Quality,*" *The Journal of Marketing*, 60, 31-46.

Zeelenberg, M. and Pieters, R.(2004), "Beyond Valence in Customer Dissatisfaction: A Review and New Findings on Behavioral Responses to Regret and Disappointment in Failed Services," *Journal of Business Research*, 57(4), 445-455.

The Effect of Cognition of Personal Information Leakage Controllability on Affection and Conation: Focused on Comparing between External Hacking and Internal Leakage

Cholong Wi* · Sundong Kwon**

Abstract

Until now, research on Management Information Systems and Information Security has focused on rational aspects such as security technologies and policies that emphasize human rationality. Therefore, there are almost no emotional research such as customer's disappointment or betrayal due to personal information leakage. As a result, corporate responses to personal information leak did not satisfy customers' needs and slowed the speed of service recovery. Therefore, in this study, we applied cognition · affection · conation theory which has been studied in psychology and marketing, to personal information leakage, and found out the relationship between emotion and intention in the accident of personal information leakage. This research model is that controllability of personal information leakage affects affection and then that affection influences conation, while this effect varies depending on the source of the internal leakage and external hacking.

We surveyed people who had experience of personal information leakage. People were asked to respond the scenario of survey, on which the cause of personal information leakage was divided into external hacking and internal leakage. 460 data were collected and Smart-PLS 2.0 tool was used to verify the research model.

The results of this study are as follows. First, the higher controllability of personal information leakage, the higher disappointment and betrayal, and the higher service switching and negative word of mouth. Second, when personal information is leaked by external hacking,

* CAS Corp. First Author
** Professor, Department of Management Information Systems, Chungbuk National University, Corresponding Author

cognition of controllability affects disappointment, and then the disappointment affects negative word of mouth. Third, when personal information is leaked by insiders, betrayal is triggered by cognition of controllability, and conation of service switching is increased.

The contribution of this study can be seen from the academic side and the management side. As the academic contribution, this study applied the psychological theory of cognition · affection · conation to personal information leakage and explained the effect of cognition (of controllability) on affection (of disappointment and betrayal) and conation (of service switching and negative word of mouth), when personal information was leaked. As the management contribution, this study suggested that companies should respond differently according to the causes of personal information leakage. When personal information is leaked by external hacking, companies need to focus on lowering disappointment emotion. For example, it is necessary to lower the customer's expectation, to seek customer's understanding, and to specify as-is and to-be plans. When personal information is leaked by insiders, companies need to focus on lowering betrayal emotion. For example, in order to lower and heal betrayal emotion, companies should humbly acknowledge the responsibility of this mistake first, and make a sincere apology and fair damages compensation.

Key words: External hacking, Internal leakage, Controllability, Disappointment, Betrayal, Word of mouth, Switching, Cognition · affection · conation

• 저자 위초롱은 현재 정보보호 컨설턴트로 재직하고 있다. 충북대학교 경영학부를 졸업하고, 충북대학교 정보보호경영학과에서 석사학위를 취득하였다. 주요 관심 분야는 개인정보 유출 이후 고객의 감정과 행동반응, 개인정보 유출 상황에서 기업의 대응책 등이다.

• 저자 권순동은 현재 충북대학교 경영정보학과 교수로 재직하고 있다. 서울대학교 경영대학에서 경영정보학전공으로 박사학위를 취득하였다. 한국경영정보학회 이사, 한국경영학회 부회장, 한국정보기술응용학회 부회장을 역임하였고, 충북대학교 종합인력개발원장, 학생생활관장을 역임하였다. 주요 관심 분야는 감성(정서)이 IT활용 및 성과에 미치는 영향, 서비스 연계성의 가치, 연결되지 않을 권리 등이다.