「한국 시스템다이내믹스 연구」 제16권 제4호 (2015. 12) : 31-50

시스템 사고를 통한 금융 규제와 보안 산업의 구조 분석

A Structural Analysis between Financial Regulations and Security Industry through the Systems Thinking

이정하*
Lee, Jeong-Ha

Abstract

The purpose of this research is to understand a structural relationship between financial regulations and security industry based on the systems thinking perspective using causal loop analysis.

As a result, the positive regulations on security technology against finance security incidents shrink the autonomy of the security industry and will deteriorate the competitiveness of the security industry through the unknown feedback loop.

The conclusion provides the direction that policy makers understand causal loop diagram related current regulations and open enough to the consideration of the negative regulations.

Keywords: 정보보안정책, 전자금융거래법, 네거티브규제, 인과지도, 시스템 사고
(Information Security Policy, Electronic Financial Transaction Act, Negative Regulation, Causal Loop Diagram, Systems Thinking)

* 서울과학종합대학원대학교 경영학과 박사과정(단독저자, jasonlee2484@gmail.com)

Ⅰ. 서 론

대한민국은 초고속 인터넷 및 스마트폰의 보급률이 세계에서 가장 높으며, 이를 이용한 전자금융거래가 증가하고 있다(김인식, 2006; 이수미 외, 2011). 「감사원 감사결과보고서」(2014b)에 의하면, 2014년 금융회사에서 대량의 개인정보유출사고가 발견되어 국민이 전자금융거래에 대한 안전성과 신뢰성을 의심하여 대규모의 회원 탈퇴가 발생하였다. 개인정보 유출 사건 중 단일사건으로 가장 많은 개인정보가 유출된 사고였으며, 금융당국의 사건 공표 후 약 1개월 동안 금융회사에 대한 신뢰를 잃고 6%~12%의 고객이 탈퇴를 하였다(윤일한 외, 2015). 이러한 일이 발생할 때마다 금융회사를 감독하는 규제 당국은 대응 대책을 마련하고 점검을 수행하며 재발을 방지하고자 노력하고 있으나, 금융 보안 사고는 끊임없이 발생하고 있다.

금융 보안 사고가 발생하면 규제 당국은 정책을 수립하고 엄격한 규제를 나열하여 금융회사의 보안을 강화하였지만, 단선적인 사고를 통하여 수립된 이러한 포지티브(Positive) 규제[1]는 보안 산업의 자율성을 위축시키는 결과로 나타나고 있다(황태희, 2011). 최근에는 공인인증서를 사용하기 위해 불가피하게 이용되던 액티브엑스(ActiveX)[2]에 대한 취약점이 발견되면서 공인인증서의 의무사용에 대한 이슈가 제기되었다.

본 연구의 목적은 금융 보안 사고에 대한 정부의 규제가 조직의 정보보호활동 및 보안 산업과 어떠한 인과관계를 나타내고 있는지에 대해 시스템 사고를 통해 인과지도를 작성하고자 하며, 작성된 인과지도를 통하여 정부의 정책 결정 시 고려하여야 할 사항들을 이해할 수 있도록 하여 궁극적으로 금융 보안 사고를 예방하고 전자금융거래의 안전성과 신뢰성을 회복하는 데 이바지하고자 한다. 본 연구에서는 금융 보안 사고와 규제의 현황을 살펴보고, 정보보호활동의 선행연구를 기초하여 금융 보안 사고에 대해 시스템 사고로 접근하여 해석해보았다. 또한, 금융 보안 사고에 대응하기 위한 정부의 금융 규제와 보안 산업 간의 시스템 구조를 이해하기 위해 통합적인 인과지도를 작성하여 시스템다이내믹스 관점에서의 분석을 수행하고 인지의 한계로 인하여 고려되지 못한 루프에 대해 이해할 수 있도록 시스템 구조를 설명하였다.

---

1) 규제의 근거가 되는 법령에서 원칙적으로 금지하고 특정한 사항을 열거하여 제한적으로 허용하는 방식

2) 마이크로소프트(Microsoft)가 개발한 재사용 가능한 객체 지향적인 소프트웨어 개발에 사용되는 기술이며, 최근 취약점이 발표되면서 보안 문제를 일으키고 있다.

II. 이론적 고찰 및 선행연구

1. 금융회사의 보안 사고 현황

국내 보안 사고는 2003년 1월 25일 KT의 DNS 서버가 공격을 받아 인터넷이 마비되었던 “1.25 인터넷 대란” 이후에 증가하고 있으며, 2009년 7월 7일 정부기관, 포털 및 은행 사이트를 마비시킨 “7.7 DDoS 공격”을 시작으로 금융회사를 대상으로 하는 보안 사고도 증가하고 있다(정익재, 2011; 감사원, 2014a; 감사원, 2014b).

〈표 1〉 금융회사의 주요 보안 사고 현황

발생 시기	사고 대상 기관	유형	피해 규모	비고
2011. 3.	A은행, B은행 등 9개 금융회사	전산망 마비	9개 금융회사 전산망 일시 마비	3·4 DDoS 공격
2011. 4.	C캐피탈	개인정보유출	175만 명	캐피탈 해킹사건
2011. 4.	D은행	전산망 마비	560억여 원	은행 전산 마비 사태
2011. 5.	E투자증권	개인정보유출	1만 3천여 건	증권사 개인정보유출
2013. 3.	F은행, G은행 등 5개 금융회사	전산망 마비	5개 금융회사의 4만 8천여 대 마비	3·20 전산 대란
2013. 4.	H은행	개인정보유출	13만 명	은행 개인정보유출
2014. 1.	I카드, J카드, K카드	개인정보유출	2천만 명	카드사 개인정보 대량유출 사건

* 자료: 감사결과보고서-금융권 정보보호 및 사이버안전 관리·감독 실태의 자료를 연구자가 다시 편집함

2013년 1월 7일 금융회사에서 1억 400만 건의 개인정보가 유출되는 초유의 정보보안 사고가 발생했고, 금융당국은 2014년 1월 8일 공표하였다(윤일한 외, 2015). 이에 대응하여 감사원은 금융회사의 개인정보 유출 관련 검사와 감독 실태를 점검하였다. 「감사원 감사결과보고서」(2014b)에 의하면, 최근 5년간(2009년~2013년) 9천만 건 이상의 개인정보 유출 사고가 발생한 것으로 나타난다.

〈표 2〉 최근 5년간 금융업권별 개인정보 유출 현황

구분	회사수	유출건수	금융회사(유출시점, 유출건수)
합계	20	91,327,562	
신용카드	4	64,269,183	AA카드(2010.1, 300), BB카드(2011.5, 97,331), CC카드(2013.2, 44,498,568), DD카드(2013.12, 19,672,984)
은행	4	24,434,056	EE은행(2009.9, 109), FF은행(2011.11, 149,151), GG은행(2012.6, 24,268,743), HH은행(2012.12, 16,053)
캐피털	6	1,946,560	II캐피털(2009.9, 90,530, 2011.12, 5,796), JJ캐피털(2009.9, 95,373), KK캐피털(2010.3, 7), LL캐피털(2010.10, 4,838), MM캐피털(2011.2, 15), NN캐피털(2011.4, 1,750,001)
투자증권	3	355,102	OO투자증권(2011.4, 342,221), PP투자증권(2011.5, 12,849), QQ투자증권(2011.5, 32)
보험	2	321,910	RR화재(2013.2, 164,009), SS손해보험(2011.3, 157,901)
신용정보	1	751	TT신용정보(2011.4, 751)

* 자료: 감사결과보고서-금융회사 개인정보 유출 관련 검사·감독 실태

금융회사의 개인정보유출 사고의 원인을 살펴보면, 〈표 3〉과 같이 취약점 방치, 내·외부직원의 관리부실이 주요 원인으로 밝혀졌으며, 2012년과 2013년은 외부의 해킹에 의한 유출 사고가 아닌 내부 업무를 수행하는 내·외부직원들에 의한 유출인 것을 알 수 있다(감사원, 2014b). 과거의 보안 사고는 정보시스템 내 방치된 취약점을 이용한 해킹사고가 상당한 부분을 차지하였지만, 최근에는 내부자에 의한 위협이 크게 증가하고 있다. 이러한 내부자에 의한 보안 사고는 정보보안인식의 강화와 정보보호활동을 통하여 방지할 수 있으며, 정보보호활동을 강화하기 위해 경영진의 리더십은 중요한 역할을 수행하는 것으로 나타났다(유진호, 2014).

〈표 3〉 최근 5년간 개인정보 유출 원인별 유출 현황

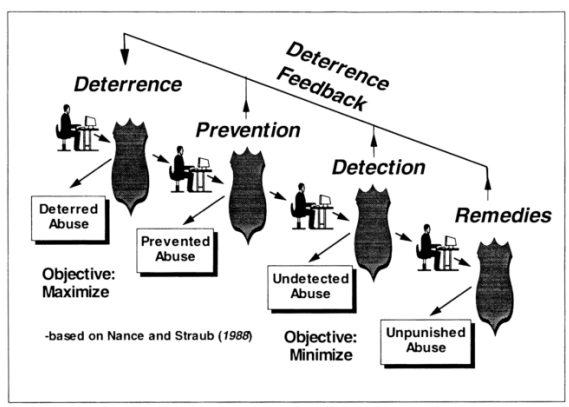
(단위: 건)

구분	합계	2009년	2010년	2011년	2012년	2013년
합계	91,327,562	186,012	5,145	2,516,048	24,284,796	64,335,561
해킹 취약점 방치	2,449,658	185,903	-	2,263,755	-	-
외부직원 관리부실	88,686,777	-	-	246,482	24,268,743	64,171,552
내부직원 열람 권한 과다설정	190,711	-	4,838	5,811	16,053	164,009
내부직원 열람권한 남용	416	109	307	-	-	-

* 자료: 감사결과보고서-금융회사 개인정보 유출 관련 검사·감독 실태

2. 정보보호활동에 대한 선행연구

정보보호활동에 대해 Straub 와 Welke(1998)는 억제이론을 바탕으로 보안활동주기(Security Action Cycle)를 설명하였다. 억제(Deterrence), 예방(Prevention), 탐지(Detection), 교정(Remedies)의 네 단계 과정을 나타내어 단계마다 보안 사고가 발생할 수 있고, 이를 방지하지 하기 위해 네 단계의 활동이 차례로 이루어진다는 것을 설명한 것이다. 이렇게 정보보호활동이 수행되는 가운데 나타나는 보안 사고는 개별적으로 발생할 수도 있고 차례대로 발생할 수도 있으며, 이러한 보안 사고가 발생할 경우 이를 억제하는 기능을 가져야 한다(Theoharidou *et al.*, 2005; Foroughi, 2008; 정우진 외, 2012).



* 자료: Straub and Welke(1998)

[그림 1] 보안활동주기(Security Action Cycle)

금융회사의 정보보호활동은 보안활동주기에 의해 설명될 수 있으며, 보안 사고를 방지하기 위해 네 단계의 영역에 해당하는 활동을 수행하고 있다. 내부 및 외부의 공격 및 남용을 억제하기 위한 활동에서부터 탐지된 공격 및 남용에 대한 대응 활동을 수행하고 있다. 협의의 정보보호활동은 회사 내에서 이루어지지만, 광의의 정보보호활동은 정부의 규제와 보안 산업으로 확대되어 이루어지고 있다고 할 수 있다.

3. 금융 정보보호를 위한 정부의 규제

2006년 4월 28일 전자금융거래법의 제정된 후, 2015년 1월 20일까지 열 차례 개정이 되었다. 전자금융거래법의 제정이유는 “인터넷뱅킹 등 전자금융거래가 확산되고 전자화폐 등

새로운 전자지급수단이 출현함에 따라 비대면성 등과 같은 전자금융거래의 특성을 반영하여 거래당사자의 권리・의무 등 법률관계를 명확히 하는 한편, 전자금융업무를 영위하는 자에 대한 허가・등록 및 감독에 관한 사항을 체계적으로 정비함으로써 전자금융거래의 안전성과 신뢰성을 확보하려는 것임"[3]이라고 밝혀져 있다. 열 차례의 개정 중 네 차례는 타법개정 때문에 발생한 것이고, 여섯 차례는 일부 개정이 발생하였다. 일부 개정은 2007년, 2008년, 2011년, 2013년, 2014년, 2015년에 발생하였으며, 제정된 초기와 최근에 개정이 잦아지는 경향이 있음을 확인할 수 있으며, 〈표 4〉와 같이 최근의 개정이유는 금융 보안 사고에 대한 대응책에 대한 내용으로 나타났다.

〈표 4〉 전자금융거래법의 최근 개정 이력

구분	개정일	개정이유
1	2014. 10.15.	개인정보 유출방지 및 해킹 등 전자적 침해사고에 대한 대응을 위하여 일정 규모 이상의 대형 금융회사 및 전자금융업자인 경우 정보보호최고책임자의 겸직을 제한하고, 정보기술 부문의 정보보호 관련 업무를 위탁받은 전자금융보조업자가 해당 업무를 제3자에게 재위탁하는 것을 원칙적으로 금지하며, 금융회사 및 전자금융업자의 정보보호 및 IT보안의 중요성을 감안하여 형벌 등의 제재수준을 상향조정하고, 징벌적 과징금제도를 도입하는 한편, 전자금융거래에 있어 공인인증서 사용을 강제하는 근거로 작용할 수 있는 규정을 보완하여 금융회사가 자율적으로 금융보안 수단을 결정할 수 있도록 하고, 이용자의 선택에 따른 전자자금이체의 지급 효력 지연조치를 의무화하며, 보존기간이 경과한 전자금융거래기록에 대한 파기의무를 부여하려는 것임
2	2013. 5.22.	전자금융거래의 안전한 기반 조성을 위하여 전자금융업자 등의 해킹 관련 책임을 명확히 하고, 금융회사 및 전자금융업자로 하여금 전자금융기반시설에 대한 취약점을 스스로 분석・평가하도록 하며, 전자금융기반시설에 대한 전자적 침해행위 금지 및 침해사고의 발생 시 금융위원회・금융회사 등 의 대응조치를 신설하고, 금융감독원장이 필요한 경우에는 전자금융보조업자에 대해서도 조사를 할 수 있도록 하는 한편, 그 밖에 현행 제도의 운영상 나타난 일부 미비점을 개선・보완하려는 것임
3	2011. 11.14.	전자금융거래의 안전성과 신뢰성을 확보하고 전자금융업의 건전한 발전을 위하여 금융기관 등으로 하여금 정보보호최고책임자를 지정하여 조직 내 정보보호 위험을 상시적으로 관리하도록 하고, 영업주가 종업원 등에 대한 관리・감독상 주의의무를 다한 경우에는 처벌을 면하게 함으로써 양벌규정에도 책임주의 원칙이 관철되도록 하는 한편, 양벌규정의 적용대상이 되는 일부 벌칙조항 중 벌금형이 별도로 규정되어 있지 않은 경우에는 벌금액을 개별적으로 규정함으로써 벌칙 적용을 명확히 하려는 것임

* 자료: 국가법령정보센터 사이트

3) 국가법령정보센터 인용(http://www.law.go.kr)

전자금융거래법은 금융회사에서 발생한 보안 사고에 대해 법적인 규제를 강화하기 위해 지속해서 개정됐다. 또한, 보안 사고와 개정된 내용의 관계를 보면 〈표 5〉와 같이 나타나며, 사고에 대한 대응으로 전자금융거래에 대한 규제를 강화하고 있는 것을 알 수 있다.

〈표 5〉 금융회사의 보안 사고와 전자금융거래법의 개정간의 관계

시기	보안 사고 유형	개정일 및 주요 개정 내용
2011.3.	3・4 DDoS 공격	〔2011년 11월 14일 일부개정〕 정보보호최고책임자 지정 의무화 정보보호최고책임자의 업무수행범위 양벌규정에 책임주의 원칙 반영
2011.4.	해킹 사건	
2011.4.	전산 마비 사태	
2011.5.	개인정보유출	
2013.3.	3・20 전산 대란	〔2013년 5월 22일 일부개정〕 해킹 관련 전자금융사업자 등의 책임 명확화 정보기술부문 계획수립 및 제출 의무화 전자금융기반시설에 대한 취약점 분석・평가 의무화 전자적 침해행위 금지 및 침해사고 대응 근거 마련 현금자동지급기 등 전자적 장치로부터의 현금인출 최고한도 제한 신설 전자금융보조업자에 대한 조사 강화
2013.4.	개인정보유출	
2014.1.	개인정보 대량유출 사건	〔2014년 10월 15일 일부개정〕 전자자금이체의 일정시간 지급효력 지연 조치 공인인증서 사용의 자율화 정보보호최고책임자의 겸직을 제한 불필요한 전자금융거래기록의 파기근거 마련 정보보호 관련 업무를 제3자에게 재위탁 금지 전자금융거래정보를 제공・누설하거나 업무상 목적 외에 사용한 경우에 대한 과징금 부과규정을 신설 타인에게 제공・누설하거나 업무상 목적 외에 사용하는 행위에 대한 벌칙을 강화 전자금융거래의 안전성과 신뢰성을 위한 의무를 이행하지 않을 경우 등에 대한 과태료 부과규정을 신설

* 자료: 감사원과 국가법령정보센터의 자료를 연구자가 다시 편집함

2014년 5월 전국경제인연합회가 국내에 사업하는 외국계 금융회사를 대상으로 조사한 '한국 금융의 경쟁력 현황 및 개선 과제'[4]에 따르면, 선진국에 대비하여 한국 금융회사의

4) 전국경제인연합회 홈페이지 (http://www.fki.or.kr/FkiAct/Promotion/Report/View.aspx?content_id=925f5ad5-1df4-49c6-aa32-8f484bbebf76)

경쟁력은 67.5점으로 낮게 평가되었다. 응답한 기업의 64.2%가 최대의 문제점으로 지적한 것은 '과도한 규제 및 정부 개입'이었다. 금융회사 자체도 규제로 발목이 잡히는 상황에서 다른 분야와 연결된 사업에 대하여는 더욱더 악영향이 있을 수 있다. 특히, 정보보안같이 IT와 관련이 많은 산업과의 결합에서는 더 큰 괴리감이 존재한다.

정부 규제의 형태는 네거티브(Negative) 규제[5]와 포지티브 규제로 나누어서 설명할 수 있다. 포지티브 방식은 "규제의 근거가 되는 법령에서 특정한 사항을 열거하여 제한적으로 허용하는 방식으로 되어 있는 규제"이며, 반대로 네거티브 방식은 "특정한 사항을 제한적으로 금지하는 방식"으로 정의되어 있다. 규제의 형태가 포지티브에서 네거티브로 변경되면, 산업의 자율성과 영업의 자유가 보장될 가능성이 크며, 규제 당국의 행정에 집행되는 비용이 경감될 가능성도 있다(황태희, 2011). 전자금융거래법의 행정규칙인 전자금융감독규정 및 전자금융감독규정 시행세칙은 근거법령에서 허용하는 사항을 열거하는 포지티브한 방식의 규제를 취하고 있다. 규제 당국은 법령에 허용된 내용이 포함되지 않은 경우에는 일단 금지된 것으로 해석하는 것이 일반적이고, 그로 인해 민간 부분에 대한 경제적 행위의 포괄적인 금지가 이루어져 상당한 부분에 대한 과잉 규제 혹은 불필요한 규제가 이루어지고, 결과적으로 민간 부분의 자율성을 침해하거나 경제적인 활동을 위축시키는 부작용을 일으킬 수 있다(황태희, 2011).

4. 시스템다이내믹스 분석의 필요성

현대사회에서 수행되는 기능 대부분은 복잡하고 다양하여 시스템 상호 간의 연관성 및 의존성을 중요한 특성으로 하고 있으나, 정부의 많은 정책 결정자들은 인과관계를 이해하지 못하고 단일 방향만으로 흐르는 정태적인 시각과 임기 내 성과를 달성하기 위한 단기적인 시각을 가지고 전문적인 분야에 국한된 사고를 벗어나지 못하고 있으며 이를 단선적 사고의 결과라고 말한다(장남정 외, 2013).

시스템다이내믹스는 이러한 복잡한 문제들에 대해 구조적인 원인을 파악하고 구조에서 문제의 해결책을 찾아내기 위한 연구방법론으로 단선적이고 정태적인 시각으로 원인을 알 수 없었던 정부의 정책 혼란 등을 해결하기 위한 도구로써 경영 및 행정 등 다양한 분야에서 문제 해결을 위한 도구로 사용된다(김도훈 외, 1999).

정책수립에서의 시스템 사고는 궁극적으로 시스템을 개선할 수 있는 문제를 통합된 구조로 바라봄으로써 접근 시각에서 정태성, 단기간성, 부분성을 버리고 인과관계를 이해하여 쌍방향으로 흐르는 피드백을 이해하여 효과적인 문제 해결 지점을 발견하는 것이다. 시

5) 규제의 근거가 되는 법령에서 원칙적으로 허용하고 특정한 사항을 열거하여 제한적으로 금지하는 방식.

스템다이내믹스를 적용하기 위해서는 우선 문제를 식별하고 문제의 원인을 파악하고 결과와의 구조를 파악하여 시스템의 전체 구조를 작성하여 분석한다(김도훈 외, 1999). 구조란 인과의 상호 연계성을 고려하여 피드백 루프(Feedback loops)를 말하며, 행태(Behavior)란 다양한 변화의 동태적인 행태 유형(Dynamic pattern of behavior)으로 설명된다(김동환, 2000). 전체적인 구조를 이해하고 분석을 하면 작은 노력으로 큰 결과를 얻을 수 있는 정책수립의 방향과 지점인 '전략적 지렛대'를 발견할 수 있게 된다(장남정 외, 2013).

금융보안정책 및 보안 산업과 관련한 시스템다이내믹스 연구로는 정보보호 산업 육성정책의 상대적 효과 분석(전재호, 2003)을 찾아볼 수 있었으나, 정부의 산업 육성을 위한 정책에 대한 시스템 사고를 통한 모형과 시뮬레이션을 제시하였으며 정부의 규제에 대한 부분은 설명이 없어 금융보안정책에 대한 직접적인 선행연구는 찾아보기 어려웠다.

금융회사의 보안 사고에 대한 정부의 정책에서 시스템다이내믹스를 통한 시스템 사고로 문제를 볼 필요성은 다음과 같은 관점으로 말할 수 있다.

첫째, 단순한 원인과 결과를 가정한 단선적 사고를 버리고, 정책의 통합적이고 시스템 사고 관점에서 금융 보안 사고에 대한 정부의 정책을 수립할 수 있다(장남정 외, 2013).

둘째, 금융 보안 사고와 정부 정책에 대한 강화 루프와 균형 루프를 이해하여 시스템 전체의 구조를 이해하고 다이내믹한 효과를 고려하여 정책을 수립할 수 있다(장남정 외, 2013).

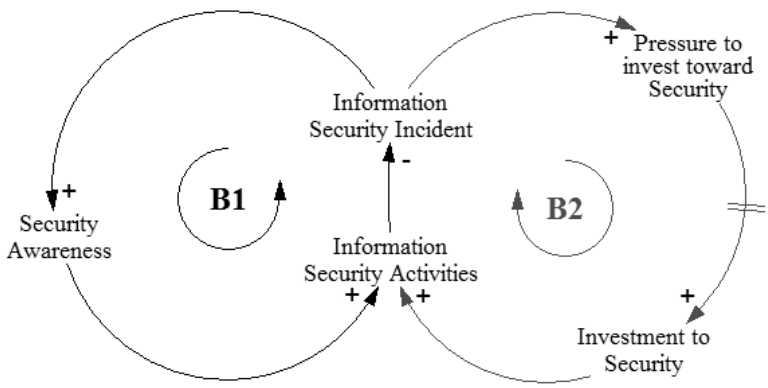
본 연구에서는 금융회사의 보안 사고에 따른 정부의 정책이 보안 산업에 미치는 영향을 인과지도로 나타내어 정책 결정 시 단선적인 시각과 단기적인 견해를 고려하는 정태적인 관점에서 벗어나 보안 산업의 자율성을 보장하여 보안 산업 발달에 이바지할 수 있는 정책을 수립하는 데 도움을 주고자 한다.

III. 금융 보안 사고에 대한 시스템 사고

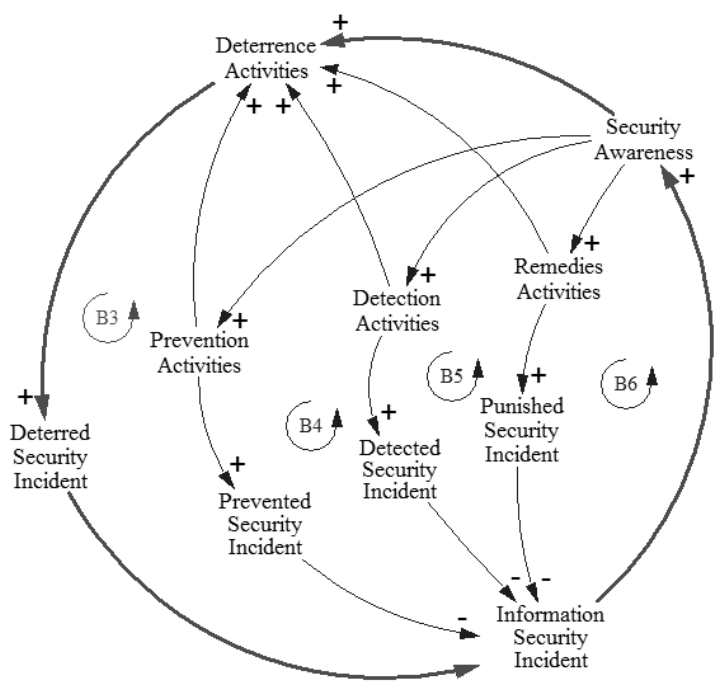
1. 정보보호활동에 대한 시스템 사고

보안 사고에 대한 경험은 보안인식에 긍정적인 영향을 미치며, 보안인식은 정보보호활동에 영향을 미친다(김상현 외, 2012). 이러한 측면에서 인과지도를 작성해보면, 금융회사의 보안 사고가 발생하면 임직원의 보안 인식이 강화되어 회사의 정보보호활동 강화를 발생시켜 보안 사고를 감소시키는 B1 루프에 의해 보안 사고의 발생 건수는 균형(Balancing)을 유지하게 된다. 또한, 보안 사고는 회사의 정보보호투자에 대한 압력을 증가시켜 정보보호투

자를 상승시키며 정보보호활동의 강화를 유발해 보안 사고를 감소시키는 B2 루프에 의해서도 균형을 유지한다.



[그림 2] 보안 사고에 따른 정보보호활동



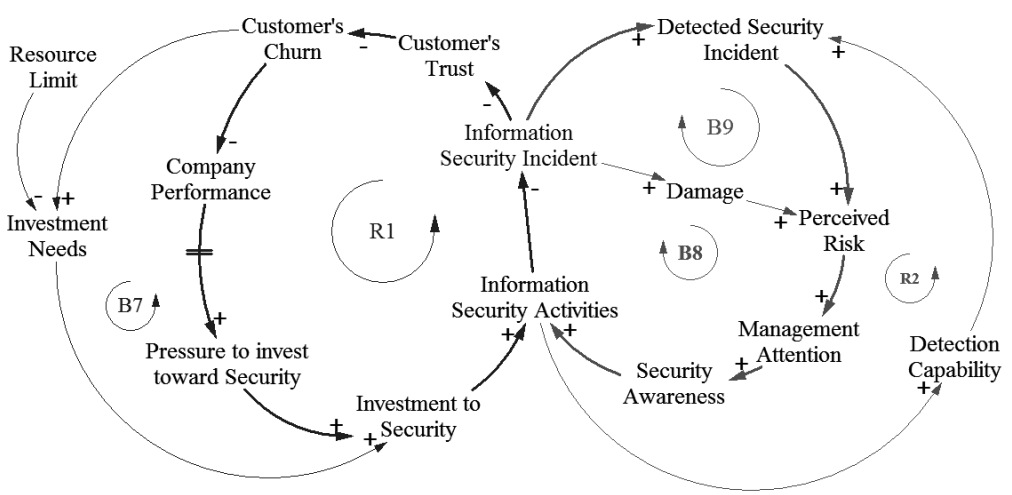
[그림 3] 보안활동주기에 따른 정보보호활동 모형

이러한 정보보호활동은 Straub 와 Welke(1998)의 보안활동주기에 따라서 수행되고 있으

며 서로 간에 피드백 구조로 되어 있다. 보안활동주기는 선형 관계로 해석되는 것이 아니라 시스템 사고에 의해 상호 피드백을 주고받는 피드백 구조로 인식되며 이를 기준으로 인과지도를 작성할 수 있다. 회사의 정보보호활동은 억제, 예방, 탐지, 교정 활동의 네 단계의 보안활동주기로 이루어지며, 교정, 탐지, 예방 활동은 억제 활동에 피드백을 준다. 결과적으로 세 가지의 활동은 보안 사고를 감소시키기 위한 핵심 활동인 억제활동에 영향을 주어 금융 보안 사고가 발생하는 것을 감소시킬 수 있는 피드백 구조로 되어 있다.

2. 보안 사고의 피해에 대한 시스템 사고

2014년 공표된 카드사 개인정보 대량 유출 사고를 살펴보면, 전자금융사고가 발생한 후, 해당 카드사는 고객으로부터의 신뢰를 잃고 다수의 고객이 이탈하는 현상이 발생하였으며, 보안 사고에 의한 피해는 회사의 성과에 영향을 주는 것으로 나타난다(윤일한 외, 2015). 보안 사고로 인하여 고객 이탈이 발생하면, 보안 투자의 필요성과 정당성을 높여주어 보안 투자를 높여주는 루프(B7)가 단기적으로 발생할 것이다. 그러나 금융회사의 투자 여력과 자원의 한계로 인한 “성장의 한계”(김도훈, 1999) 아키타입(Archetype)과 같이 계속된 투자 증가는 가져올 수 없을 것이다. 결국, 고객 이탈은 회사의 성과에 영향을 주고, 성과는 정보보호투자에 부담을 주어 장기적으로는 투자에 대한 감소를 발생시킬 것이다. 이러한 강화(Reinforcing) 루프(R1)에 의해 해당 회사의 보안 사고는 증가할 수 있을 것이다.



[그림 4] 금융 보안 사고에 대한 금융회사의 피해

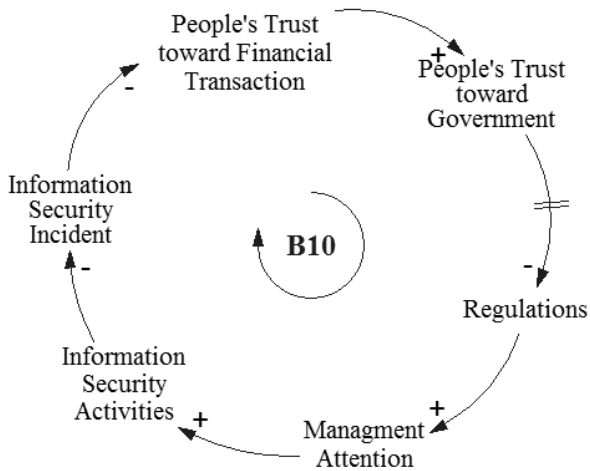
보안 사고가 발생한 회사가 입은 피해로 인하여 인지된 위험은 증가할 것이며, 이로 인한 경영진의 관심이 증가할 것이다. 경영진의 보안 사고에 대한 관심은 조직의 정보보안인식을 향상하고, 향상된 정보보안인식은 조직의 정보보안활동을 강화하여 보안 사고를 감소시키는 균형 루프(B8)가 그려진다. 또한, 강화된 정보보호활동은 조직의 탐지능력을 향상해 탐지되는 보안 사고의 건수를 증가시켜 인지된 위험의 상승을 나타내는 강화 루프(R2)에 의해 정보보안활동은 상승하게 된다. 이러한 상승은 보안 사고의 감소로 이어져 탐지되는 사고의 건수가 감소하게 되는 균형 루프(B9)에 의해서 설명된다(Anderson *et al.*, 2004).

결국, 금융회사에서 보안 사고가 발생하면, 경영진은 회사의 여력을 고려하여 보안 투자를 고려하고, 조직 내에는 정보보안을 강조하는 균형 루프가 존재하지만, 고객 이탈이 지속해서 발생할 경우에는 자원의 한계로 인하여 투자 부담이 증가하여 정보보호활동을 위축시켜 보안 사고를 증가시키게 되는 것이다.

3. 정부 규제에 대한 시스템 사고

심우현(2011)의 연구에 따르면, 보안 사고의 증가에 따른 정부의 전자금융거래법 제정은 금융회사의 정보보안 활동의 증가에 긍정적인 영향에 미치는 것을 실증하였으며 정보보호를 위한 보안책임 및 규제에 대한 법률이 정보보안이 지속해서 발전할 수 있는 방향이라고 주장하였다. 전자금융감독규정은 행정규칙으로써 금융회사에서 발생한 보안 사고를 금융회사의 경영실태 평가에 반영하고 있으며, 이로 인하여 경영진에게 보안 사고에 대한 관심을 촉진하고 있다. 유진호(2014)는 정보보호 거버넌스는 경영진의 정보보호 리더십이 정보보호 정책의 수립, 정보보호 조직과 인력의 구성, 정보보호 교육 훈련 및 인식, 보안 통제 활동, 모니터링 및 감사활동에 크게 영향을 준다고 주장하였다.

이를 확대하여 금융 보안 사고에 대한 정부의 규제가 미치는 영향에 대해 인과지도를 작성하여 설명할 수 있다. 보안 사고가 발생하면 국민의 금융거래에 대한 신뢰감이 저하되어 지각된 위험이 증가한다. 이러한 위험으로 인하여 정부에 대한 신뢰가 떨어지고 정부는 이에 대한 정책으로 정부의 규제를 강화하게 된다. 강화된 규제로 인하여 경영진의 보안책임에 대한 관심을 유발하고 금융회사 내의 정보보안활동을 강화하게 된다. 이에 강화된 정보보안활동으로 보안 사고를 감소시켜주는 B10 루프를 작성하였다.



[그림 5] 금융 보안 사고에 따른 정부 규제 강화

IV. 금융 규제에 대한 시스템다이내믹스 분석

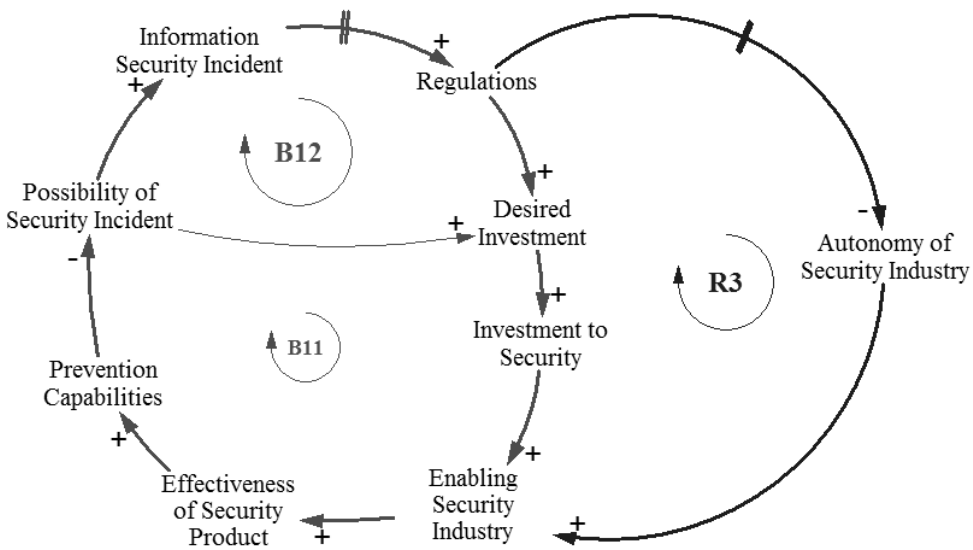
1. 금융 규제의 정책 저항 구조

금융 감독 당국의 지나친 개입은 과다한 규제비용을 발생시키지만, 보수적인 관점에서 보면 전자금융의 안전성을 위해 엄격하게 적용되어야 체계위험을 방지할 수 있다(이용수, 2006). 그러나 전자금융시장은 자유로운 경쟁 환경이 있어야 기술혁신을 촉진하여 금융 산업의 경쟁력과 금융소비자의 효용성을 증대시킬 수 있으며, 해외의 전자금융보안 부문은 국내와 달리 개별 금융회사에 의존하고 있다. 즉, 개별 금융회사가 자신의 상황에 맞게 보안기술을 채택하고 적용하고 있다(김종호, 2011). 또한, 정보보호를 위한 규제는 공정한 경쟁이 저해되어 산업의 발전을 저해할 수도 있는 것으로써, 더 큰 것을 잃게 될 수도 있다(한희원, 2009).

정보 기술과 대고객서비스 혁신의 발전 속도는 빠르게 진행되기 때문에 이에 대한 규제의 내용은 빠르게 낡은 내용으로 퇴화할 가능성이 크다. 정부의 규제는 개별 금융회사가 보안 사고를 방지하기 위해 자체적으로 보안대책에 대한 기준을 마련할 수 있도록 돕고 획일적인 규제를 지양하며 일정한 수준의 안전성 및 건전성을 확보하기 위한 최소한의 기준을 제시하여야 한다(김종호, 2011).

정보보호를 위한 정부의 규제에도 불구하고, 금융 보안 사고는 발생하고 있고 피해의 범

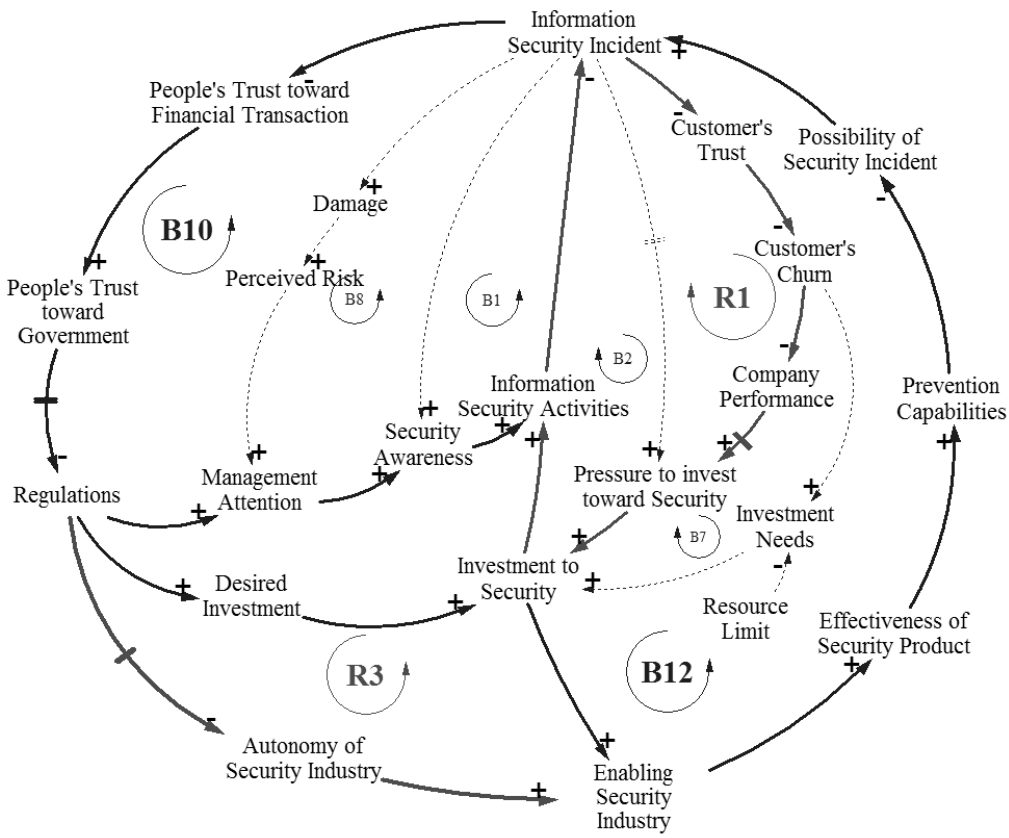
위는 더욱더 커지고 있다. 정부 규제와 보안 사고에 대한 인과지도를 통하여 정책 결정 시 인지의 한계로 고려되지 않은 루프가 있는지를 파악하기 위한 분석이 필요하다고 할 수 있으며, 전자금융거래와 관련된 정부의 지나치게 엄격한 규제의 강화에 따른 인과지도를 작성할 수 있다. 정부의 규제는 네거티브 규제와 포지티브 규제를 모두 포함하고 있지만, 기술적인 부문에서는 기술요건 자체를 구체적으로 제시하고 있어 상당한 부분이 포지티브 규제의 성격을 지니고 있다. 포지티브 규제를 과잉(Overshooting) 교정 활동으로 살펴볼 수 있고 이는 단기적으로는 보안 산업의 연구투자비를 증가시켜 보안 산업을 활성화하는 B12 루프로 균형을 유지하고 있지만, 장기적으로는 엄격하게 제시된 기술요건이 보안 산업의 자율성을 제한하는 과잉 규제로 인지되어 보안 산업의 경쟁력을 약화해 보안 산업의 자율성을 저해하는 R3 루프를 인지할 수 있다. 이는 단기적으로 효과적인 처방인 포지티브 규제가 장기적으로 예상하지 못한 결과를 초래한 "처방의 실패"(김도훈, 1999) 아키타입에 의해 설명될 수 있다.



[그림 6] 정부 규제 강화에 따른 보안 산업의 자율성 제약

지금까지의 인과지도를 기반으로 금융 보안 사고에 따른 금융회사의 정보보호활동, 금융회사의 피해, 정부의 규제 및 보안 산업 시장의 인과지도를 작성하여 통합 모형을 살펴보면, 균형 루프(B10, B12)와 강화 루프(R1, R3)로 이루어진 시스템 구조를 확인할 수 있다. 금융회사는 온 국민을 대상으로 금융서비스를 제공하고 있으며, 기술의 발전으로 사용이

쉽고 유용한 전자금융거래가 상당한 부분을 차지하고 있다. 국민에게 전자금융거래에 대한 안전성과 신뢰성을 확보하기 위해 전자금융거래법을 통한 규제에 대해 당시 일과 관련된 시각으로 접근하기보다는 제시된 모형을 기준으로 시스템 사고를 통하여 전체 구조를 이해할 수 있는 시각이 필요함을 알 수 있다.

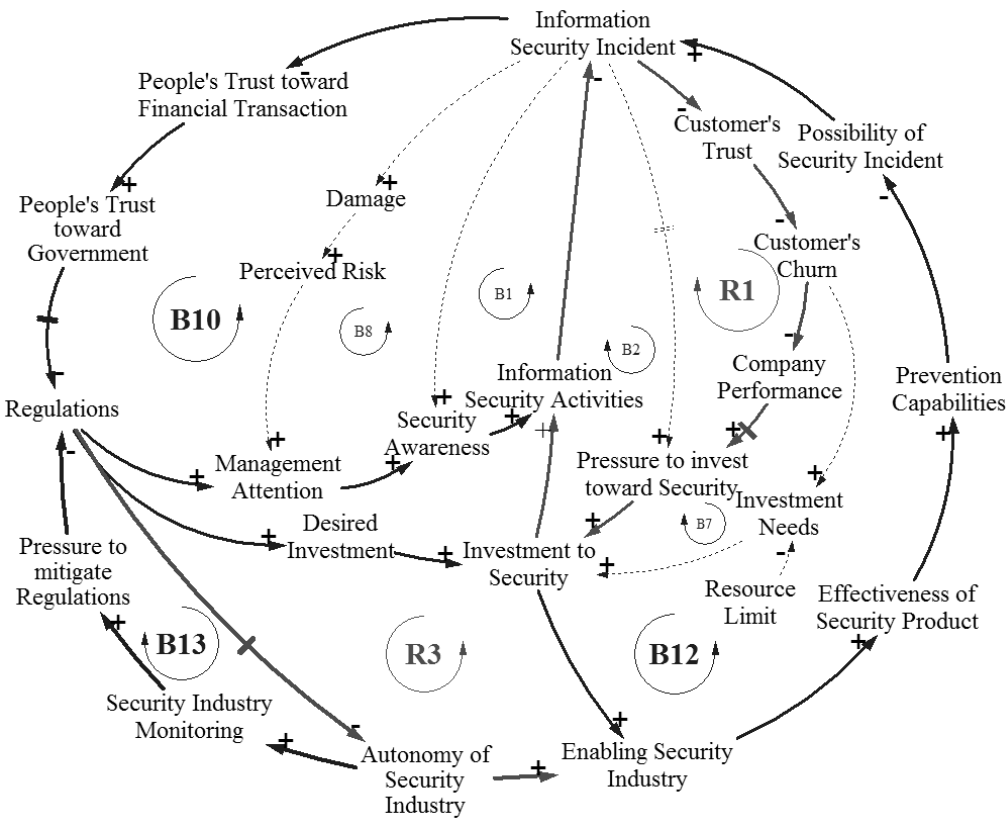


[그림 7] 보안 사고 대응의 통합 모형

2. 정책 저항 해소를 위한 시스템 구조 개선

정보보안은 기술적 보호조치에 대한 규제와 더불어 정책적인 대응전략이 상호보완적으로 연계되어야 보안 사고의 위험을 줄일 수 있으며(정익재, 2011), 정부의 규제는 보안 사고를 감소시키는 데 중요한 역할을 하게 된다. 하지만 금융 보안 사고에 대한 엄격한 정부 규제만으로는 당시 일과 관련된 성과만을 기대할 수 있으며, 보안 산업의 자율성을 위축하는 결과를 초래할 수 있다. 이에 대한 해결책으로 정부는 규제를 수립할 때, 보안에 대한

기술적인 규제에 대하여는 네거티브 규제 방식을 고려하여야 할 것이다. 네거티브 규제는 주어진 자율권적 권리를 더욱더 확장하여 보장하기에 규제 개혁 및 규제 완화 효과가 있으며, 규제 네거티브화로 인해 투자유치 및 고용창출 등의 효과가 더 크게 나타날 것으로 판단된다(최승필, 2011; 김태윤 외, 2015). 또한, 네거티브 규제 방식은 보안 산업의 자율성을 증대시키고, 당국의 규제 비용을 줄이며, 불필요하거나 이중적인 규제들을 방지하는 이점이 있어 적극적인 채택을 고려하여야 할 것이다(황태희, 2011).



[그림 8] 보안 산업 모니터링을 통한 보안 산업의 자율성 보장 모형

정부의 포지티브 규제를 통한 기술요건제약이 보안 산업의 자율성에 미치는 악영향을 감소시켜 전체적인 균형을 유지하기 위해 보안 산업의 자율성에 대한 모니터링을 강화하여 자율성에 부의 영향을 주는 포지티브 규제는 제거하고 정의 영향을 주는 네거티브 규제를 적절하게 사용하여 전략적인 지렛대 효과를 통해 보안 산업의 자율성을 보장하고 경쟁력을 증대시켜야 한다. 궁극적으로 금융 보안 사고를 방지하여 법률의 제정이유에서 언급한 전

자금융거래의 이용자들에게 안전성과 신뢰성을 보장해 줄 수 있을 것이다. 따라서 위에서 인지의 한계로 강조되지 못했던 루프인 R3에 대한 균형을 유지하기 위해 보안 산업의 자율성에 대한 모니터링 활동을 추가하여 B13 루프를 이용한 인과지도를 작성할 수 있다.

개선된 시스템 구조에서는 균형 루프(B10, B12, B13)와 강화 루프(R1, R3)가 시스템 전체의 행태를 바람직한 규제의 완화를 통하여 안정적인 모습으로 유지할 것이다.

V. 결 론

금융회사의 보안 사고는 이용자들에게 전자금융거래에 대한 안전성과 신뢰성을 감소시켜 금융거래에 드는 사회적 비용을 증가시키고 있다. 정부는 금융 보안 사고가 발생하면 법률과 행정규칙을 강화하는 방향으로 개정하여 대응하고 있으며, 이러한 대응은 단기적으로는 효과가 있지만, 장기적으로는 보안 산업의 자율성을 제약하는 포지티브 규제가 많은 부분을 차지하고 있다. 시스템 사고를 통하여 포지티브 규제를 통한 엄격한 기술제약을 강화하면, 보안 산업의 자율성을 제한하여 보안 산업의 성장을 가로막는 인지되지 못해 강조되지 않았던 인과루프가 있음을 알게 되었다.

본 연구의 시사점으로는 첫째, 정보보호활동에 대한 보안활동주기 모형에 대하여 시스템 사고를 통해 전통적인 선형 관계에서 상호 피드백을 주고받는 피드백 루프 구조로 인식하고 인과지도로 설명한 점이다. 이러한 인과지도를 통해 억제, 예방, 방지 및 교정활동이 함께 피드백 구조 모형을 이루어야 하며, 정보보호활동은 하나의 활동에 의해 금융 보안 사고가 감소되어지는 것이 아니라 네 가지 활동이 상호 피드백 구조를 이루고 있음을 이해하고 실무에서 정보보호활동을 설계할 때 고려하여야 할 것이다.

둘째, 금융 보안 사고에 대한 방지를 위해 단선적인 사고를 통한 정책의 수립은 단기적으로는 보안 산업에 영향이 없는 것으로 보이지만, 장기적으로는 보안 산업의 자율성에 영향을 주고 국내 보안 산업의 경쟁력을 하락시키는 결과를 가져올 수 있다는 시스템 구조를 보여준 점이다. 인과지도에서 나타났듯이 정부규제에 대한 시간 지연효과로 인해 보안 산업의 자율성을 저해하는 것을 이해하지 못해 정책결정자가 단기적인 사고로 정책을 너무 성급하게 결정하여 역효과가 나올 수 있다는 것을 이해할 수 있다.

셋째, 포지티브 규제로 인한 보안 산업의 자율권 저해를 억제하기 위해 보안 산업의 모니터링을 통하여 적절한 네거티브 규제를 고려하는 규제 개혁이 전체 시스템 구조를 안정적인 모습으로 발전시킬 수 있다는 점이다. 네거티브 규제는 행정 절차를 간소화시키고, 행정 부담을 감소시킬 수 있어(황태희, 2011), 네거티브 규제를 통한 규제 개혁이 국가의 정

책을 지지하는 것이다. 금융 규제 당국은 보안 산업의 모니터링을 통한 규제의 현실에 대한 이해를 바탕으로 시스템 구조를 개선할 있을 것이다.

최근 정부는 쟁점이 되었던 공인인증서의 의무화를 폐지하여 인증수단에 대한 자율성을 보장하였으며, 단말기 접근 제어에 대한 일부 엄격한 내용을 삭제하였다. 또한, 보안성 심의제도를 폐지하고 망분리 적용이 업무상 불가피한 경우에 대한 세부기준을 마련하여 금융회사 스스로 위험평가를 실시 후 대체통제를 점검하여 예외를 허용하는 방안을 마련하였다. 이는 경험적으로 수집된 데이터를 이해하여 기술적인 제약으로 인한 보안 산업의 제약을 이해하고 규제를 축소하는 움직임으로 판단된다. 하지만 이러한 대응은 부분적인 성과만을 바랄 수 있을 뿐, 시스템 사고를 통한 이해를 기반으로 전반적인 규제의 개정을 수행하여 자율성을 강조하는 정책의 수립이 필요하다고 할 수 있다. 금융 보안 사고를 방지하기 위해 수립된 정부의 규제는 당시 일과 관련된 성과만을 바라보고 수립하여서는 아니 되며 장기적인 관점의 시각을 고려하여야 할 것이다. 또한, 보안 산업의 자율성에 악영향을 미치는 규제의 내용을 파악하기 위한 모니터링 활동을 강화하여 보안 산업을 육성하여야 할 것이다. 정책 결정 시 인지하지 못하여 시스템 구조의 문제를 파악하지 못하는 것은 금융 규제뿐만 아니라, 일반적인 행정 규제의 결정에서도 같은 문제를 가지고 있을 수 있으며 규제의 완화에 대한 모니터링을 확대하고 강조하여야 할 것이다.

그러나 본 논문에서는 정부의 규제 형태에 대해 기술적인 제약이 엄격한 포지티브 규제와 네거티브 규제를 적절하게 사용하여야 함을 주장하지만, 얼마나 많은 부분의 규제를 어떻게 개정할 것인가에 대하여는 언급하지 않았다. 또한, 시스템다이내믹스의 연구는 컴퓨터 시뮬레이션을 수행하여 시뮬레이션 모형의 특성을 체계적으로 분석하는 방법론임에도 구조 분석을 통한 인과지도만을 작성하였다. 향후 정량적인 모형으로 발전시킬 때에 측정 가능한 변수로 변환이 가능한 것이 얼마나 될 것인지를 생각할 때 정량 모형으로의 발전 가능성은 한계가 있을 것으로 판단되지만, 정량 변수를 포함하는 인과지도로 발전시켜 시뮬레이션 모형을 작성하여 정량 모형으로 시뮬레이션 분석한 결과를 통하여 재해석되어 질 수 있을 것으로 생각한다.

【참고문헌】

감사원. (2014a).「감사결과보고서-금융권 정보보호 및 사이버안전 관리・감독 실태」

감사원. (2014b).「감사결과보고서-금융회사 개인정보 유출 관련 검사・감독 실태」

김도훈・문태훈・김동환. (1999).「시스템다이내믹스」. 대영문화사.

김동환. (2000). "인과지도의 시뮬레이션 방법론: NUMBER".「시스템다이내믹스」제1권 제2호, pp.91-111.

김상현・송영미. (2012). "보안관리 인지 요인이 조직의 정보시스템 보안위험관리에 대한 인식 및 개발의지에 미치는 영향".「Information System Review」제14권 제2호, pp.21-46.

김인석. (2006). "電子金融과 정보보호에 관한 연구".「우정정보」제2006권 제3호, pp.39-58.

김종호. (2011). "전자금융 감독제도의 강화를 통한 금융거래 위험의 관리방안".「성균관법학」제23권 제1호, pp.233-273.

김태윤・이수아. (2015). "규제네거티브화 효과의 시론적 평가와 측정-새만금지영 투자 및 고용창출을 중심으로".「규제연구」제24권 제1호, pp.3-48.

심우현. (2011). "보안책임과 규제가 기업의 보안활동에 미치는 영향 분석".「한국전자거래학회지」제16권 제4호, pp.53-73.

윤일한・권순동. (2015). "정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구".「Information System Review」제17권 제1호, pp.114-169.

이수미・성재모. (2011). "국내 전자금융 현황 및 보안위협 분류".「정보보호학회지」제21권 제7호, pp.53-61.

이용수. (2006). "전자금융거래법 시행에 따른 전자금융의 과제".「우정정보」제2006권 제4호 pp.45-63.

유진호. (2014). "최고경영층의 정보보호 리더십에 따른 정보보호 통제활동의 차이 분석".「한국전자거래학회지」제19권 제1호, pp.63-78.

장남정・김민경・양고수. (2013). "시스템다이내믹스 기법을 이용한 온실가스 감축정책 평가".「시스템다이내믹스」제14권 제1호, pp.55-68.

전재호. (2003). "정보보호 산업육성 정책의 상대적 효과 분석".「시스템다이내믹스」제4권 제2호, pp.5-44.

정우진・신유형・이상용. (2012). "금융회사의 고객정보보호에 대한 내부직원의 태도 연구".「Asia Pacific Journal of Information Systems」제22권 제1호, pp.53-77.

정익재. (2011). "정보사회의 불확실성 관리를 위한 정책 논리와 대응: 정보보안 사고의 유형화

와 대응책". 「국가정책연구」 제25권 제4호, pp.55-77.

최승필. (2011). "규제완화에 대한 법적 고찰-인・허가 및 신고, 등록제도와 네거티브 규제를 중심으로". 「공법학연구」 제12권 제1호, pp.317-347.

한희원. (2009). "연구논문(硏究論文): 정보보안(保安)의 규제 혁신에 대한 고찰 - 산업기술의 유출방지 및 보호에 관한 법률을 중심으로". 「법조」 제58권 제4호, pp.258-301.

황태희. (2011). "네거티브 규제와 규제 방식의 개선". 「성산법학」 제10호, pp.81-102.

Andersen, D., D. M. Cappelli, J. J. Gonzalez, M. Mojtahedzadeh, A. P. Moore, E. Rich, J. M. Sarriegui, T. J. Shimeall, J. M. Stanton, E. Weaver, and A. Zagonel. (2004). "Preliminary system dynamics maps of the insider cyber-threat problem". *Proceedings of the 22nd International Conference of the System dynamics Society*.

Foroughi, F. (2008). "The application of system dynamics for managing information security insider-threats of IT organization". *Lecture Notes in Engineering and Computer Science*, vol.2170, no.1, pp.528-531.

Gefen, D., V. S. Rao, and N. Tractinsky. (2003). "The conceptualization of trust, risk and their electronic commerce: the need for clarifications". *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003.*

Straub, D. W., and R. J. Welke. (1998). "Coping With Systems Risk: Security Planning Models for Management Decision Making". *MIS Quarterly*, vol.22, no.4, pp.441-469.

Theoharidou, M., S. Kokolakis, M. Karyda, and E. Kiountouzis. (2005). "The insider threat to information systems and the effectiveness of ISO17799". *Computers and Security*, vol.24, no.6, pp.472-484.

http://www.bai.go.kr, 10 Jul., 2015.

http://www.laws.go.kr, 10 Jul., 2015.

http://www.fki.or.kr/FkiAct/Promotion/Report/, 10 Jul., 2015.

▶ 접수일 : 2015. 8. 30. / 수정일 : 2015. 11. 18. / 게재확정일 : 2015. 11. 23.