Information Systems Review
Vol. 17, No. 1 April 2015 http://dx.doi.org/10.14329/isr.2015.17.1.141

정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구

A Study on the Effect of Information Security Compliance and Crisis Management on Information Security Trust

윤 일 한 (Il-han Yoon) 충북대학교 정보보호경영학과 석사과정
권 순 동 (Sun-dong Kwon) 충북대학교 경영정보학과 교수, 교신저자

요 약

전자금융 관련 사고에서는 개인정보 유출이 가장 많이 일어나고 있으며 개인정보 유출로 인한 보이스피싱 등의 2차 피해가 일어나 사회적으로 막대한 손실을 가져와 문제가 되고 있다. 본 연구는 대량의 개인정보 유출 시 금융정보보안 위험을 효과적으로 낮추기 위한 방안을 사전대응・사후대응・개인정보 유출자 관점으로 나누어 살펴보았다. 구체적인 연구모형은 금융정보보안 컴플라이언스가 금융기관 및 금융당국의 위기대응에 영향을 미치고 이러한 위기대응 활동은 금융정보보안 신뢰에 영향을 미친다는 것이다. 실증연구를 위해 개인금융정보 유출 경험이 있는 사람들을 대상으로 설문지를 배포하였고 총 103부의 설문지를 회수하여 분석하였다.

실증분석 결과, 금융정보보안 컴플라이언스는 금융당국에 더 큰 영향을 미치는 것으로 나타났고, 금융기관 위기대응과 금융당국 위기대응은 금융정보보안 신뢰에 영향을 미치는 것으로 나타났다. 조절효과 분석에서 개인금융정보 중요도는 금융기관 위기대응이 금융정보보안 신뢰에 미치는 영향을 조절하는 것으로 나타났고, 개인금융정보 유출수준은 금융당국 위기대응이 금융정보보안 신뢰에 미치는 영향을 조절하는 것으로 나타났다. 이러한 분석이 시사하는 바는 다음과 같다.

첫째, 컴플라이언스에 대한 관리・감독을 철저히 할 필요가 있다. 금융당국은 금융기관이 금융정보보안 컴플라이언스를 준수하고 있는 지에 대한 관리 감독을 철저히 하고, 정부부처 별로 흩어져있는 대응체계를 효과적으로 컨트롤할 수 있어야 한다. 둘째, 금융기관은 전자금융 정보보안 신뢰를 위해서 돌발적인 보안사고에 대처할 수 있는 능력을 갖추고 고객정보 관리에 대한 컨트롤타워를 마련하여 계열사에게 분산 공유되는 정보를 통합관리할 필요가 있다. 셋째, 이용자 금융정보의 중요도와 유출수준이 높은 집단이 금융정보보안 신뢰회복 수준이 낮게 나타났다. 따라서 정보보안 위기상황 시에 맞춤대응 전략을 개발하여 대응함으로써 금융정보보안 신뢰를 효과적으로 회복할 수 있다.

키워드 : 전자금융, 금융정보보안 신뢰, 정보보안 컴플라이언스, 개인금융정보

† This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA (Korea Internet Security Agency)(H2101-15-1001).
2014년도 경영정보학회 추계학술대회 최우수논문상을 수상한 논문임.

Ⅰ. 서 론

인터넷 뱅킹은 전자금융 이용수단 중 하나로 최근 들어 심각한 정보보안 위협에 직면하고 있다. 전자금융 보안과 관련된 대표적 사건으로 2013년 1월 7일 우리나라에서 농협은행, 국민카드, 롯데카드 등의 은행과 카드 사에서 총 1억 400만 건의 고객정보가 유출되는 사상 초유의 정보보안 사고가 일어났고, 금융당국은 2014년 1월 8일 이를 공표하였다. 이는 지금까지 개인정보 유출 사건 중 단일사건으로는 가장 많은 개인정보가 유출된 사건이다. 유출된 내역을 살펴보면 개인별로는 최대 20가지 전후의 개인정보가 유출되었고, 이중에는 신용등급, 연 소득, 주거현황, 직장 등 민감한 개인정보 등이 포함되어 2차 피해가 우려되고 있다(한국경제, 2014).

이와 같은 개인정보 유출은 전자금융에 대한 신뢰를 약화시켰다. 실제로 개인정보가 유출된 카드사의 카드 재발급·해지·탈회 건수를 보면 <표 1>에서 보듯이 신뢰회복은 안전한 금융거래를 위해 선결되어야 하는 요인이다.

지속적인 금융보안 사고의 발생은 결국 금융정보보안 신뢰 하락으로 이어진다. 따라서 보안사고에 대한 방어대책이 요구되는데 그동안의 보안대책은 기술적인 방법에 치우쳐 있었다. 기술적인 보안대책의 개발은 많은 시간과 비용이 드는데 반해 해킹 기술은 정교하지 않은 방법으로도 정교하게 만들어진 기술적인 보안을 뚫는 경우가 상당히 많이 있다. 또한 전자금융이 정보시스템을 이용하여 서비스를 제공하는 한 해킹에 의한 사고는 계속적으로 일어나는 환경에 처해있다고 할 수 있다.

따라서 금융정보보안에 대한 대응은 정보 유출로 인한 피해를 최소화하는데 목적을 두어야 한다. 본 연구에서는 이러한 필요성을 절감하여 보안사고의 사전대응 요인으로 금융정보보안 컴플라이언스를 도출하였는데 보안의 시작은 각종 법률·정책적인 규제나 가이드라인을 준수하는 것부터 시작되기 때문이다. 또한 사전대응 요인과 조화를 이룰 수 있게 사후대응 요인으로서 금융기관과 금융당국의 위기대응을 요인으로 도출하였는데 위기대응의 본질이 정보보안 사고의 위험을 최소화하는 과정이기 때문이다.

한편, 본 연구에서는 조절효과로서 최근 심각한 보안 위협으로 떠오르고 있는 개인정보와 관련하여 개인정보 중요도와 개인정보 유출수준이 금융기관과 금융당국의 위기대응 시 어떠한 영향을 미치는지 알아보았다. 개인정보나 프라이버시에 대한 염려가 정보시스템 이용에 영향을 미친다는 기존의 연구들은 본 연구의 상황보다 일반적인 상황인 경우가 대부분이다(기소진, 이수영, 2013; Milne *et al*., 2009; 장익진, 2009; 박정훈, 이숙현, 2007; Bellman *et al*., 2004). 여기서의 일반적인 상황이란 실제로 개인정보 유출이 없었거나 상대적으로 개인정보 유출이 적은 상황이다. 본 연구의 1억 건이 넘는 개인정보 유출은 일반적인 상황과는 다른 민감한 시기에서의 상황을 배경으로 하고 있다. 따라서 이러한 상황

〈표 1〉 정보 유출 3개 카드사 재발급·탈회 현황

구 분	K카드	L카드	N카드
재발급	125만 3000건	99만 3000건	158만 6000건
해지	97만 3000건	50만 9000건	80만 1000건
탈회	28만 5000건	28만 6000건	33만 7000건
카드해지비율	8.30%	5.90%	12.00%

주) 2014 1월 20일~2월 1일까지의 누적 카드 수 기준.
자료: 각사 업무보고서.

하에서 개인정보 중요도와 개인정보 유출수준의 정도가 금융소비자의 성향에 따라 다르게 나타난다면 금융권이 일반적인 상황과는 다른 위기 상황 시에 전자금융 소비자의 성향에 따라 개인정보 유출 문제 해결을 위해 어떠한 노력을 해야 하는지에 대한 시사점을 줄 수 있을 것이다.

Ⅱ. 전자금융 정보보안 현황 및 선행연구

2.1 전자금융 보안사고 현황

전자금융(electronic finance)의 정의는 다양한데 금융정보화추진분과위원회 사무국 한국은행 금융결제국(2009)에 따르면 “은행, 증권회사 및 보험회사 등의 금융기관이 컴퓨터, 정보통신기술 등을 활용하여 금융업무와 관련한 시스템을 전산화하고 금융상품의 판매, 금융서비스 채널의 제공, 지급결제 등 금융업무 및 관련 부수 업무를 전자적 방식에 의해 처리하는 것”으로 정의하고 있다.

본 연구에서는 전자금융 중에서 인터넷 뱅킹에 초점을 두고 있다. 김현욱 등(2002)에 따르면 인터넷 뱅킹은 고객이 인터넷을 통한 금융제반 업무를 처리하는 시스템을 지칭하는 것으로서, 넓은 의미에서 인터넷 뱅킹과 전자금융이 같은 의미로 혼용되고 있다. 이상의 의미를 종합하면 전자금융이란 소비자가 금융회사의 점포를 직접 방문하지 않고 인터넷 등의 네트워크 시스템을 이용하여 금융관련 업무를 처리하는 것이라고 정의할 수 있다.

전자금융 보안사고의 심각성을 알기 위해서는 지금까지의 현황 파악이 중요한데, 금융보안사고는 사고 그 자체보다 금융정보가 유출되어서 일어나는 2차 피해가 훨씬 심각하다.

<표 2>는 2009년부터 전자금융 사고현황을 정리해놓은 것으로 지속적으로 전자금융 정보보안사고가 일어나고 있으며 주로 개인정보 유출과 관련하여 문제가 됨을 알 수 있다. <표 3>에서는 정보기술관련 사고 중 전자금융 사고의 규모가 큼을 알 수 있다.

<표 4>에서 최근 5년 동안 전자금융사기 피해현황을 보면 보이스피싱은 해마다 줄고 있지만 피해액은 3700억으로 가장 많았다. 신종 전자금

〈표 2〉 전자금융 사고 현황

구 분	발생일	금융회사명	사고 개요
DDoS 공격 (2건)	2009년 7월	7개 은행	DDoS 공격으로 인터넷 뱅킹 서비스 일시중단
	2011년 3월	D증권	약 3시간 동안 DDoS 공격으로 접속지연
정보 유출 (6건)	2009년 9월	○○캐피탈	홈페이지 해킹으로 고객정보 유출
	2011년 4월	H캐피탈	공개용 웹 서버 해킹으로 고객정보 유출
	2011년 4월	S신용정보	홈페이지 해킹으로 고객정보 유출
	2011년 5월	N증권	홈페이지 해킹으로 고객정보 유출
	2011년 5월	R증권	홈페이지 해킹으로 고객정보 유출
	2011년 6월	N증권	프로그램 오류로 타 고객에게 매매내역 노출
	2013년 3월	S은행, N은행	개인정보 유출
	2013년 4월	J은행, C은행	개인정보 유출
	2014년 1월	K은행 · N은행 · L카드	개인정보 대량 유출
해킹장애(1건)	2011년 4월	N중앙회	해킹으로 인한 영업점, 인터넷 뱅킹 등 장애

자료: 위키피디아, 금융감독원(원 자료의 내용을 저자가 수정 · 보완).

〈표 3〉 정보기술부문 및 전자금융 사고 발생현황

(단위: 건, 백만 원)

구 분		2004년	2005년	2006년	2007년	2008년	2009년	2010년	2011년	2012년	2013년 6월
IT 보안사고	건수								8	9	8
전자금융사고	건수	20	11	2	23	10	24	16	10	82	224
	금액	192	411	15	331.5	428.0	384.2	591.6	130.3	2058.9	2271.3
정보기술장애	건수	20	17	20	30	25	7	22	34	102	143

자료: 금융감독원.

〈표 4〉 전자금융사기 피해 현황

(단위: 건/백만 원)

시기	보이스피싱		파밍		스미싱		메모리해킹		총계	
	건수	피해액	건수	피해액	건수	피해액	건수	피해액	건수	피해액
2009	6,720	62,100							6,720	62,100
2010	5,455	55,400							5,455	55,400
2011	8,244	101,900							8,244	101,900
2012	5,709	59,500							5,709	59,500
2013	4,749	55,300	3,218	16,424	76,356	4,807	463	2,762	84,786	79,293
2014년 6월	2,851	36,900	1,628	6,842	4,459	276	97	522	9,035	44,540
합계	33,728	371,100	4,846	23,266	80,815	5,083	560	3,824	119,949	402,733

자료: 경찰청(스미싱은 전화결제산업협회)/파밍, 스미싱, 메모리해킹은 2012년 이후 신종 범죄.

융사기인 스미싱은 작년 한해만 7만 600건의 피해가 발생해 건수가 가장 많았다. 이는 개인정보 유출로 인한 2차 피해가 개인정보 유출 자체보다 심각함을 알 수 있다(전자신문, 2014). 2013년을 기준으로 피해건수가 갑자기 늘어난 것은 본 연구의 동기가 된 카드 3사 등의 개인정보 유출 사건과 시기적으로 일치하므로 1억 건이 넘는 개인정보 유출이 실제 2차 피해와 직결된다고 추정할 수 있다.

전자금융 정보보안 사고에 대한 이상의 자료를 종합해보면 사고 발생 건수는 일정치 않지만 피해규모가 증가하고 있는 것을 알 수 있다. 또한 개인정보 유출이 실제 2차 피해와 직결되는 것은 금융소비자에게 있어서 심각한 위협이 된다. 따라서 금융권은 이와 같은 보안사고로 인한 피해규모를 줄이기 위해 노력해야 한다. 본 연구에서는 이와 같은 전자금융 정보보안 사고를 줄이기 위한 대응방안에 초점을 두고 있다.

2.2 전자금융 정보보안 관련 선행연구

전자금융과 관련한 일련의 보안사고들이 지속적으로 발생하고 있고 개인정보보안에 대한 관심이 높아지면서 이에 대한 다양한 연구가 시도되었다. 전자금융 사고와 관련한 기술적 측면의 연구와 관리적 측면의 연구가 주를 이루었고 전자금융 정보보안 준수를 통한 조직혁신, 조직성과 관점에서도 연구가 되었다. <표 5>에서 보듯이 기존의 연구들은 주로 현황파악이나 정책개발, 기술적 대책을 제시하는 연구가 주를 이루었다. 본 연구에서는 초점을 달리하여 대량의 개인정보 유출시 금융소비자의 인식이 정보보안 사고의

〈표 5〉 전자금융 정보보안 관련 6선행연구

관점	연구자	연구내용
기술 관점	김소이 (2009)	◦ 전자금융 사고를 기술적 유형으로 분류하고 사전대응과 사후대응을 각종 기술적 측면에서 제시 ◦ IT 보안대책 준수를 제시하고 사후대응으로 손해배상과 피해규모 최소화 방안을 제시
	이수미 등 (2011)	◦ 국내 전자금융 현황을 조사하고 네트워크, 전자적 장치 등의 전자금융 구간별로 발생한 또는 발생 가능한 전자금융 보안위협을 제시
	이상진 (2005)	◦ 인터넷을 이용한 금융거래 시 보안성 강화 수단에 관해 공인인증서의 문제점, 메모리 해킹의 문제점을 지적하고 스마트카드나 USB 토큰 등의 강력한 개인정보보호 매체의 도입 필요성을 제안
정책 관점	김영태 (2012)	◦ 전자금융 정책 및 감독 선진화를 위한 주요국 사례분석에서 주요국의 조사결과를 바탕으로 전자금융 활성화 방안과 관련하여 정책적 관점에서 금융기관이 다양한 공격 및 사고에 대응하기 위한 인증 및 정보보안 관리/통제를 통한 보안대응 강화를 제시 ◦ 관리적 측면에서 금융기관에서 정보보호 관리체계에 관한 표준도입의 시급성 지적
	한세진 (2013)	◦ 개인정보보호법과 기존의 금융 관련 개별법간의 상충되는 측면을 현장 실태조사 자료를 기반으로 개인정보관리 전반에 대한 문제점을 지적 ◦ 해결방안으로 개인정보보호 체계를 전적인 정부주도 보다는 일정 부분은 산업분야 자율에 맡기는 것이 산업 활성화 측면에서 바람직하다고 제시
	김태호 등 (2008)	◦ 인터넷 전문은행 설립 시 예상되는 전자금융 리스크와 관련한 연구에서 인터넷 전문은행 설립 시 예상되는 보안 리스크와 인터넷을 중심으로 각국의 사례를 연구
	조성인 (2008)	◦ 전자금융거래법에서의 전자금융사고 대응방안에 관한 연구에서 전자금융사고 발생 현황을 은행/증권/보험/카드로 나누어 조사 ◦ 전자금융거래법 시행에 따른 금융회사의 금융사고 대응 한계를 지적하고 해결방안으로 IT 컴플라이언스 기능 강화를 통해 금융회사가 대응해야 함을 제시
	이병수 등 (2013)	◦ 국내 시중에 304개 금융회사를 대상으로 한 연구에서 개인정보 수집·이용 제공 동의서 운영실태 점검 결과 총 49개 금융회사에서의 개인정보관리 문제를 발견 ◦ 해결책으로서 금융기관이 개인정보의 법적 IT 컴플라이언스 준수의 공감대 형성을 제시
	조화제, 김귀남 (2008)	◦ 원래 군사 전략이었던 종심방어 전략을 금융 정보보호에 도입하기 위한 방안으로 정보보호 아키텍처 수립, 정보보호 기준 확립, 평가된 제품의 획득 및 통합, 시스템 위험평가 등을 제시
	이정호 (2008)	◦ 인터넷 뱅킹을 중심으로 전자금융 침해사고 발생현황을 조사하고 효과적인 대응방안으로 공인인증서를 중심으로 한 전자금융 접근매체 강화방안을 제안 ◦ 전자금융 서비스를 제공하는 금융기관과 금융감독 기관이 유기적인 공조를 기반으로 한 침해사고 공동대응체계의 구축 및 운영을 위한 시스템의 구성방법, 운영 프로세스, 관련 법률의 검토 및 대응 방법 등을 제안
조직 혁신 관점	이장형 (2010)	◦ 금융기관의 보안과 통제가 ERP 시스템에 미치는 영향에 관한 실증연구를 금융기관의 901명의 종업원을 대상으로 실시하여 보안과 통제에 관한 위험평가, 문서보안, 감시활동 등의 요인을 도출 ◦ 이들 요인이 ERP 시스템 성과에 유의미한 영향을 미치는 것을 실증함
	김근아 (2013)	◦ 인터넷을 이용한 금융거래 시 보안성 강화 수단에 관해 공인인증서에 문제점, 메모리 해킹의 문제점을 지적하고 스마트카트나 USB 토큰 등의 강력한 개인정보보호 매체의 도입 필요성을 제안

대응 틀을 다시 세우는데 중요한 영향을 미치는 것으로 보아 이에 대한 실증분석을 하였다.

2.3 금융정보보안 신뢰회복의 영향요인 및 선행연구

본 연구에서는 대량의 개인정보 유출 시에 금융정보보안 신뢰회복을 위해 어떻게 금융기관과 금융당국이 대응을 해야 하는지에 관한 연구이다. 그러므로 금융정보보안 신뢰회복에 영향을 미치는 주요 연구변수를 살펴보면 다음과 같다.

2.3.1 금융정보보안 컴플라이언스

베버는 컴플라이언스를 “전통, 감성적인 믿음, 가치적인 믿음이 조직 구성원의 합법적인 약속을 바탕으로 한 실천적인 규약”으로 정의하고 있다(Weber, 1997). 기업은 위험관리를 위해서 법령준수 등을 통한 컴플라이언스 체제를 정비하게 한다. 기업 컴플라이언스에는 법령뿐만 아니라 사회규범도 포함해야 된다. 법령과 사회규범이 모두 고려된 기업 컴플라이언스는 법령위반을 저지하면서도 회사 외부의 권한당국에게는 기업이 법령위반을 방지할 조치를 취하고 있다는 신뢰를 준다(육태우, 2013; 落合誠一, 2012; Baer, 2009).

이상의 내용을 종합하면 금융정보보안 컴플라이언스란 “외부 규제나 표준을 정의하고 지속적인 관찰을 통해 준수여부를 확인하며, 발견된 문제를 개선하고 발전시켜나가는 활동”이라고 정의할 수 있다(디지털타임스, 2008). 금융정보보안 컴플라이언스와 관련된 현행 법률로는 전자금융거래법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신기반 보호법, 신용정보의 이용 및 보호에 관한 법률, 개인정보보호법, 금융실명거래 및 비밀보장에 관한 법률, 자본시장과 금융 투자업에 관한 법률 등이 있으며 세부적인 내용은 다음과 같다(한국인터넷진흥원, 2010b).

이러한 금융정보보안 컴플라이언스는 정부측면에서는 전술한 선행연구에서 보듯이 기업을 관리하고 통제하는 시스템의 일환이고, 기업 측면에서 조직성과나 조직혁신 등에 영향을 미친다

〈표 6〉 전자금융 관련 법률

법률	소관부처	법률내용
개인정보보호법 (2011년 3월 29일)	행정자치부	개인정보의 수집·이용·제공·파기에 관한 규제, 개인정보의 안전한 관리, 손해배상의 입증책임의 전환 미 개인정보 단체소송 도입을 규정
금융실명법 (1997년 12월 31일)	금융위원회	실지 명의에 의한 금융거래에 관한 상세한 기준 준수의무를 규정
신용정보보호법 (1995년 1월 5일)	금융위원회	개인·법인 신용정보의 수집·이용·제공에 관한 규제, 신용정보전산시스템의 안전보호를 위한 기술적·물리적·관리적 보안대책 수립의무, 손해배상 입증책임의 전환을 규정
전자금융거래법 (2006년 4월 28일)	금융위원회	전자거래 안정성 확보와 이용자 보호를 위한 각종 의무·인력·조직관리, 외주관리 시설설비기준, 정보기술 시스템 상 보호관리대책(해킹방지, 계정관리 등), 내부통제에 관한 상세한 기준 준수의무를 규정
전자상거래법 (2002년 7월 24일)	공정거래 위원회	전자상거래 및 통신판매 등에 의한 재화 또는 용역의 공정한 거래에 관한 사항을 규정
정보통신망법 (2001년 1월 16일)	방송통신 위원회	개인정보의 수집·이용·제공·파기에 관한 규제, 개인정보보호를 위한 기술적·관리적 조치 의무 및 기준 준수 의무를 규정
전자거래기본법 (1998년 2월 8일)	미래창조 과학부	전자문서의 효력 및 암호기술사용, 전자거래 사업자의 일반적인 준수사항, 전자거래 사업자에 대한 인증을 규정

(김근아 등, 2013). 영미권에서 컴플라이언스는 금융조직의 경영투명성을 확보하기 위해 발전했는데 사베인-옥슬리법(SOX)은 회계감사의 투명성 제고, 바젤 II(자기자본규제법)은 금융권 리스크 관리와 관련된 내용을 담고 있다(조창훈, 이정진, 2013; 디지털타임스, 2008).

기업의 사회적책임(corporate social responsibility)이 개인 프라이버시・지적재산권보호 등과 관련하여 증가하고 있으며, 개인정보 유출・내부자에 의한 기밀 유출 등으로 내부통제가 강화될 필요성이 증대하고 있고, 또한 사회 환경변화와 맞물려 정보보호 관련 법률 제정 및 제도가 강화되고 있다(박준호, 2011). 국내의 전자금융 분야도 보안사고가 지속적으로 발생함으로써 금융정보보안 컴플라이언스 준수가 중요해지고 있다.

2.3.2 금융기관 위기대응

전자금융 침해사고 발생 시 이를 해결하기 위한 금융기관(financial institution)의 노력이 필요하다. 금융기관의 개인정보 유출은 기업측면에서 보면 서비스 실패라고 할 수 있다. 따라서 서비스 실패 후 기업은 이를 만회하기 위해 노력을 기울이게 된다(Goodwin and Loss, 1998). 금융기관 입장에서는 조직의 명성에 치명적인 흠집을 예방하고 피해를 최소화하기 위해 실추된 이미지를 빠르게 회복하는 것이 신뢰회복의 관건이다(Jarvenpaa and Todd, 1996).

보안사고에 대해서 금융기관은 공정한 위기대응을 해야 하는데 이를 세분화하면 절차 공정성(procedural justice)・상호작용 공정성(interaction justice)・분배 공정성(distributive justice)으로 나누어진다(Goodwin and Ross, 1992; Hocutt *et al*., 1997; Tax *et al*., 1998; Tax and Brown, 2012). 절차 공정성이란 교섭이나 의사결정과정이 공정해야 한다는 것으로 전자금융 소비자는 보안사고 발생의 처리과정이 절차적으로 공정하길 원한다. 상호작용의 공정성은 서비스 실패 후 만회 절차와 결과가 공정했음에도 인간적인 측면에서 공정한 대우를 받았는지에 대한 자각으로 보안사고에 대한 민원을 해결하는 과정에서 직원이 전자금융 소비자에게 최선을 다하고 있다는 인식을 주는 것을 말한다. 분배 공정성은 상호의존적 관계에 있어서 서로에게 할당된 몫을 배분하는 방법이 얼마나 공정한가에 대한 지각으로 보안사고의 배상과정에서 피해자가 인식하기에 합당한 보상을 하는 것을 말한다. 이러한 공정성이론은 기업의 서비스 실패에 대해 기업이 고객의 불만족을 해결하기 위한 제반 활동을 다루고 있다(Grönroos, 1998).

2.3.3 금융당국 위기대응

금융당국(financial authority)은 위험관리기관으로서 정책을 결정하고 의사결정을 수행한다. 일반시민은 정부의 위험관리역량에 대해 평가를 하게 되고 이러한 평가가 정부에 대한 신뢰로 이어지게 된다(Eiser, 1990). 금융당국은 정보보안 사고 발생 후 위험관리의 일환으로서 이를 수습하기 위한 대책을 마련하고 실행한다(White and Eiser, 2006). 즉, 정보보안 사고에 대한 위기대응은 정부의 위험관리 정책의 일환이라고 할 수 있다(White and Eiser, 2006). 정부가 금융정보보안에 대한 각종 규제를 만들어 준수하게 하였는데도 사고가 일어난 것은 금융기관이 법률적인 규제나 제도를 준수하지 않은 측면도 있고 금융당국이 감독기관으로서 제 역할을 다하지 못한 측면도 있다. 따라서 개인정보 유출사고는 금융기관만의 책임이 아닌 금융당국과 공동의 책임인 것이다.

정보보안 사고는 “정보화 사회를 배경으로 발생하는 대표적인 인위적 위험이며 동시에 기술위험”이다(Chung, 2011). 이러한 위험은 기술적 측면・사회적 측면에서 문제가 되고 있다. 기술적인 측면에서 정부는 보안기술에 대한 가이드라인을 제시해서 기업이 준수하게 해야 하고 기업은 이를 따라야 한다. 사회적 측면에서 정보보안 사고는 더 이상 기업의 책임만이 아니라 개인정보 유출처럼 정부가 보호해야하는 사회적인 문제이다. 따라서 정보보안 사고는 기업뿐만 아니라 정부의 신

뢰 문제로 직결된다(최진혁, 2010, White and Eiser, 2006; Eiser, 1990).

2.3.4 개인정보와 개인정보 유출

개인정보의 유출은 단순히 정보시스템에 위협을 미치는 것을 떠나서 위의 여러 개인정보 사고 관련 현황 표에서 본 것처럼 기업의 사활이 걸린 문제로 대두되고 있으며, 기업뿐만 아니라 정부의 보안정책 신뢰에도 중요한 영향을 미치는 요인으로 대두되고 있다. 개인정보보호법 제2조 제1호에 따르면 “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다고 정의하고 있다. 이중 개인금융정보는 개인정보의 유형 중 재산적 정보에 속한다.

정보시스템 위험관리에서 개인정보는 보호해야할 자산으로서 중요하게 다루어진다(Boehmer, 2009). 정보시스템 자산이란 “조직이나 개인이 가지고 있는 유형·무형의 가치가 있는 재화나 서비스를 지칭하며, 물리적인 자산, 소프트웨어 자산, 조직이나 개인의 무형 이미지 등을 포괄하는 개념”으로 사용된다(김종기, 이동호, 2005). 개인정보에 관한 연구에서 개인정보는 정보시스템 위협이나 위험에 영향을 미치는 요인으로서 정보보안 사고 시 정부와 기업의 위기대응에 영향을 미치는 요인이라고 할 수 있다(김정덕, 2008). 또한 과거의 개인정보는 데이터베이스에 저장되어 있는 것이 아닌 문서로 기록된 것이어서 유출이 되어도 그 정보를 축적하여 개인에 관한 신상을 알아내는데 한계가 있었다. 그러나 현대사회에서는 합법적으로 개인정보를 수집·축적·활용하는 정보시스템의 등장으로 정보시스템 해킹만으로도 개인에게 심각한 위협이 될 수 있다(윤상오, 2009). 개인정보 유출의 심각성을 정부에서도 인식하여 최근에는 개인정보보호법이나 전자금융거래법, 신용정보보호법 등에서도 개인에 관한 정보의 활용이나 폐기에 관한 규정이 있고 이를 어길시 처벌규정을 두고 있다.

개인정보와 개인정보 유출자의 관계를 보다 명확히 하기위해 프라이버시에 대한 이론을 살펴보면 프라이버시 염려에 대한 인식 수준에 따라 개인정보 유출자의 정보보호에 대한 인식이 달라진다는 많은 연구들이 있다(기소진, 이수영, 2013; Pavlou, 2011; 이미나, 심재웅, 2009; buchanan *et al*., 2007; Harris, 2004; Malhotra *et al*., 2004; Smith *et al*., 1996). 본 연구는 사상초유의 개인정보 유출을 배경으로 하고 있다. 기존의 프라이버시에 대한 이론에 따르면 프라이버시 염려에 대한 개인의 인식은 외적인 영향을 많이 받는다고 한다(이미나, 심재웅, 2009). 그러므로 본 연구가 대상으로 하는 개인정보 유출자의 개인정보에 대한 인식은 연구 당시의 상황에 영향을 받아 기존의 일반적인 상황에서의 연구와는 다른 결과를 가져올 것이다.

Ⅲ. 연구모형 및 가설

3.1 연구모형

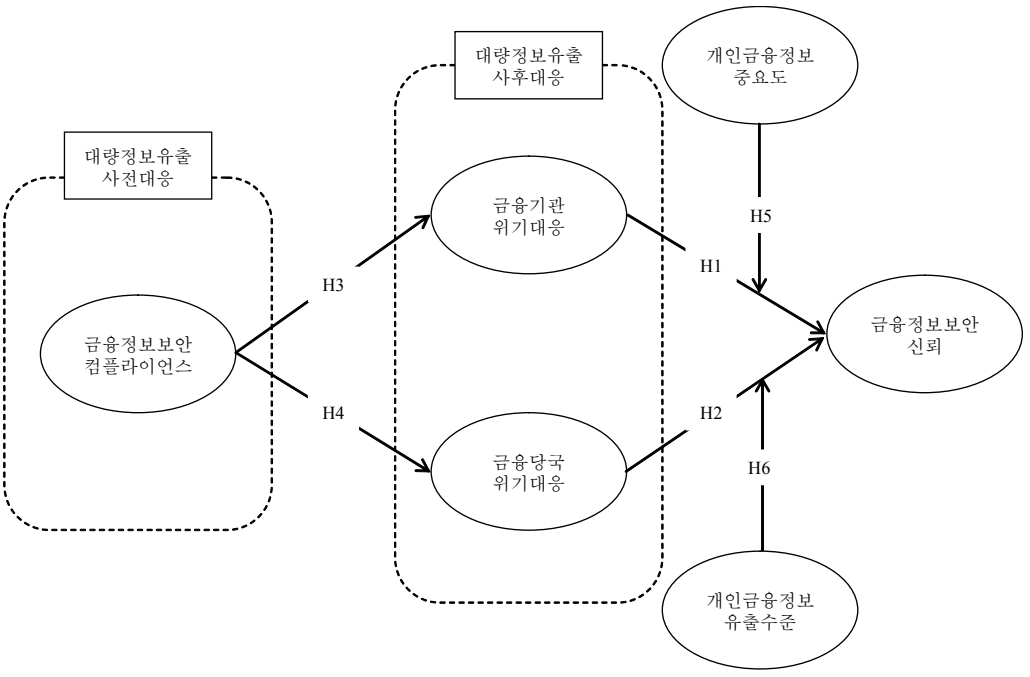
본 연구의 목적은 대량의 개인정보 유출 시 금융권의 사전대응과 사후대응을 통한 금융정보보안 신뢰를 향상시키는 방안을 도출하는 것이다. 기존의 전자금융 정보보안에 관한 연구는 기술적인 보안방법을 제시하고 있는 경우가 많았다(이준택, 차인환, 2013; 신용녀 등, 2011; 이정호, 2008; Kalakota *et al*., 2002). 본 연구에서는 기존의 경영정보학 분야의 기술적인 전자금융 정보보안에 대한 연구를 수용하면서도 정보보호학과 법학의 금융정보보안 컴플라이언스, 개인금융정보의 중요도와 행정학의 위기관리 이론을 통해 도출한 금융기관 위기대응 및 금융당국 위기대응을 함께 고려하였다.

많은 경우 정보보안 문제가 기술적인 대응책

에만 관련되어 있다는 시각에서는 정보보안 문제를 첨단 기술과 새로운 보안 알고리즘 개발을 통해 해결 가능하다고 보는데 이는 새로운 침해기술이 등장하면 이에 대응하는 보안기술이 개발되어야 하는 끝나지 않는 순환과정으로 이어지게 된다(Chung, 2011). 따라서 정보보안 문제를 다루는 시각을 넓혀서 의도치 않거나 바람직하지 않은 사건이나 사고로 보안 문제를 인식한다면 예방과 사후처리에 중점을 두어 정보보안을 관리할 수 있을 것이다(정익재, 2007). 정보보안은 결국 위험관리의 문제이며 위험관리는 위험을 소멸시키는 것이 아닌 위험을 회피하거나 위험을 줄이는 것에 중점을 둔다.

현재 국내의 전자금융 정보보안을 관리하는 정부조직을 보면 금융위원회, 방송통신위원회, 행정자치부, 국가정보원, 미래창조과학부 등에서 관련된 업무를 담당하고 있으며, 정보보안에 대한 법령 또한 금융위원회의 전자금융거래법·신용정보보호법, 방소통신위원회의 정보통신망법, 행정자치부의 개인정보보호법, 개인정보보호위원회의 개인정보보호법 등으로 혼재되어 있다. 금융기관과 관련해서도 기업 내에서 계열사를 관리하고 정보보안에 대한 컨트롤을 할 수 있는 시스템이 마련되어 있지 못하다. 이는 정보보안 관리에 대한 비용증가로 이루어지고 기업이나 국가차원에서 큰 손실로 이어진다.

따라서 전자금융 정보보안에 대한 문제는 정보보안에 대한 사전대응과 사후대응 과정이 조화를 이루어야 하며 민간과 공공부문의 협력을 통한 대응이 필요하다. 본 연구모형에서 이러한 정보보안 정책의 필요성을 절감하여 연구모형으로 <그림 1>을 도출하였다. 금융정보보안 컴플라이언스는 사전대응 요인으로 설정하였고 금융기관·금융당국의 전자금융 위기대응은 사후대응 요인으로 설정하였다. 그리고 본 연구모형에서는 개인정보 중요도와 유출수준을 위기대응이 금융정보보안 신뢰에 영향을 조절하는 요인으로 설정하였다.



〈그림 1〉 연구모형

3.2 가설의 설정

3.2.1 금융기관 위기대응과 금융정보보안 신뢰와의 관계

신뢰에 관한 일반적인 정의를 살펴보면 신뢰란 "자신감을 가지고 있는 또 다른 당사자에 대해 기꺼이 의지하려는 성향"이라고 한다(Moorman *et al*., 1992). 정기한 등(2007)은 기업의 사회적 책임에 대한 연구에서 경제적 책임, 법적 책임, 윤리적 책임, 자선적 책임 등이 기업의 이미지를 제고시켜 고객신뢰로 이어짐을 실증하였다. 이를 정보보안 사고에 비추어보면 개인정보 유출이라는 기업의 위기상황에 대한 대응으로 경제적 책임, 법적 책임, 윤리적 책임을 회피하지 않고 자신감을 가지고 최선을 다하면 전자금융 소비자는 금융기관에게 의지하려 할 것이다. ***금융기관 신뢰***에 관한 연구를 살펴보면, Jarvenpaa and Todd(1996)는 인터넷 구매환경에서 신뢰란 위험의 인식도를 감소시키는 것이라고 하였다.

인터넷 뱅킹과 같은 온라인 환경은 물리적 접촉 없이도 쉽게 범죄가 일어나고 그 결과가 이용자의 부정적 행동으로 나타나 신뢰나 고객만족에 영향을 미친다(Cheung and Lee, 2006; Cunningham *et al*., 2005; Einwiller and Will, 2001; Schlosser *et al*., 2006; Kuhlmeier and Knight, 2005; Laforet and Li, 2005; Pires *et al*., 2004). 따라서 개인정보 유출로 인한 정보보안 사고는 전자금융 소비자가 향후 전자금융을 이용하는데 부정적인 영향을 미친다. 기업은 이러한 상황을 해결하기 위해서 정보보안사고가 일어났을 때 서비스를 정상화하기 위해 적정한 노력을 기울여야 한다. 기업 차원에서 서비스 회복이란 결국 위기에 대한 대응이라고 할 수 있다. 금융기관이 위기대응을 잘하면 고객은 금융기관에 의지하게 되고 결국 정보보안 위험의 인식도 감소를 통해 금융기관 신뢰로 이어질 것이다. 이러한 금융기관 신뢰에 관한 논의를 통해 다음과 같은 가설을 도출하였다.

가설 1: 금융기관의 정보보안 사고 위기대응 수준은 금융정보보안 신뢰에 긍정적인 영향을 미칠 것이다.

3.2.2 금융당국 위기대응과 금융정보보안 신뢰와의 관계

금융당국 신뢰에 관한 정의를 보면 "정부가 시민들이 신탁한 일을 시민들의 이익을 위해 유능하고 올바르게 수행할 것이라는 기대에 대한 긍정적 피드백"로 정의 한 경우도 있고(김왕식, 2011), "정부가 시민들이 신탁한 일을 시민들의 이익을 위해 유능하고 올바르게 수행할 것이라는 시민들의 기대"로 정의한 것이 있다(박종민, 배정현, 2011). 이상의 정부 신뢰에 관한 정의를 종합해보면 정부의 위기관리에 대한 신뢰란 정부가 투명하고 공정하게 최선을 다해 위기상황에 대응 할 것이라는 믿음이라고 할 수 있다. 최진식, 강영철(2012)은 정부신뢰에 관한 연구에서 위험관리 역량요인으로 위험반응의 적절성·위험 식별능력·위험 공개(위험을 투명하게 드러내는 것)의 요인들이 정부의 위험관리 신뢰에 영향을 미치는 것임을 실증하였다.

금융정보보안 사고에 대한 정부의 위기관리 역량은 금융당국이 사고에 대해 얼마나 신속하게 대응했는가, 사고조치가 적절했는가, 책임 있는 사고관련자에 대한 처벌이 이루어 졌는가에 대한 금융소비자의 인식수준이라고 할 수 있다. 금융당국이 실제 정보보안 사고 발생 시 위 요소들을 고려하여 대응한다면 금융소비자는 금융당국의 위기관리 능력에 대해 신뢰하게 될 것이다. 또한 금융당국이 정보보안 사고에 책임에 대해 회피하지 않고 최선을 다해 사고수습에 노력을 기울인다면 금융소비자의 신뢰가 회복 될 것이다. 이러한 여러 논의를 통해 다음과 같은 가설을 도출하였다.

가설 2: 금융당국의 정보보안 사고 위기대응 수준은 금융정보보안 신뢰에 긍정적인 영향을 미칠 것이다.

3.2.3 금융정보보안 컴플라이언스와 금융기관 위기대응과의 관계

위기관리 이론에 따르면 위기란 “어떤 임박하고도 갑작스러운 변화를 수반하는 불안정하고 위험한 정치・경제・사회적 상황, 또는 자연적 재난이나 사건”을 말한다(최진혁, 2010). 금융기관의 개인정보 유출 사고는 기업을 위기에 빠뜨리는 인위적 사건이나 재난이라고 할 수 있다. 따라서 기업은 위기상황을 잘 대처할 수 있는 방법을 찾거나 위기관리로 인한 영향이나 충격을 최소화해야 한다(Erickson, 1999). 기업의 위기에 대한 대응으로 공공 및 민간부문 파트너십이 중요한 요소로 언급되고 있다(Deloitte, 2009). 기업이 정부와 공조한다는 것은 정부가 제시한 각종 기준을 준수하는 것이다.

금융소비자는 기업이 개인정보보호를 위한 법・제도를 준수 할 때 기업의 위기대응 능력에 대해 신뢰할 것이다. 왜냐하면 정보보안을 위한 각종 컴플라이언스와 가이드라인을 준수한다는 것은 정보보안을 위한 첫걸음이기 때문이다. 기업은 이러한 컴플라이언스를 준수하고 있다는 것을 방송광고나 신문광고 또한 자사의 웹 사이트 등을 통한 다양한 수단으로 홍보할 수 있고 이는 기업의 위기관리에 대한 믿음으로 이어질 수 있다. 이러한 컴플라이언스나 각종 가이드라인 중에는 개인금융정보 보호기술에 대한 것도 있는데, 기술적인 컴플라이언스 준수는 금융기관의 정보시스템 관리에 대한 믿음으로 이어지게 될 것이다. 지속적이고 불확실한 보안 위협으로부터 컴플라이언스를 준수하는 것은 전자금융 소비자에게 긍정적인 영향을 미칠 것이다. 또한 이러한 긍정적인 인식은 보안사고 발생 후에 위기대응에도 보안 컴플라이언스 준수가 잘 이루어지는 기업이 위기대응도 잘할 것이라는 인식을 금융소비자에게 줄 수 있다. 이상의 논의를 통해 다음과 같은 가설을 도출하였다.

가설 3: 금융정보보안 컴플라이언스 수준은 금융기관 보안사고 위기대응에 긍정적인 영향을 미칠 것이다.

3.2.4 금융정보보안 컴플라이언스와 금융당국 위기대응과의 관계

정부의 위험관리에 대한 사례 중 하나인 고리원전 관리 실패에서 정부의 각종 컴플라이언스에 대한 관리・감독이 얼마나 중요한 것인지 알 수 있다. 고리원전은 1978년도에 처음 가동된 원전으로 국내에서 가장 오래된 원전이다. 하지만 애초의 계획대로라면 폐지되어야 했을 원전이 과학기술부 고시를 근거로 수명을 10년 더 연장하였는데 수명연장 후 매년 3~4회가 고장 및 사고가 발생하던 중 2012년 2월에는 차단기 손상이 원인이 된 오작동으로 12분 동안 정전이 발생하여 냉각수의 온도가 급상승 하는 사건이 발생하였다(최진식, 강영철, 2012, 한겨레, 2012; 국민일보, 2012). 이 과정에서 정부가 법률적 컴플라이언스 기준을 제시하였지만 한수원 측도 이를 지키지 않고 정부도 이에 대한 관리・감독을 소홀히 하였다.

이를 본 연구에 비추어 보면 금융당국이 마련해 놓은 전자금융 정보보안에 대한 컴플라이언스의 관리・감독을 철저히 하지 않는다면 이는 막대한 규모의 피해로 이어질 것이다. 실제 본 연구의 배경이 된 개인금융정보 유출사건에서도 그 피해와 규모면에서 단일사건으로는 최대 규모의 피해가 발생하였다. 금융당국이 자신들이 만든 컴플리이언스에 대한 관리・감독을 제대로 했다면 사건이 일어나지 않았거나 피해규모를 최소화 할 수 있었을 것이다. 따라서 개인금융정보 보호를 위한 첫 단추는 금융당국이 컴플라이언스에 대한 관리・감독을 철저히 하는 것이다. 이와 같은 사전대응으로서의 금융당국의 컴플라이언스에 대한 관리・감독은 관보나 뉴스 또는 금융당국의 웹 사이트 등을 통해 홍보할 수 있고 이는 금융소비자에게 금융당국이 위기대응에 대한 준비를 철저히 하고 인식을 주게 될 것이다. 따

라서 다음과 같은 가설을 도출하였다.

가설 4: 금융정보보안 컴플라이언스 수준은 금융당국 보안사고 위기대응에 긍정적인 영향을 미칠 것이다.

3.2.5 금융정보보안 신뢰와 금융정보 중요도와의 관계

개인이 금융 서비스를 이용하기 위해서 금융기관에 개인금융정보를 제공해야만 한다. 이러한 개인금융정보에 대해 인지하는 중요도는 개인금융정보 유출로 인해 빚어지는 피해의 정도에 대한 인식 차에 따라 그리고 그러한 개인금융정보 유출에 대한 개인의 처리능력이나 익숙함에 따라(Slovic, 1987) 사람마다 다를 수 있다.

가설 1에서는 금융기관의 개인금융정보 유출사고에 대한 위기대응 수준이 금융정보보안 신뢰에 영향을 미친다는 것을 살펴보았다. 여기서는 이러한 영향이 개인금융정보의 중요도에 따라 다르다는데 초점을 두고 있다. 즉, 개인금융정보 중요도 수준을 높게 인지하는 집단과 낮게 인지하는 집단에 따라 금융기관 위기대응이 금융정보보안 신뢰에 미치는 영향이 다르다는 점이다. 본 연구에서 중요도는 기존 마케팅 분야의 연구에서 관여도로서 연구되어 왔다. 관련 마케팅 문헌들을 살펴보면 다음과 같다.

서건수(2008)는 인터넷 쇼핑에서 관여도가 낮을수록 인터넷 쇼핑의 사용성이 고객충성도에 미치는 영향이 높다는 것을 보여주었다. Venkatesh *et al.*(2003)은 관여도가 낮을수록 웹 사이트를 피상적으로 평가하기 때문에 웹 사이트의 이용편리성이 사용의도에 미치는 영향이 높다는 것을 입증하였다. 이태민, 김동원(2011)은 모바일 상거래의 맞춤서비스 비경험자가 경험자보다 맞춤서비스가 만족도에 미치는 영향이 더 높은 것을 확인하였다.

이러한 선행연구에서는 공통적으로 경험이 적거나 관여도가 낮을수록 영향관계가 더 높게 나타났다. 이를 본 연구에 적용하면 개인금융정보의 중요도가 낮을수록 금융기관의 금융정보 위기대응 수준이 금융정보보안 신뢰에 미치는 영향이 높다고 가정할 수 있다. 1억 건이 넘는 초유의 개인정보 유출사건이라는 민감한 상황에서 개인금융정보를 매우 중요하게 생각하는 사람들은 금융기관의 위기대응 수준을 충분치 않게 생각하거나 불만을 가질 수 있어서 금융정보보안 신뢰가 높지 않을 수 있다. 이에 비해 개인금융정보를 덜 중요하게 생각하는 사람들은 상황을 상대적으로 냉정하게 판단하여 금융기관의 위기대응에 따라 높은 수준의 금융정보보안 신뢰수준을 갖게 될 것이다. 따라서 개인금융정보 고중요도 집단보다 저중요도 집단에서 금융기관 위기대응이 금융정보보안 신뢰에 미치는 영향의 조절효과가 더 크게 나타날 것이다. 이상의 논의를 본 연구에 적용하여 다음과 같은 가설을 도출하였다.

가설 5: 금융기관 위기대응이 금융정보보안 신뢰에 미치는 영향은 개인금융정보 중요도가 낮은 경우가 높은 경우보다 클 것이다.

3.2.6 금융정보보안 신뢰와 금융정보 유출수준과의 관계

개인금융정보 유출수준은 CVC번호, 금융거래내역이나 신용등급 같은 유출자체로 위험한 정보가 있는가하면 이름이나 전화번호같이 유출 자체로는 위험이 낮은 정보가 있다. 이와 같은 개인금융정보 유출수준은 사고 후에 금융소비자가 인식할 수 있는 문제인 동시에 금융당국의 정보보안사고 시 책임소재를 판단하거나 배상액을 결정하는데 중요하게 작용하게 된다. 따라서 금융소비자는 개인금융정보 유출수준에 따른 문제해결에 있어서 금융기관보다는 금융당국의 역할을 더 기대할 것이다.

가설 2에서 금융당국의 정보보안 사고 위기대응 수준이 금융정보보안 신뢰에 미치는 영향을

살펴보았다. 여기서는 이러한 영향이 개인금융정보 유출수준에 따라 다르다는 점에 초점을 맞추었다. 1억 건이 넘는 개인정보 유출사고 발생했다는 것이 2014년 1월에 공표되었고, 본 연구는 이러한 초유의 개인정보 유출사고에 대해 여론이 매우 뜨거웠던 2014년 2월에 설문조사 연구를 수행하였다. 이 시기에 특히 금융정보 유출수준이 높은 사람들은 금융당국의 역할에 거는 기대가 매우 높았을 것이다. 그러나 사실상 금융당국의 위기대응 수준이나 책임자 처벌 수위가 유출 피해자의 기대를 충족시키지 못하였다. 이러한 불만족은 금융보안 신뢰에 그대로 영향을 미쳤을 것이라 예상된다. 따라서 전술한 논의를 본 연구에 적용하여 조절효과로서 다음과 같은 가설을 도출하였다.

가설 6: 금융당국 위기대응이 금융정보보안 신뢰에 미치는 영향은 개인금융정보 유출수준이 낮은 경우가 높은 경우보다 클 것이다.

3.3 연구변수의 조작적 정의와 측정항목

본 연구에서는 선행연구를 토대로 하여 구성개념에 대한 조작적 정의와 구성개념의 측정항목을 도출하여 5점 리커트 척도로 측정하였고, 그 중 개인금융정보 유출수준은 상(5점)/중(3점)/하(1점)로 나누어 측정하였다. 그 내용은 <표 7>와 <표 8>에서 확인할 수 있다.

Ⅳ. 연구방법

4.1 자료수집 및 표본의 특성

본 연구의 설문배포 및 수집은 2014년 1월 8일에 대량의 개인금융정보 유출 사고를 금융당국이 공표한 1개월 이후인 2014년 2월 23~24일에 수행하였다. 이때 국민적 관심과 여론이 개인금융정보 사고수습에 초점이 맞춰져 있었다. 조사대상은 연구 설문의 특성상 인터넷 뱅킹을 이용하는 사람들 중 개인정보가 유출된 사람만을 대상으로 하였다. 설문지의 구성은 매우 그렇다(5점), 그렇다(4점), 보통이다(3점), 그렇지 않다(2점), 전혀 그렇지 않다(1점)인 5점 리커트 척도로 구성하였다. 그 중 불성실하게 작성된 설문지를 제외하고 103부(회수율: 89.5%)의 설문지를 분석에 이용하였다.

응답자의 인구 통계학적 특성을 살펴보면 남성이 62%, 여성이 38%인 것으로 나타났다. 나이는 20대가 41%, 30대가 40%, 40대가 11%, 50대 이상이 9%인 것으로 나타났다. 직업에 대한 분포는 대학생 및 대학원생 31%, 사무직 25%, 전문직 18%, 공무원 14%, 자영업 12%로 나타났다. 인터넷 뱅킹 사용기간은 5년 이상이 55%로 가장

〈표 7〉 조작적 정의

구 분	내용
금융정보보안 컴플라이언스	◦ 전자금융 소비자가 인지한 금융기관이 금융당국에서 정하고 있는 정보보안의 기술적·관리적 법률과 제도를 준수하고 있다고 전자금융 소비자가 인지하는 수준
금융기관 위기대응	◦ 전자금융 소비자가 인지한 금융사고에 대한 금융기관의 적절한 대응수준
금융당국 위기대응	◦ 전자금융 소비자가 인지한 금융사고에 대한 금융당국의 적절한 대응 수준
금융정보 보안신뢰	◦ 전자금융 소비자가 인지한 금융기관과 금융당국의 금융정보보안 위기대응에 대한 평가 수준
금융정보 중요도	◦ 전자금융 소비자가 인지한 금융기관에 제공하는 개인금융정보의 중요도 수준
금융정보 유출수준	◦ 전자금융 소비자가 인지한 금융당국이 보호해야할 개인금융정보의 유출수준

〈표 8〉 요인별 측정항목 및 참고문헌

구성개념	설문문항	출처
금융정보보안 컴플라이언스	개인정보보호를 위한 법·제도의 준수	박준호(2011), 조창훈, 이정진(2013)
	개인정보보호를 위한 기술·관리적 준수	
	개인정보가 안전하게 지켜짐	
금융기관위기대응	기대했던 서비스를 받음	White and Eiser(2006) Goodwin and loss(1992)
	새롭게 안전장치를 마련	
	불만처리가 신속	
금융당국 위기대응	사후대책이 마음에 듦	White and Eiser(2006) 최진식, 강영철(2013)
	사후대책이 시기적절	
	각 정부부처 별 사후대책에 대해 만족	
	관련자 처벌 조치에 만족	
	관련자를 처벌하기 위한 법·제도적 근거에 만족	
금융정보보안신뢰	돌발 상황 발생 시 대처능력을 가짐	Jarvenpaa and Todd(1996) 최진식, 강영철(2013)
	거래정보 유출방지를 위해 최선을 다 함	
	고객의 개인정보를 은행이 임의로 활용하지 않음	
	관련법에 명시된 기간을 준수하여 개인정보를 파기	
금융정보중요도	은행에 제공하는 개인정보의 중요도	Boehmer(2009), 김종기, 이동호(2005)
	개인정보가 의미가 있다고 생각하는 정도	
	개인정보 활용에 대한 불안감	
	개인정보보호 기술 활용정도	

많았으며 1년 미만은 1%로 가장 적었다. 수입 또는 용돈은 100만 원에서 200만 원 사이가 35%로 가장 많았고 400만 원 이상이 5%로 가장 적게 나타났다. 월평균 인터넷 뱅킹 사용금액은 30만 원 이하가 31%로 가장 많았으며 60만 원에서 120만 원 사이도 23%로 높게 나타났다 150만 원 이상도 18%나 되었다.

또한 개인정보 유출 수준에 대한 응답 결과를 살펴보면 고급정보(카드 CVC번호, 신용등급)가 16%, 중급정보(주민등록번호, 직장전화번호)가 57%, 하급정보(이름, 집 전화번호)가 27% 유출되어 중급정보가 유출됐다고 응답한 사람이 가장 많은 것으로 나타났다. 개인정보가 유출된 은행이나 카드사의 숫자를 살펴보면 1곳이라는 응답이 48%, 2곳이라는 응답이 37%, 3곳이라는 응답이 14%로 2곳 이상의 은행이나 카드사에서 정보가 유출된 사람의 비율이 과반 수 이상인 것으로 나타났다. 이와 같은 결과에서 개인을 식별할 수 있는 수준의 정보가 유출되어 이로 인한 2차 피해가 일어날 가능성이 높다는 것을 알 수 있었다.

4.2 분석방법

본 연구에서는 SmartPLS 2.0 패키지의 PLS algorithm과 PLS bootstrapping을 이용하여 측정모형과 구조모형을 분석하였다. 측정모형 분석에서는 신뢰성 및 타당성을 검증하기 위해 내적일관성, 집중타당성, 판별타당성 등을 분석하였다. PLS 분석은 엄격한 이론적 기반을 요구하는 AMOS나 LISREL과 달리 탐색적 연구를 지원한다(고미현, 권순동, 2008; Gefen *et al*., 2000). PLS 분석

〈표 9〉 응답자의 인구통계학적 특징

변수	구분	응답자 수	퍼센트
성별	남자	64	62%
	여자	39	38%
학력	20대	42	41%
	30대	41	40%
	40대	11	11%
	50대 이상	9	9%
직업	공무원	14	14%
	사무직	26	25%
	자영업	12	12%
	전문직	19	18%
	대학생 및 대학원생	32	31%
인터넷 뱅킹 사용 기간	1년 미만	1	1%
	2년 미만	12	12%
	3년 미만	12	12%
	4년 미만	14	14%
	5년 미만	7	7%
	5년 이상	57	55%
합계		103	100%

에서도 기존의 선행연구에 따라서 측정항목을 개발할 경우 탐색적 요인분석보다 확인적 요인분석을 요구한다(고미현, 권순동, 2008; Gefen and Straub, 2005).

구조모형 분석에서는 경로분석을 통해서 구조모형의 적합도와 설명력, 경로계수 및 가설의 유의성을 분석하였다.

Ⅴ. 실증분석

5.1 측정모형의 신뢰성 및 타당성

5.1.1 내적일관성(Internal Consistency) 분석

본 연구에서는 리커트 척도로 구성된 표준화된 척도에 사용하는 내적 일관성을 통해 신뢰도를 검증하였다. <표 10>와 같이 각 잠재변수의 복합신뢰도(composite reliability)와 Cronbach α가 모두 0.7 이상이고, 각 잠재변수의 평균 분산추출(AVE: averaged variance extracted)이 Fornell and Larcker (1981), Chin(1998) 등이 주장하는 기준치인 0.5 이상으로 나타났다. 따라서 본 모델은 높은 수준의 내적일관성을 보여주었다.

〈표 10〉 내적일관성 검증

구성 개념	복합신뢰도	AVE	Cronbachs Alpha
금융정보보안 컴플라이언스	0.935	0.828	0.896
금융기관 위기대응	0.864	0.864	0.765
금융당국 위기대응	0.942	0.764	0.923
금융정보보안 신뢰	0.866	0.617	0.797
개인금융정보 중요도	0.925	0.805	0.879

5.1.2 집중타당성(Convergent Validity) 분석

<표 11>와 같이 측정모형에서 각 차원의 AVE가 0.5 이상이고, 표준화된 요인적재량이 0.73~0.95 사이의 값이며(0.7 이상을 권장), 요인적재량의 t-값들이 1.965 이상으로 유의하기 때문에(유의수준 0.05, t값 > 1.965, p < 0.05) 집중타당성이 있는 것으로 나타났다(우종필, 2012; Gefen and Straub, 2005; Srite and Karahanna, 2006; Bhattacherjee and Sanford, 2006). 표에서 t-값은 bootstrapping을 수행하여 나온 결과이다.

5.1.3 판별타당성(Discriminant Validity) 분석

본 연구에서는 <표 12>의 대각선 축에 표시되는 AVE의 제곱근 값이 다른 구성개념 간의 상관계수 값보다 큰가의 여부로 판별타당성을 검증하였다(우종필, 2012; Fornell and Lacker, 1981). 검증

〈표 11〉 집중타당성 검증

구성개념	측정문항	개념평균	표준편차	항목 평균	요인 적재값	표준 오차	T-값
금융정보 보안 컴플라이언스	compliance1	2.117	0.990	2.223	0.854	0.022	19.211
	compliance2			2.039	0.924	0.011	30.806
	compliance3			2.087	0.949	0.010	35.351
금융기관 위기대응	institution1	2.078	0.927	1.903	0.784	0.032	11.101
	institution2			2.184	0.871	0.020	20.633
	institution3			2.146	0.816	0.030	14.566
금융당국 위기대응	authority1	1.788	0.847	1.816	0.900	0.011	23.185
	authority2			1.816	0.871	0.009	25.588
	authority3			1.680	0.822	0.011	19.344
	authority4			1.845	0.846	0.013	19.218
	authority5			1.786	0.870	0.013	17.641
금융 정보보안 신뢰	trust1	2.248	1.077	2.252	0.836	0.025	15.496
	trust2			2.146	0.812	0.021	16.157
	trust3			2.262	0.760	0.021	12.481
	trust4			2.330	0.731	0.020	14.083
개인 금융정보 중요도	personal1	4.505	0.879	4.524	0.906	0.077	4.254
	personal2			4.544	0.923	0.055	6.567
	personal3			4.447	0.861	0.104	4.083

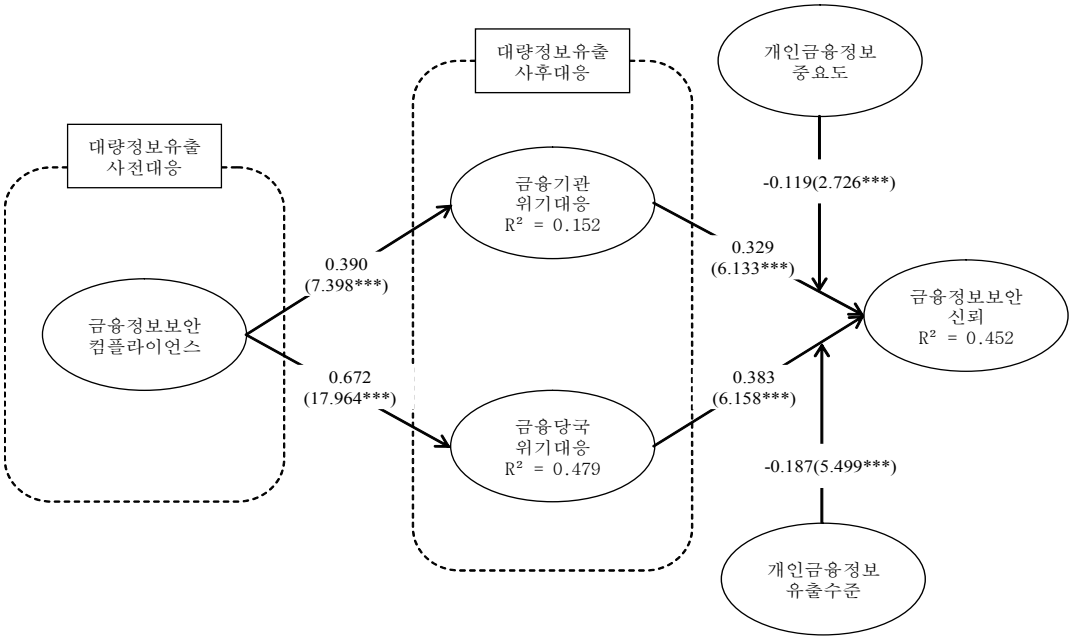
〈표 12〉 판별타당성 검증

	개인금융정보 중요도	금융기관대응	금융당국대응	금융정보보안 신뢰	금융정보보안 컴플라이언스
개인금융정보 중요도	**0.897**				
금융기관대응	-0.150	**0.825**			
금융당국대응	-0.318	0.495	**0.874**		
금융정보보안 신뢰	-0.231	0.546	0.594	**0.785**	
금융정보보안 컴플라이언스	-0.311	0.390	0.672	0.632	**0.910**

주) 상관관계 표에서 대각선 요소는 AVE의 제곱근을 나타낸 것이며, 대각선 외 요소는 개념 간 상관관계이다.

결과 AVE의 제곱근 값 중 가장 작은 값(0.785)이 가장 큰 상관계수 값(0.672)보다 상회하여 본 연구모델의 구성개념은 판별타당성이 있음이 검증되었다. 또한 측정모형에서 외생변수인 구성개념간의 상관계수가 모두 0.9 이하이기 때문에 차원들 간의 다중공선성은 없는 것으로 나타났다(김중인, 2012; Kutner *et al.*, 2004).

본 연구의 측정모형에서 신뢰성, 집중타당성 및 판별타당성이 있는 것으로 나타났기 때문에 단일차원성이 검증되었다(김대업, 2009; Fornell and



주) $^{**}P < 0.05$, $^{***}P < 0.01$.

〈그림 2〉 경로분석 결과

Larker, 1981).

5.2 구조모형의 경로분석

5.2.1 구조모형의 적합도 및 설명력 분석

PLS 분석에서 전체 데이터의 경로모델의 설명력은 내생변수의 설명력을 나타내는 결정계수(explained variance) R^2값을 예측적합도 지수로 사용하며, 상(0.26 이상), 중(0.13～0.26), 하(0.02～0.13)로 구분하여 판단한다(Barclay *et al*., 1995; Chin and Gopal, 1995). <표 13>에서 보는 것처럼 금융정보보안 컴플라이언스의 금융기관 위기대응과 금융당국 위기대응의 설명력인 R^2값은 각 0.152, 0.479로 나타났고, 앞의 두 매개변수의 금융정보보안 신뢰의 설명력 R^2값은 0.465로 나타났다.

〈표 13〉 구조모형의 적합도

구성개념	R^2	중복성	공통성
금융정보보안 컴플라이언스			0.828
금융기관 위기대응	0.152	0.101	0.680
금융당국 위기대응	0.479	0.342	0.764
금융정보보안 신뢰	0.452	0.017	0.617
평균	0.352	0.153	0.616
전반적 적합도	0.465		

PLS 분석은 내생변수의 중복성(redundancy)값을 예측적합도 지수로 사용하며, 이 값이 0보다 크면 예측적합도가 있는 것으로 판단한다(Wixom and Watson, 2001). 연구모형의 평균 중복성은 0.153으로 예측적합도가 있는 것으로 나타났다.

구조모형의 전반적 적합도(goodnees-of-fit, GoF)는 모든 내생변수의 R^2의 평균과 각 차원들의 공통성(communality)평균을 곱한 값의 제곱근으로 산출하며, 상(0.36 이상), 중(0.25～0.36), 하(0.10～0.25)로 구분하여 판단한다(Tenenhaus *et al*., 2005; Wetzels *et al*., 2009). 분석결과 GoF의 영향도는 0.465로서 Wetzels(2009) 등이 제시한 0.36(상)보다

커서 모형의 적합도가 매우 높은 것으로 나타났다.

5.2.2 구조모형의 경로계수 유의성 검증

경로계수는 두 변수간의 인과관계에 대한 정보를 제공한다(Wixom and Watson, 2001). PLS algorithm을 통해 나온 표준화된 경로계수들과 PLS bootstrapping을 통해 나온 경로계수의 t-값들과 유의성 검증 결과는 <표 14>와 같다. 본 연구의 모형에서 가장 작은 t-값은 6.133(금융기관 위기대응 → 금융정보보안 신뢰) 가장 큰 t-값은 17.964(금융정보보안 컴플라이언스 → 금융당국 위기대응)으로 나타나 H1～H4의 가설은 유의수준 0.01에서 채택되었다.

본 연구에서는 금융기관의 위기대응과 개인금융정보 중요도의 상호작용 효과가 금융정보보안 신뢰에 영향을 미칠 것이라는 조절효과(H5)를 설정하였고 또한 금융당국의 위기대응과 개인금융정보 유출수준의 상호작용 효과가 금융정보보안 신뢰에 영향을 미칠 것이라고 조절효과(H6)를 설정하였다. 이를 분석하기 위해 PLS에서 Chin *et al.*(2003)이 제시한 조절변수의 상호작용효과 분석절차에 따라 표준점수화방법(standardize indicator values before multiplication)을 이용하여 분석하였다. PLS bootstrapping을 이용하여 t-값을 계산하였다. 조절효과의 가설 검증 결과 가설 5와 가설 6 모두 유의한 것으로 나타났다.

5.2.4 연구결과 논의

본 연구에서는 대량의 개인정보 유출이라는 정보보안 사고에 대해 영향을 미치는 요인을 사전대응과 사후대응 관점으로 나누고 금융정보보안 컴플라이언스, 금융기관 정보보안 위기대응, 금융당국 정보보안 위기대응, 금융정보보안 신뢰의 요인을 도출하여 관계를 규명하였다.

연구모형을 인터넷 뱅킹 이용자를 대상으로 실증분석 한 결과, 각각의 요인이 전자금융 정보보안 신뢰에 유의미한 영향을 미치는 것으로 나타났다. 한편 본 연구의 중심인 조절요인인 개인금융정보 중요도는 금융기관 위기대응이 금융정보보안 신뢰사이에 미치는 영향을 조절하는 것으로 나타났다. 또한 개인금융정보 유출수준은 금융당국 위기대응이 금융정보보안 신뢰에 미치는 영향을 조절하는 것으로 나타났다. 연구결과의 의미를 사전대응 관점·사후대응 관점·개인정보 유출자 관점으로 나누어 살펴보면 다음과 같다.

(1) 대량 정보 유출 사전대응 관점(**금융정보보안 컴플라이언스**)

금융정보보안 컴플라이언스는 금융기관 위기대응(β = 0.390)보다 금융당국 위기대응(β = 0.672)

〈표 14〉 경로계수의 유의성 검증

가설	경로	경로계수(β값)	T-값	결과
H1	금융기관 위기대응 → 금융정보보안 신뢰	0.329	6.133***	채택
H2	금융당국 위기대응 → 금융정보보안 신뢰	0.383	6.158***	채택
H3	금융정보보안 컴플라이언스 → 금융기관 위기대응	0.390	7.398***	채택
H4	금융정보보안 컴플라이언스 → 금융당국 위기대응	0.672	17.964***	채택
H5	금융기관 위기대응 → 금융정보보안 신뢰 ↑ 개인금융정보 중요도	-0.119	2.726***	채택
H6	금융당국 위기대응 → 금융정보보안 신뢰 ↑ 개인금융정보 유출수준	-0.187	5.499***	채택

주) $^{**}P < 0.05$, $^{***}P < 0.01$.

에 더 큰 영향을 미치는 것으로 나타났다.

첫째, 이와 같은 결과는 대량정보가 유출된 당시 상황에 기인한 것이라고 볼 수 있다. 1억 건이 넘는 사상 초유의 개인정보 유출은 지금까지의 보안사고와 비교하여 가장 많은 개인정보가 유출된 사건이고 이러한 금융정보는 2차 피해와 직결될 수 있는 중요한 사건이었다. 따라서 금융소비자들은 금융기관의 역할보다 금융당국의 역할에 더 큰 기대를 하였고 이러한 기대가 본 연구결과에 그대로 반영되어 나타난 것이라 할 수 있다.

둘째, 금융당국은 금융정보보안 컴플라이언스에 대한 법률・제도적인 가이드라인을 만들고 이러한 금융정보보안 컴플라이언스가 제대로 적용되고 있는지를 관리・감독한다. 또한 개인정보 유출로 인한 손해배상에 대한 판단도 하게 된다. 금융소비자들은 이와 같은 금융당국의 역할에 기대를 거는 것이다. 지금까지 개인정보 유출사고에서 기업들은 책임을 회피하려는 모습을 보여왔다. 이러한 성향이 연구결과에 반영되어 금융기관으로 이어지는 경로계수가 금융당국으로 이어지는 경로계수보다 작게 나타난 것이라 해석된다.

(2) 대량 정보 유출 사후대응 관점(**금융기관/당국 위기대응**)

위기대응이 금융정보보안 신뢰로 이어지는 경로계수는 금융기관(β = 0.329)보다 금융당국(β = 0.383)이 약간 높게 나타났다. 이 역시 금융소비자가 대량의 개인정보 유출사고에 있어서 정부역할을 기대하고 있다는 것을 반영하는 것이라 볼 수 있다.

첫째, 사후대응에 있어서 금융기관의 역할은 얼마나 신속하게 서비스를 정상화 하느냐 이다. 보안사고에 있어서 서비스를 정상화 한다는 것은 피해자에 대한 구제를 확실히 하는 것이다. 먼저 최대한 빠르게 피해자에게 사고 소식을 알리고, 구제절차에 대한 가이드라인을 제시하여야 한다. 또한 실제적인 피해보상을 해야 하고 사고가 일어난 시스템에 대해 금융정보보안 컴플라이언스 기준을 준수하여 안전장치를 점검하고 대책을 마련해야 한다. 또 다른 중요사항은 구제 절차과정에서 금융소비자에게 기업이 피해구제에 최선을 다하고 있다는 인식을 주어야 한다는 점이다. 전자금융 정보보안 신뢰를 위해서 금융기관은 돌발적인 보안사고에 대처할 수 있는 능력을 갖추어야 하며, 거래정보 유출방지를 위해 최선을 다해야 한다. 또한 금융기관은 고객정보 관리에 대한 컨트롤타워를 마련하여 계열사에게 무분별하게 공유되는 정보를 관리하여야 한다.

둘째, 금융당국은 금융기관이 금융정보보안 컴플라이언스를 준수하고 있는 지에 대한 관리 감독을 철저히 해야 하며, 정부부처 별로 흩어져있는 대응체계를 효과적으로 컨트롤할 수 있어야 한다. 또한 금융소비자가 보안 사고 처리에서 불만족하는 부분이 없도록 정보보안사고 관련자에 대해 적절한 조치를 취해야 한다.

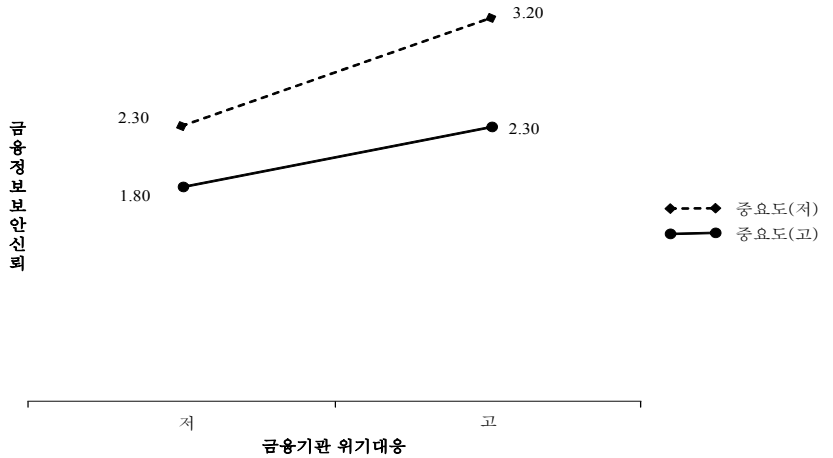
(3) 개인정보 유출자 관점(**중요도와 유출수준**)

개인금융정보 중요도와 유출수준의 조절효과는 유의한 것으로 나타났다. 특히 본 연구의 배경이 된 사상초유의 개인정보 유출사건은 정보유출이 없거나 상대적으로 적은 상황과는 다른 배경을 가지고 있다. 따라서 일반적인 상황에서의 조절효과와는 반대방향의 조절효과가 나타났다. 조절효과를 보다 분명하게 파악하기 위해 이를 도식화 하였다.

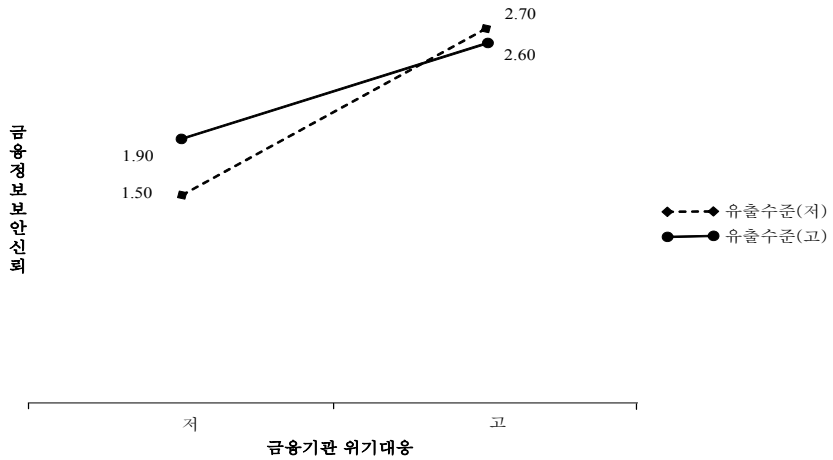
첫째, <그림 3>은 ***개인금융정보 중요도***가 낮은 집단에서 금융기관 위기대응이 금융정보보안 신뢰에 미치는 효과가 더 크게 나타나고 있음을 보여주고 있다. 이는 선행연구와 연구가설에서도 밝혔듯이 개인금융정보 고중요도 집단은 1억 건이 넘는 개인정보 유출이라는 초유의 사태 시에는 고중요도 금융소비자가 민감하게 반응하여 금융기관의 위기대응에 관해 불만족하는 성향을 가진 집단이라고 가정한 특성이 실증분석 결과

에서도 드러난 것이다. 따라서 대량의 정보 유출이라는 초유의 위기상황 시에 금융기관이 금융정보보안 신뢰 회복을 위해서 개인금융정보가 중요도가 높은 집단을 위한 서비스 전략을 개발하는 것이 필요하다. 즉, 금융기관의 정보보안 능력에 대한 신뢰가 높아지도록 정보보안 컴플라이언스를 철저히 준수하고 각종 정보보안 인증을 받아 홍보하는 노력이 필요하고, 정보보안에 대한 확신을 줄 수 있는 기술과 인력도입이 필요하다. 이를 위해서 정보보안 전담 부서를 설치하고 장식용 부서가 아닌 기업 내에서 중요한 위치를 가질 수 있도록 최고경영자와 이사회의 관심이 있어야 할 것이다.

둘째, <그림 4>는 ***개인금융정보 유출수준***이 낮은 집단에서 금융당국 위기대응이 금융정보보안 신뢰에 미치는 효과가 더 크게 나타나고 있음을 보여주고 있다. 이 역시 선행연구의 논의와 일치하는 것으로 개인금융정보 고유출수준 집단은 금융당국의 위기대응 처리과정에서 개인정보 유출자의 처벌수위에 불만족하는 성향의 집단이



〈그림 3〉 개인금융정보 중요도에 따른 금융기관 위기대응과 금융정보보안 신뢰와의 관계



〈그림 4〉 개인금융정보 유출수준에 따른 금융당국 위기대응과 금융정보보안 신뢰와의 관계

라고 할 수 있다. 이와 같은 결과는 금융당국에게 다음과 같은 시사점을 줄 수 있다. 금융당국이 고유출 수준 집단에게 금융정보보안 신뢰를 회복하기 위해서는 지금까지의 정보보안 사고에서 보여 주었던 사고 대처방식이 아닌 진정성을 가지고 사고에 대한 철저한 진상규명을 위해 노력하는 모습을 보여 주어야 할 것이다. 또한 여기저기 산재해 있는 금융정보보안에 관한 법률을 통합하고 금융정보보안에 대한 전담부처를 지정하여 전문성과 책임성을 가지고 보안사고에 임해야 할 것이다.

Ⅵ. 결 론

6.1 연구결과의 요약

전자금융 관련 사고가 끊임없이 일어나고 있으며, 이러한 사고는 기술적 원인, 인적 원인 구조적 원인 등 여러 가지 원인이 복합적으로 작용하여 일어나고 있다. 전자금융 관련 사고는 개인정보 유출이 가장 많고 개인정보 유출로 인한 보이스피싱 등의 2차 피해가 일어나 사회적으로 심각한 손실을 가져와 문제가 되고 있다.

기존의 전자금융 정보보안 대책은 기술적인 면이 강조되었다. 하지만 새로운 해킹 방지기술을 만든다고 해도 더 최신의 해킹기술이 등장한다면 기술적인 방지대책으로는 전자금융 정보보안 사고를 막는데 한계가 있다고 할 수 있다. 또한 정보시스템의 취약점을 전혀 존재하지 않게 만든다는 것은 불가능 하다. 따라서 본 연구에서는 전자금융 정보보안 위험을 최소화하는데 초점을 맞추어 사전대응과 사후대응의 관점으로 나누어 각 관련 주체가 어떻게 행동해야 금융신뢰가 회복될 수 있는지에 관해 연구하였다. 연구모형은 금융정보보안 컴플라이언스가 금융기관 및 금융당국의 위기대응에 영향을 미치고 이러한 위기대응 활동은 금융정보보안 신뢰에 영향을 미친다는 것이다. 총 103부의 설문지를 실증연구를 위해 구조방정식 모형으로 분석하였다.

실증분석 결과, 사전대응 관점에서는 금융정보보안 컴플라이언스는 금융당국에 더 큰 영향을 미치고, 금융기관 위기대응과 금융당국 위기대응이 금융정보보안 신뢰에 영향을 미치는 것으로 나타났다. 다음으로 조절효과 분석에서 개인금융정보 중요도는 금융기관 위기대응이 금융정보보안 신뢰사이에 미치는 영향을 조절하는 것으로 나타났으며, 개인금융정보 유출수준은 금융당국 위기대응이 금융정보보안 신뢰에 미치는 영향을 조절하는 것으로 나타났다.

6.2 연구결과의 시사점

본 연구결과가 기존의 연구와 **차별되는 점**은 다음과 같다. ***첫째***, 대량정보 유출 시 전자금융 정보보안에 대한 사전대응과 사후대응을 금융소비자의 입장에서 실증함으로써 전자금융 사고가 일어났을 때 정부와 기업이 어떻게 대응을 해야 금융소비자가 신뢰할 수 있는지를 밝혔다는 점이다. ***둘째***, 금융정보보안에 대한 신뢰가 금융권의 위기관리 역할이나 역량에 기초한 신뢰라는 점을 연구를 통해 규명했다는 점이다. ***셋째***, 본 논문은 일반적인 상황과는 다른 사상초유의 개인정보 유출사태를 배경으로 하여 전자금융사고 대응의 전체적인 시스템을 제시해서 이와 같은 위기상황 시에 금융권 정보보안 대응 틀로 유용하게 사용될 수 있을 것이다.

본 연구는 위기의 순간에 평상시와 같은 대응으로는 금융소비자에게 만족을 줄 수 없다는 것을 반영하여 중대한 전자금융 정보보안 사고 발생 시 금융권의 대응방안을 법률・조직・정책의 3가지 관점에 살펴보면 다음과 같다.

첫째, ***법률적 관점***에서 우리나라의 정보보안 관련 법률들은 상호간 불균형, 중복, 공백 등의 문제를 가지고 있어 IT 컴플라이언스 준수기준을 제대로 제시하고 있지 못하다. 또한 전자금융 정보보안뿐만 아니라 정보보안 관련 법률의 분

산으로 국가적 보안사고 발생 시 체계적 대응, 책임소재, 부처 간 정보의 공유 등에 있어서 문제를 안고 있다(윤광석, 2013). 2014년 7월 11일에 열린 “개인정보보호 통합법 제정을 위한 공청회”에서 지적된 개인정보보호 관련법의 문제로 그동안 금융권, 이동통신사업자, 병의원, 교육기관 등 각 기관 마다 흩어진 법률로 인하여 중복된 규제를 받고 있어서 막대한 규제비용이 든다는 점과 개인정보 유출자의 입장에도 개인정보 유출 사고 시 흩어진 법률로 인하여 권리를 보장받기 쉽지 않았다는 점 등이 지적됐다. 또한 그동안 낮은 수위의 처벌로 논란이 되었던 개인정보 유출사고에 대해 통합법 제71조 제1항에 따르면 개인정보를 취급하는 사업자가 전체 보유하고 있는 개인정보 중 4분의 3 이상을 유출시켰을 경우 이에 따르는 손해액을 3배 배상 청구할 수 있도록 하였다(지디넷코리아, 2014). 따라서 통합된 법률의 제정, 기본법의 제정에 대한 발의 안을 통과시켜 그동안 혼란을 빚었던 법률체계를 개선하고 개인정보 유출자의 권리 보장 강화를 위해 정보보안에 대한 일반법을 제정해야 한다.

둘째, ***조직적 관점***에서 우리나라의 경우 정보보안 업무를 공공기관은 정보통신기반보호위원회가 담당하고 민간부문은 방송통신위원회가 맡고 있다. 정보보안 총괄기구인 국가사이버전략회의(국가사이버안전관리 규정 제6조)와 국가사이버안전대책회의(위 법 제7조)를 두고 있기는 하지만 상위법인 정보통신기반 보호법과의 법정합성 차원에서 어긋나기 때문에 사실상 관할할 수 있는 업무가 거의 없다(한국인터넷진흥원, 2010a). 전자금융 정보보안도 행정자치부, 개인정보보호위원회, 금융위원회, 공정거래위원회, 방송통신위원회, 미래창조과학부 등으로 소관부처가 다양하고 각 부처별 소관법률도 법정합성차원에서 문제가 되고 있다. 나아가 정보통신망과 정보보안은 공공부문과 민간부문을 서로 분리할 수 없고 중대한 정보보안 사고 발생 시에는 통합 컨트롤타워가 필요한데 현재 우리나라의 법제는 이에 대한 관련 법률이 마련되어 있지 못하다. 또한 금융회사도 각 계열사의 개인정보를 통제할 수 있는 시스템을 갖추지 못하고 있어 내부 개인정보 흐름을 통제 할 수 있는 컨트롤타워가 마련되어야 한다.

셋째, ***정책적 관점***에서 우리나라의 전반적인 정보보안기술은 침해기술에 대응할 수 없을 정도로 매우 낙후되어 있다. 최근 한수원에서 원전 설계도와 같은 중요한 문건 유출이 일어났는데도 정부는 뒤늦게 원인 파악에 나서고 있으며 아직까지도 정확한 원인을 찾지 못하고 있다(한겨레, 2015). 원전은 정부가 관리하는 위험시설 중 최상위의 시설인데도 불구하고 침해기술을 대응기술이 따라가지 못하고 있는 것이다. 그 원인은 영세한 보안산업 규모, 정부의 R&D 투자 미흡, 정부 및 기업의 보안의식 미흡, 외국 보안기술 의존, 정부 간 협력 미흡, 민관협력 미흡 등의 문제가 지적되고 있다. 따라서 전자금융 정보시스템 보안사고에 대비하기 위하여 정부차원에서 보안산업을 육성하여 기술개발과 보안인력 육성을 강화하고, 보안사고에 적절히 대응할 수 있도록 보안 예산 정책을 강화하는 것이 필요하다(윤광석, 2013).

결론적으로, 전자금융 정보보안은 최신의 해킹 방어 기술만 도입한다고 해서 전자금융 정보보안 신뢰가 회복되는 것이 아니라, 정보보안에 대한 사전대응과 사후대응 시스템이 조화를 이룰 수 있게 각종 법률과 제도의 정비가 필요하고 위기의 정도에 따른 적절한 대응이 필요한 것이다.

6.3 연구결과의 한계 및 향후 연구방향

본 연구는 표본 상의 한계를 지닌다. 첫째, 표본에 있어서 대학생이나 대학원생과 20대와 30대가 가장 많기 때문에 표본의 대표성에 대한 문제가 있을 수 있다. 따라서 향후연구에서는 연구의 표본이 대표성을 가질 수 있게 다양한 계층과 연령대를 대상으로 하여 설문조사가 이루어져야 할 것이다.

둘째, 본 연구는 사상초유의 개인정보 유출사건을 배경으로 하고 있다. 따라서 본 연구의 조절효과인 개인금융정보 중요도와 유출수준이 일반적인 상황에서는 기존의 선행연구에서처럼 나타날 것인지에 대한 비교연구가 필요하다. 이와 같은 점을 보완하여 향후 연구에서는 전자금융 정보보안에 대한 보다 일반화된 연구결과가 도출될 수 있기를 기대해 본다.

참 고 문 헌

고미현, 권순동, “인터넷 커뮤니티에서 사용자 참여가 밀착도와 지속적 이용의도에 미치는 영향”, Asia Pacific Journal of Information Systems, 제18권, 제2호, 2008, pp. 41-72.

금융정보화추진분과위원회 사무국 한국은행 금융결제국, “전자금융총람”, 2009, http://dl.bok.or.kr/search/DetailView.ax?cid=176116.

기소진, 이수영, “프라이버시 염려와 자기효능감에 따른 SNS 이용자 유형에 관한 탐색적 연구”, 한국언론학보, 제57권, 제1호, 2013, pp. 81-110.

김근아, 김상현, 박근재, “금융기업의 보안대책이 금융 IT 보안책임과 위험감소 그리고 기업성과에 미치는 영향”, 한국경영과학회지, 제38권, 제4호, 2013, pp. 95-112.

김대업, “Amos A to Z: 논문작성절차에 따른 구조방정식 모형분석”, 서울: 학현사, 2008.

김소이, “전자금융사고 발생유형 및 대응현황”, 금융결제원, 지급결제와 정보기술, 2009, pp. 34-62.

김영태, “전자금융 정책 및 감독 선진화를 위한 주요국 사례분석”, 금융보안연구원, 2012.

김왕식, “정부신뢰에 미치는 영향요인에 관한 연구”, 사회과학연구, 제27권, 제2호, 2011, pp. 141-161.

김정덕, “개인정보보호를 위한 관리체계와 거버넌스”, 정보보호학회지, 제18권, 제6호, 2008, pp. 1-5.

김종기, 이동호, “전자상거래 사용자의 신뢰에 영향을 미치는 정보보안 위험 기반의 선행요인 연구”, Asia Pacific Journal of Information Systems, 제15권, 제2호, 2005, pp. 65-96.

김중인, “반영지표 vs. 조형지표: 이론적 논의, 실증적 비교, 그리고 실무적 유용성”, 마케팅연구, 제27권, 제4호, 2012, pp. 199-226.

김태호, 박태형, 임종인, “국내 인터넷전문은행 설립시 예상되는 전자금융 리스크에 대한 대응방안 연구”, 정보보호학회지, 제18권, 제5호, 2008, pp. 33-48.

김현욱, 박창균, “인터넷 뱅킹의 확산에 따른 금융산업 구조변화에 관한 연구: 은행산업의 수익, 경쟁구조변화를중심으로”, 한국개발연구원, 2002.

막스 베버(박성환 역), “경제와 사회 I”, 문학과지성사, 1997.

박정훈, 이숙현, “정보 프라이버시와 관련한 개인의 태도 및 행동 경로분석”, 행정논총, 제45권, 제1호, 2007, pp. 281-307.

박종민, 배정현, “연구논문: 정부신뢰의 원인: 정책결과, 과정 및 산출”, 정부학연구, 제17권, 제2호, 2011, pp. 117-143.

박준호, “국방부 정보보호 관리체계 구축안”, 사이버테러정보전 컨퍼런스 및 학술대회, 제12권, 2011, pp. 30-47.

서건수, “인터넷 쇼핑 사이트의 사용성 및 신뢰성과 고객 충성도간의 관계에서 인터넷 쇼핑 관여도의 조절효과”, 한국IT서비스학회지, 제7권, 제3호, 2008, pp. 1-29.

신용녀, 김영진, 전명근, “바이오 보안 토큰과 PKI 연계방안”, 한국정보기술학회논문지, 제9권, 제5호, 2011, pp. 207-216.

우종필, “구조방정식 모델 개념과 이해”, 서울: 한나래출판사, 2012.

육태우, “미국에서의 기업 컴플라이언스의 발전”, 강원법학, 제39권, 2013, pp. 133-173.

윤광석, “공공부문 정보보안 정책 실태분석 및 개선방안 연구”, 한국행정연구원 연구보고서, 2013.

윤상오, “전자정부 구현을 위한개인 정보보호 정책에 관한 연구: 정부신뢰 구축의 관점에서”, 한국지역정보화학회지, 제12권, 제2호, 2009, pp. 1-29.

이미나, 심재웅, “성별에 따른 온라인 프라이버시 염려와 프라이버시 보호전략 사용의 차이에 관한 연구”, 미디어, 젠더와 문화, 제12권, 2009, pp. 165-190.

이병수, 황지상, 황동욱, 최봉철, 홍용진, “금융권 개인정보 활용 실태와 개인정보보호법 시행에 따른 IT 컴플라이언스 준수방안 연구”, 정보보호학회지, 제23권, 제1호, 2013, pp. 35-43.

이상진, “인터넷을 이용한 금융 거래 시 보안성 강화 수단에 관한 고찰”, 정보보호학회지, 제15권, 제4호, 2005, pp. 38-42.

이수미, 성재모, “국내 전자금융 현황 및 보안위협 분류”, 정보보호학회지, 제21권, 제7호, 2011, pp. 53-61.

이장형, “금융기관의 보안과 통제가 ERP 시스템 성과에 미치는 영향”, 회계연구, 제15권, 제1호, 2010, pp. 309-329.

이정호, “전자금융 침해사고 예방 및 대응 강화 방안, 정보보호학회지”, 제18권, 제5호, 2008, pp. 1-20.

이준택, 차인환, “금융분야의 정보보안 기술의 동향”, 전자공학회지, 제40권, 제8호, 2013, pp. 16-29.

이태민, 김동원, “모바일 인터넷 서비스 품질의 구성요인이 고객만족에 미치는 영향에 관한 연구-관여도의 조절효과와 항공 서비스 전략적 시사점을 중심으로”, 한국항공경영학회지, 제9권, 제1호, 2011, pp. 51-70.

장익진, “인터넷 사용자의 위험 지각, 효능감과 개인정보 유출 예방 활동 간의 관계 연구: RPA 프레임웍을 기반으로”, 국민대학교 대학원 석사학위논문, 2009.

정기한, 허미옥, 신재익, “기업의 사회적 책임, 이미지, 신뢰, 몰입, 고객충성도 간의 관계에 관한 연구”, 한국경영학회 통합학술발표논문집, 2007, pp. 1-14.

정익재, “정보보안 취약성 분석과 정책적 대응논리”, 한국정책학회보, 제16권, 제2호, 2007, pp. 211-239.

조성인, 박태형, 임종인, “새로운 전자금융 거래법에서의 전자금융 사고 대응방안에 관한 연구”, 융합보안논문지, 제8권, 제4호, 2008, pp. 9-19.

조창훈, 이정진, “효과적인 컴플라이언스 기능 운영에 관한 소고”, 강원법학, 제38권, 2013, pp. 695-739.

조화제, 김귀남, “종심방어개념의 금융정보보호 적용 연구”, 융합보안논문지, 제9권, 제1호, 2009, pp. 55-63.

최진식, 강영철, “직관적 탐지이론을 통한 정부의 위험관리 신뢰요인에 관한 연구; 고리원전사고 위험관리에 대한 신뢰를 중심으로”, 정부학연구, 제18권, 제3호, 2012, pp. 325-358.

최진혁, “기업 위기관리(Crisis Management) 전략에 관한 연구-해외 Pandemic Planning 사례를 중심으로”, 기업경영연구(구 동림경영연구), 제36권, 2010. pp. 149-169.

한국인터넷진흥원, “독일의 IT법제 현황 및 국내 법적 개선방안 연구”, 방송통신정책연구, 10-진흥-라-4, 2010a, www.kcc.go.kr/download.do?fileSeq=31994.

한세진, “개인정보보호법이 금융권에 미치는 영향과 문제점에 관한 고찰”, 융합보안논문지, 제13권, 제1호, 2013, pp. 31-36.

정익재, “정보사회의 불확실성 관리를 위한 정책논리와 대응: 정보보안 사고의 유형화와 대응책”, 국가정책연구, 제25권, 제4호, 2011, pp. 55-76.

Baer, M. H., "Governing Corporate Compliance", *Boston College Law Review*, Vol.50, 2009, pp. 949-958.

Barclay, D., C. Higgins, and R. Thompson, "The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration", *Technology studies*, Vol.l2, No.2, 1995, pp. 285-309.

Bellman, S., E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International differences in information privacy concerns: A global survey of consumers", *The Information Society*, Vol.20, No.5, 2004, pp. 313-324.

Bhattacherjee, A. and C. Sanford, "Influence processes for information technology acceptance: an elaboration likelihood model", *MIS quarterly*, Vol.20, No.4, 2006, pp. 805-825.

Boehmer, W., "Cost-benefit trade-off analysis of an ISMS based on ISO 27001", Availability, Reliability and Security, ARES International Conference on *IEEE*, 2009, pp. 392-399.

Buchanan, T., C. Paine, A. N. Joinson, and U. D. Reips, "Development of measures of online privacy concern and protection for use on the Internet", *Journal of the American Society for Information Science and Technology*, Vol.58, No.2, 2007, pp. 157-165.

Cheung, C. M. and M. K. Lee, "Understnding consumer trust in internet-shopping: a multidisciplinary approach", *Journal of the American Society For Information Science and Technology*, Vol.57, No.4, 2006, pp. 479-92.

Chin, W. W., "The partial least squares approach to structural equation modeling", *Modern methods for business research*, Vol.295, No.2, 1998, pp. 295-336.

Chin, W. W. and A. Gopal, "Adoption intention in GSS: relative importance of beliefs", *ACM Sig MIS Database*, Vol.26, No.2/3, 1995, pp. 42-64.

Chin, W. W., B. L. Marcolin, and P. R. Newsted, "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study", *Information systems research*, Vol.14, No.2, 2003, pp. 189-217.

Cunningham, L. F., J. Gerlach, and M. D. Haper, "Perceived risk and e-banking services: an analysis from the perspective of the consumer", *Journal of Financial Services Marketing*, Vol. 10, No.2, 2005, pp. 165-178.

Einwiller, S. and M. Will, "The role of reputation to engender trust in electronic markets", *Proceedings of the 5th International Conference on Corporate Reputation, Identity, and Competitiveness*, Vol.17, No.19, 2001, pp. 196-209.

Eiser, J. R., "Social judgment", U.K: Open University Press, 1990.

Erickson, P. A., *Emergency response planning: for corporate and municipal managers*, Academic Press, 1999.

Fornell, C. and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol.18, No.1, 1981, pp. 39-50.

Gefen, D. and D. Straub, "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example", *Communications of the Association for Information systems*, Vol.16, No.1, 2005, pp. 91-109.

Gefen, D., D. Straub, and M. C. Boudreau, "Structural equation modeling and regression: Guidelines for research practice", *Communications of the association for information systems*, Vol. 4, No.7, 2000, pp. 1-70.

Goodwin, C. and I. Ross, "Consumer responses to

service failures: influence of procedural and interactional fairness perceptions", *Journal of Business Research*, Vol.25, No.2, 1992, pp. 149-163.

Grönroos, C., "Defining marketing: a market-oriented approach", *European journal of marketing*, Vol.23, No.1, 1989, pp. 52-60.

Hocutt, M. A., M. R. Bowers, and D. Todd Donavan, "The art of service recovery: fact or fiction?", *Journal of Services Marketing*, Vol.20, No.3, 2006, pp. 199-207.

Jarvenpaa, S. L. and P. A. Todd, "Consumer reactions to electronic shopping on the World Wide Web", *International Journal of electronic commerce*, Vol.1, No.2, 1996, pp. 59-88.

Kalakota, R., M. Robinson, and D. R. Kalakota, "M-Business: the race to mobility", New York: McGraw-Hill, 2002.

Kuhlmeier, D. and G. Knight, "Antecedents to internet-based purchasing: a multinational study", *International Marketing Review*, Vol.22, No.4, 2005, pp. 460-73.

Kutner, M. H., C. Nachtsheim, and J. Neter, "Applied linear regression models", McGraw-Hill/ Irwin, 2004.

Laforet, S. and X. Li, "Consumers' attitudes towards oline and moblile banking in china", *International Journal of Bank Marketing*, Vol.23, No.5, 2005, pp. 32-80.

Malhotra, N. K., S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol.15, No.4, 2004, pp. 336-355.

Milne, G. R., L. I. Labrecque, and C. Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices", *Journal of Consumer Affairs*, Vol.43, No.3, 2009, pp. 449-473.

Moorman, C., G. Zaltman, and R. Deshpande, "Relationships between providers and users of market research: The dynamics of trust", *Journal of marketing research*, Vol.29, No.3, 1992, pp. 314-328.

Pavlou, P. A., "State of the information privacy literature: where are we now and where should we go", *MIS quarterly*, Vol.35, No.4, 2011, pp. 977-988.

Pires, G., J. Stanton, and A. Eckford, "Influences on the perceived risk of purchasing oline", *Journal of Consumer Behaviour*, Vol.4, No.2, 2004, pp. 118-131.

Schlosser, A. E., T. B. White, and S. M. Lloyd, "Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online Purchase intentions", *Journal of Marketing*, Vol.70, No.2, 2006, pp. 133-148.

Slovic, P., "Perception of risk", *Science*, Vol.236, No.4799, 1987, pp. 280-285.

Smith, H. J., T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review", *MIS quarterly*, Vol.35, No.4, 2011, pp. 989-1016.

Srite, M. and E. Karahanna, "The role of espoused national cultural values in technology acceptance", *MIS quarterly*, Vol.30, No.3, 2006, pp. 679-704.

Tax, S. S. and S. W. Brown, "Recovering and learning from service failure", *Sloan Management Review*, Vol.49, No.1, 2012, pp. 75-88.

Tax, S. S., S. W. Brown, and M. Chandrashekaran, "Customer evaluations of service complaint experiences: implications for relationship marketing", *The Journal of Marketing*, Vol.40, 1998, pp. 60-76.

Tenenhaus, M., V. E. Vinzi, Y. M. Chatelin, and

C. Lauro, “PLS path modeling”, *Computational statistics and data analysis*, Vol.48, No.1, 2005, pp. 159-205.

Venkatesh, V., M. G. Morris, and F. D. Davis, “User acceptance of information technology: toward a unified view”, *MIS Quarterly*, Vol.27, No.3, 2003, pp. 425-478.

Wetzels, M., G. Odekerken-Schröder, and C. Van Oppen, “Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration”, *MIS Quarterly*, Vol.33, No.1, 2009, pp. 177-195.

White, M. P. and J. R. Eiser, “Marginal trust in risk managers: Building and losing trust following decisions under uncertainty”, *Risk Analysis*, Vol.26, No.5, 2006, pp. 1187-1203.

Wixom, B. H. and H. J. Watson, “An empirical investigation of the factors affecting data warehousing success”, *MIS quarterly*, Vol.25, No.1, 2001, pp. 17-41.

落合誠一, “企業コンプライアンス確立の意義(特集 企業コンプライアンスの深 化: いま, 企業に求められているもの)”, ジュリスト, 제3권, 제1438호, 2012, pp. 12-17.

지디넷코리아, “흩어진 개인정보보호법 통합 법안 발의”, http://www.zdnet.co.kr/news, 2014.

전자신문, “전자금융사기 급증 5년간 4020억 원 털렸다”, http://www.etnews.com, 2014.

디지털타임스, “(DT 광장) 보안 컴플라이언스 대응위한 파트너십”, http://www.dt.co.kr, 2008.

국민일보, “핵연료 손상 ‘원전사고’ … 설비기능 이상시 ‘고장’”, 2012.

한겨레, “고리 1호기 ‘노심 손상빈도’ 기준치 넘고도 수명연장”, 2012.

한겨레, “‘원전 해커’ 석달만에 재등장 … 돈 요구”, http://www.hani.co.kr/arti/society/society_general/682095.html, 2015.

한국경제, “개인정보 털릴라 … 꼭꼭 숨는 소비자”, http://www.hankyung.com, 2014.

경찰청, http://www.police.go.kr/main.html.

국민카드, https://www.kbcard.com.

금융감독원, http://www.fss.or.kr/fss/kr/main.html.

농협, https://www.nonghyup.com/Main/main.aspx.

롯데카드, http://www.lottecard.co.kr/app/index.jsp.

위키피디아, http://ko.wikipedia.org/wiki.

한국은행, “6월 말 현재 국내 인터넷 뱅킹 서비스 이용현황”, http://www.bok.or.kr, 2014.

한국은행, “2012년 중 국내 인터넷 뱅킹 서비스 이용현황”, http://www.kif.re.kr, 2013.

한국인터넷진흥원, “IT 컴플라이언스와 정보보호관리체계(ISMS)”, KISA 기업보안관리팀, http://home.sogang.ac.kr, 2010b.

한국전화결제산업협회, http://www.kpbia.org.

Deloitte, “Pandemic Planning: Can Your Business Withstand Major Workforce Disruption?”, www.deloitte.com, 2009.

Harris, “National survey on consumer privacy attitudes”, http://www.epic.org/privacy/survey, 2004.

Information Systems Review
Volume 17 Number 1
April 2015

A Study on the Effect of Information Security Compliance and Crisis Management on Information Security Trust

Il-han Yoon* · Sun-dong Kwon**

Abstract

Electronic financial accidents are constantly happening and these accidents are taking place by a combination of several causes such as technique, human, and structure. Among electronic financial accidents, personal information disclosure is most frequently happening and becomes big problems, because secondary damage like voice phishing causes great loss to society.

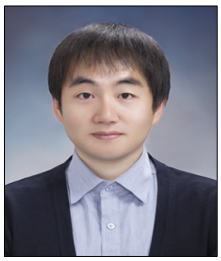
This research model is that financial information security compliance affects the crisis response of financial institutions and financial authorities and these crisis responses affect financial information security trust. Research target is people who experienced the disclosure of their own financial information. For empirical verification, survey questionnaires were distributed and total 103 questionnaires were collected and analyzed.

As results of data analysis, all hypotheses were accepted. First, financial information security compliance influenced the crisis response of financial institutions and authorities. Second, the crisis response of financial institutions and authorities affect financial information security trust. Third, at the moderating effect analysis, the importance of personal financial information moderated the effect of the crisis response of financial institutions on financial information security trust. And the disclosure level of personal financial information moderated the effect of the crisis response of financial authorities on financial information security trust.

Keywords: ***Electronic Finance, Financial Information Security Trust, Information Security Compliance, Personal Financial Information, Crisis Management***

* Department of Information Security Management, Chungbuk National University
** Corresponding Author, Department of MIS, Chungbuk National University

◐ 저 자 소 개 ◑



윤 일 한 (ismbest@cbnu.ac.kr)

충북대학교 법학과를 졸업하고 현재 충북대학교 정보보호경영학과 석사과정 재학 중이다. 한국경영정보학회 학술대회, 한국경영학회 통합학술대회, Pacific Asia Conference on Information Systems workshop 등에서 개인정보 유출 시 인터넷 뱅킹의 지속적 사용의도, 대량 개인정보 유출시 금융당국과 금융기관의 대응 등의 논문을 발표를 하였다. 주요 관심분야는 금융정보보안 컴플라이언스, 잊혀질 권리, ICT 부작용, 정보보안 법률, 정보보호 전략 등이다.

권 순 동 (sdkwon@cbnu.ac.kr)

현재 충북대학교 경영정보학과 교수로 재직하고 있다. 서울대학교 경영대학에서 경영정보학전공으로 박사학위를 취득하였다. British Journal of Management, Effective Executive, Journal of Information Technology Application and Management, Information Systems Review, Asia Pacific Journal of Information Systems, 한국경영과학회지, 경영학연구 등의 국내·외 저널에 다수의 논문을 발표하였고, 저서 및 역서로 한국기업의 경영정보시스템 변천사(서울대), 경영정보론(홍문사), 비즈니스 정보시스템(생능출판사), B2B와 e마켓플레이스(법문사), 대학경영혁신과 정보인프라 구축(서울대) 등이 있다. 주요 관심분야는 정보보호, 전자상거래에서의 위험관리, 국가문화, SCM, 전자매체 커뮤니케이션의 성과향상방안 등이다.

논문접수일 : 2015년 01월 16일 **게재확정일 : 2015년 04월 06일**
1차 수정일 : 2015년 03월 18일