Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.881

전자금융거래 시 보안 통제 사항의 개선 연구

이 강 신[†‡]
김·장 법률사무소

A Study on Improving Security Controls in the Electronic Financial Transaction

Gangshin Lee[†‡]
KIM & CHANG

요 약

금융분야에서 개인신용정보 유출사고로 인하여 금융당국은 전자금융거래법등에 통제사항을 강화하여 왔다. 이에 따라 정보보호 수준이 한 단계 향상이 되었지만 추가로 개선할 사항이 더 없는지 연구해볼 필요가 있게 되었다. 본 논문은 정보보호 분야에서 통제사항을 총 망라하는 정보보호관리체계인증의 통제사항과 비교하여 추가로 개선할 통제사항을 전문가들의 의견을 모아 일정 중요도 이상이 되는 19개를 도출하였다.

ABSTRACT

Financial Authorities have added security controls to the Electronic Financial Transaction Act and the Supervisory Regulation according to the recent frequent personal credit information leakages. Accordingly, the security level has been upgraded. But it is necessary to study more security controls to add. This paper deduces 19 security controls over the mean value to be added to the financial area receiving 15 security consultant's help.

Keywords: Financial, Security control, Act, Personal Credit Information

I. 서 론

2005년 5만여개의 리니지 게임 계정을 만들어 판매한 명의도용 사건은 국내 개인정보 유출의 심각성을 알려준 사실상 최초의 사건이었다. 이후 2008년 옥션 해킹, GS칼텍스의 내부자에 의해 개인정보가 유출되면서 본격적으로 크고 작은 유출사건들이 줄을 이어 발생하였다.

특히 금융권의 경우 2009년 하나캐피탈 해킹, 2011년 한화손해보험의 해킹을 시작으로 최근 은행권과 카드사들의 개인신용정보 유출로 사회적 불안이 극에 달하고 있다. 2014년도 발생한 카드사의 개인정보 유출 규모는 1억 4백만건으로 우리나라 역사상 가장 큰 규모로 기록되고 있으며 전 세계적으로도 유출규모상 Fig.1.에서 알 수 있듯이 9위[1]로 기록된 매우 큰 사건이다.

이와 같이 사회적으로 큰 이슈가 된 개인정보 유출에 대하여 전 국민의 관심 속에 금융기관에서는 2011년 4월 농협사건 이후 2011년 10월에 전자금융감독규정[2]에 총 임직원 수 대비 정보기술부분 인력을 5% 이상, 정보기술 부분 인력 대비 정보보호 인력을 5% 이상, 정보기술부문 예산 대비 정보보호 예산을 7% 이상 책정하도록 하는 5·5·7제를 도입하는 등 보호 의무를 대폭 강화하였고, 2013년도 방송을 포함한 금융기관에 대한 3.20 사이버테러로 2013년 5월에 전자금융거래법상 보호조치의 근

접수일(2015년 3월 3일), 수정일(1차: 2015년 5월 26일, 2차: 2015년 6월 23일), 게재확정일(2015년 6월 23일)
† 주저자, gangshin.lee@kimchang.com
‡ 교신저자, gangshin.lee@kimchang.com(Corresponding author)

Largest Incidents

RECORDS	DATE	ORGANIZATIONS
220,000,000	2014-08-22	Unknown Organization
152,000,000	2013-10-03	Adobe Systems, Inc.
150,000,000	2012-03-17	Shanghai Roadway D&B Marketing Services Co. Ltd
145,000,000	2014-05-21	eBay Inc.
140,000,000	2013-06-08	Unknown Organization
130,000,000	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank, North Middlesex Savings Bank, Golden Chick
110,000,000	2013-12-18	Target Brands, Inc., Fazio Mechanical Services, Inc.
109,000,000	2014-09-02	Home Depot, Unknown Organization
104,000,000	2014-01-20	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card
94,000,000	2007-01-17	TJX Companies Inc.

Fig. 1. Largest Incident worldwide (2015.3.3)

거였던 제21조 안전성의 확보의무에 정보보호최고책임자의 지정, 전자금융기반시설의 취약점 분석·평가, 전자적 침해행위의 금지, 침해사고의 통지 및 대응조항을 신설하게 되었다. 같은 해 6.25 사이버테러가 추가로 발생되면서 개정된 법과 추가 이행이 필요한 사항을 전자금융감독규정에 반영하여 2013년 12월 3일에 개정 및 시행하게 되었다.

또한 2013년 12월 은행권의 개인정보 유출과 2014년 1월 카드사 개인정보 유출 등 사회적으로 절정에 달한 금융권의 개인신용정보의 유출로 전자금융거래법은 개정되어 2015.4.6.일 시행하고, 신용정보의이용및보호등에관한법률도 개정안이 2015.2.16.일 국회 본회의를 통과하였다.

본 논문에서는 2015년 2월말 기준으로 전자금융거래법 관련 기존 내부 통제사항과 새롭게 추가된 통제사항들이 한국인터넷진흥원에서 운영하고 있는 정보보호관리체계인증(ISMS)을 위한 통제사항과 비교하였을 경우 추가 반영을 고려할 수 있는 보호조치에 대하여 고찰하였다.

II. 전자금융거래법과 ISMS의 비교 분석

2.1 전자금융거래법

전자금융거래법, 시행령, 금융위원회의 고시인 전자금융감독규정과 금융감독원에서 운영하는 시행세칙이 있다(이하, "전자금융거래법등"). 전자금융거래법은 2007년 1월 제정 및 시행된 시점에는 가장 기본적인 사항을 내용으로 하는 제21조인 안전성의 확보조치 의무만이 있었으나 현재는 6개 조항으로 확대되었다[3].

제21조의2는 금융회사 또는 전자금융업자는 정보보호최고책임자를 지정하도록 하며 총 자산이 2조원 이상이고 상시 종업원 수가 300명 이상인 경우는 임원급으로 지정하도록 하였다. 그리고 정보보호책임자의 역할과 책임을 정의하였다.

21조의3은 지정하는 전자금융기반시설에 대해서는 매년 취약점 분석평가를 실시하여 그 결과를 금융위원회에 보고하도록 명시하였다. 이는 취약점 분석·평가를 매년 실시하게 함으로써 새롭게 나타나는 취약성에 대해서 지속적으로 점검하도록 함으로써 정보보호는 지속성을 가져야 한다는 의미를 부여하고 있다.

21조의4는 누구든지 전자금융기반시설에 접근권한이 없음에도 불구하고 접근할 경우 처벌할 수 있도록 명시하였다. 이를 위반하게 될 경우 가장 무거운 벌칙인 7년 이하의 징역 또는 5천만원 이하의 벌금을 부과할 수 있다.

21조의5는 개인신용정보 유출 등 침해사고가 발생될 경우 금융위원회에 지체 없이 알리고 스스로는 원인을 분석하여 피해확산 방지 노력을 하도록 했다. 과거에는 비록 관행적으로 보고는 하였으나 명시적인 근거가 없었다. 이제는 명시적인 근거에 따라 금융위원회에 미 신고 시에는 1천만 원 이하의 과태료를 부과할 수 있도록 책임성을 강화하였다는데 의미가 있다.

21조의6은 21조의5에 따른 침해사고 신고를 받은 금융위원회는 대응을 위해 법률적인 근거를 마련함으로써 신속하고 명확하게 대응을 지휘할 수 있도록 하는데 있다.

2011년, 2013년, 2015년 개정된 전자금융감독규정의 내용도 대폭적으로 보강이 되었다. 특히 개정 시 보완된 내용을 보면 보안규정을 위반한 경우 내부 임직원을 처벌할 수 있는 절차를 마련, 정보보호위원회를 운영하여 심의 및 의결한 사항을 CEO에게 보고, 금융전산망의 외부망과 분리 및 차단, 내부 통신망에서 파일 배포 시 반드시 무결성 검증, 침해사고 대응 및 복구훈련계획을 수립하여 시행하는 등이다.

이처럼 몇 차례의 사고를 계기로 전자금융 환경에서 내부통제를 강화함으로써 사이버 공격 및 사고로부터 위험성을 대폭 줄인 상태인데도 불구하고 추가로 고려할 사항이 없는지에 대하여 ISO 표준과 유사한 국내의 ISMS 통제사항과 비교하는 것은 의미가 있다고 하겠다.

2.2 ISMS

2001년 7월에 정보통신망이용촉진및정보보호등에 관한법률 제47조에 기업등이 정보보호 관련 종합적

및 체계적으로 추진하도록 제3자가 심사 후 인증서를 발급하는 정보보호관리체계인증 근거를 마련하였다.

이후 약 14년이 지난 지금은 400여개의 기업이 인증을 받음으로써 정보보호의 수준을 한 단계 끌어 올렸다는 평가를 받고 있다. 수 차례 기준 개정을 통하여 2013년 2월에 개정된 정보보호 관리체계 인증 등에 관한 고시[4]의 통제사항 수는 관리과정 12개와 정보보호대책 92개 등 총 104개로 구성되어 있다.

동 통제사항 중 관리과정에는 정보보호 정책 수립 및 범위 설정, 경영진 책임 및 조직 구성, 위험관리, 정보보호대책 구현, 사후관리 등 5개 영역으로 구성되어 있다. 정보보호대책에서는 정보보호정책, 정보보호조직, 외부자 보안, 정보자산 분류, 정보보호 교육, 인적보안, 물리적 보안, 시스템 보안, 암호통제, 접근통제, 운영보안, 침해사고 관리, IT재해복구 등 13개 분야로 구성되어 있다.

동 ISMS의 통제사항은 국제표준인 ISO/IEC 27001과 유사하게 국내 실정에 적합하도록 설계한 것으로 정보보호 전반을 커버할 수 있는 정보보호 대책이기 때문에 이를 기준으로 국내의 입법화된 전자금융거래법등의 기준과 비교하는 것은 개선을 위한 기회가 될 수 있다는 점에서 의미가 있다.

2.3 ISMS 통제사항에 대한 전자금융거래법등의 통제사항 근거

Table 1, 2는 ISMS의 104개 통제항목에 대하여 전자금융거래법등에서 제시하고 있는 내부 통제사항의 근거를 표시한 것이다.

시행령은 제11조의2의 ②를 제외하고는 법에서 위임한 활동사항에 대한 방법은 제시하고 있으나 활동사항은 법과 동일하고, 전자금융감독규정시행세칙도 제12조의 사고보고 이외에는 전자금융감독규정의 활동사항에 대한 방법은 제시하고 있으나 활동사항은 역시 동일하기 때문에 상기 2개 사항 이외에는 별도 표기하지 않았다. 그러면 ISMS 체계에 따라 정보보호관리과정과 정보보호대책으로 나누어 살펴본다.

정보보호관리과정인 Table 1.에서 정보보호정책을 수립하는 사항과 구현된 대책을 직원들이 인지하도록 공유 및 교육하는 내용이 전자금융거래법등에 명시되어 있지 않다. 또한 프로세스 관점에서 Plan, Do, Check, Act 사이클을 운용할 수 있는 프레임워크도 명시되지 않았다.

Table 1. Requirements for Security Management Process of ISMS

Number	Management process	Control number	Detailed management process	Electronic Financial Transaction Act related
1	Establish security policy and scope	1.1	Security policy	
		1.2	Scope	Act, article 3
2	Management responsibilities and organization	2.1	Management responsibilities	Reg, article 8-2
		2.2	Security organization and resource allocation	Reg, article 8
3	Risk management	3.1	Establish risk management methodology and plan	Act, article 21-3, ①
		3.2	Risk identification and evaluation	Act, article 21-3, ①
		3.3	Select security controls and establish implementation plan	Act, article 21, ④ Enforcement decree, article 11-2, ②
4	Implement security controls	4.1	Implement security controls effectively	Act, article 21-3, ③, ④
		4.2	Internal sharing and training	
5	Monitor, review, maintain and improve ISMS	5.1	Review compliance	Reg, article 8, ①, 4
		5.2	Management the maintaining ISMS	
		5.3	Internal audit	Reg, article 22, article 58, article 59

정보보호대책의 경우는 Table 2.에서 비교되는 바와 같이 분야별로 정책 수립, 외부자 보안, 정보자산의 분류, 시설별 차별화되는 접근통제, 스마트워크 보안, 침해사고 발생 시 사후관리 등이 명시되지 않은 것으로 나타났다.

Table 2. Security Controls of ISMS

Contro clause number	Control clause	Control objective number	Control objective	Contro number	Controls	Electronic Financial Transaction Act related
1	Security policy	1.1	Approve and publish Ssecurity policy	1.1.1	Approve security policy	
				1.1.2	Publish security policy	
		1.2	Security policy architecture	1.2.1	Consistency of high level policy	
				1.2.2	Document security policy implementation	
		1.3	Maintain security policy	1.3.1	Review security policy	
				1.3.2	Manage security policy	
2	Organising information security	2.1	Organization	2.1.1	Designate Chief of Security Officer	Act, article 21-2, ①, ②
				2.1.2	Organize workers	Reg, article 8, ①, 1
				2.1.3	Security	Reg, article

					committee	8-2, ①
		2.2	Roles and responsibilities	2.2.1	Roles and responsibilities	Act article 21-2, ③, ④
3	Outsourced human resource security	3.1	Define security requirements	3.1.1	Security requirements for outsources human resources	Reg, article 8, ①, 2
		3.2	Implement outsourced human resources	3.2.1	Implement and maintain outsourced human resources	
				3.2.2	outsourced human contract timeout	
4	Asset management	4.1	Identify Information asset and allocate responsibility	4.1.1	Identify information asset	
				4.1.2	Allocate responsibility for information asset	
		4.2	Classify information asset	4.2.1	Classify information asset	
5	Security training	5.1	Establish training program	5.1.1	Training plan	Reg, article 8, ①, 3 Reg, article 19-2
				5.1.2	Trainee	Reg, article 8, ①, 3 Reg, article 19-2
				5.1.3	Training contents and method	Reg, article 8, ①, 3 Reg, article 19-2
		5.2	Training and evaluating	5.2.1	Training and evaluating	Reg, article 8, ①, 3 Reg, article 19-2
6	Human Resource security	6.1	Security responsibility	6.1.1	Designate and surveilance main worker	Reg, article 13
				6.1.2	Separation of duty	Reg, article 26
				6.1.3	Confidentialty agreement	
		6.2	Personnel policy	6.2.1	Retirement and duty change	Reg, article 13, ①, 14
				6.2.2	Reward and punishment regulation	Reg, article 8, ①, 5
7	Physical security	7.1	Physical security area	7.1.1	Designate security area	Reg, article 9, 6 / article 10
				7.1.2	Security facility	Reg, article 9, 5 / article 10
				7.1.3	Work in security area	Reg, article 9, 10
				7.1.4	Access control	Reg, article 9, 1
				7.1.5	Mobile device security	Reg, article 11, 12
		7.2	System security	7.2.1	Cable security	
				7.2.2	System setup	
		7.3	Office security	7.3.1	Personal environment security	Reg, article 12
				7.3.2	Sharing environment	

					security	
8	Information systems acquisition and development	8.1	System analysis and design	8.1.1	Security requirement definition	Reg, article 12, 4
				8.1.2	Authentication and Encryption	Reg, article 20, 4
				8.1.3	Secure logging	Reg, article 20, 4
				8.1.4	Access control	Reg, article 20, 4
		8.2	System implement and transfer	8.2.1	Implement and test	
				8.2.2	Separation of development 및 operation	Reg, article 26
				8.2.3	Transfer operation environment	
				8.2.4	Test data security	Reg, article 13, ①, 10
				8.2.5	Source code security	Reg, article 29
		8.3	Outsourced development security	8.3.1	Outsourced development security	Reg, article 60
9	Encryption	9.1	Encryption policy	9.1.1	Establish encryption policy	
		9.2	Encryption key management	9.2.1	Create and use encryption key	Reg, article 31
10	Access control	10.1	Access control policy	10.1.1	Establish access control policy	
		10.2	Access right management	10.2.1	User registration and access right provision	Reg, article 13, ①, 2, 4
				10.2.2	Administration and special right management	Reg, article 13,, ②
				10.2.3	Review access right	Reg, article 13,, ①, 14
		10.3	User authentication and identification	10.3.1	User authentication	Reg, article 13,, ①, 12
				10.3.2	User Identification	Reg, article 13,, ①, 1, ②
				10.3.3	Internal user password management	Reg, article 13,, ① / article 32
				10.3.4	User password management	Reg, article 33
		10.4	Access control area	10.4.1	Network access	Reg, article 15, ①, 3, 5 / article 18
				10.4.2	Server access	
				10.4.3	Application program access	
				10.4.4	Database access	
				10.4.5	Mobile device access	
				10.4.6	Internet access	Reg, article 15, ①, 3
11	Maintenance	11.1	Maintenance procedure and change management	11.1.1	Establish maintenance procedure	Reg, article 14, 1
				11.1.2	change management	Reg, article 14, 2
		11.2	System and service operation	11.2.1	Information system acceptance	

			security	11.2.2	Security system operation	Reg, article 15, ①, 1
				11.2.3	Performance and capability management	Reg, article 14, 4
				11.2.4	Fault management	Reg, article 14, 3, 5
				11.2.5	Remote operation management	Reg, article 12
				11.2.6	Smartwork security	
				11.2.7	Wireless network security	Reg, article 15, ⑥
				11.2.8	Webserver security	Reg, article 17
				11.2.9	Backup and Recovery	Reg, article 13, ①, 8, 9
				11.2.10	Vulnerability assessment	Act, article 21-3, ①
		11.3	E-commerce and e-transference security	11.3.1	E-commerce security	Reg, article 37
				11.3.2	Establish information tranference policy and contract	
		11.4	Media security	11.4.1	Storage management	
				11.4.2	Potable storage management	Reg, article 13, ①, 7
		11.5	Malicious code	11.5.1	Malicious code control	Reg, article 16
				11.5.2	Patch management	Reg, article 14, 7 / article 15, ①, 2
		11.6	Logging and monitoring	11.6.1	Time synchronization	
				11.6.2	Logging and preservation	Reg, article 13, ①, 11, ③
				11.6.3	access and use monitoring	Reg, article 13, ⑤
				11.6.4	Intrusion monitoring	Reg, article 14, 4, 10
12	Information security incident management	12.1	Incient response procedure and system	12.1.1	Establish Incient response procedure	
				12.1.2	Implement incident response	Reg, article 37-4
		12.2	Response and recovery	12.2.1	Incident response training	Reg, article 37-4
				12.2.2	Incient response report	Act, article 21-5, ① Reg, article 15, ④ / article 73 Operation rule, article 12
				12.2.3	Incident response and recovery	Act, article 21-5 ②
		12.3	Follow up	12.3.1	Incident analysis and sharing	
				12.3.2	Prevent re-accident	
13	Business continuity	13.1	Implement BCP	13.1.1	Implement IT disaster recovery system	Reg, article 23
		management	13.2	Implement Control	13.2.1	Disaster recovery planning	Reg, article 23
					13.2.2	Test and maintain	Reg, article 24

전자금융거래법등에 상기 Table 1, 2에서 명시되지 않은 세부관리과정과 통제사항은 통 33개가 도출이 되었는데 이는 법률과의 상세 수준이 상이할 수 있고 실제 실행되고 있을 수 있으나 본 연구에서는 필요상 단순 비교함을 전제로한다.

그러면 정보보호도 비용효과적으로 적용하여야 한다는 관점에서 어떤 통제사항을 우선적으로 적용하여야 하는지 판단이 필요하다. 이러한 판단을 위하여 다음 장에서는 실험 방법을 제시하고 이에 대한 검증을 하고자 한다.

III. 전자금융거래법등에서 보완이 필요한 통제사항의 도출 방법 설계

ISMS 104개 통제사항은 세분류의 가장 작은 단위이기 때문에 중요도 측면에서는 가중치가 동일하다는 전제하에 정보보호전문가 그룹에 의하여 중요도를 기록하게 하여 전체의 평균 중요도를 산정한다. 그리고 전자금융거래법등에서 미 반영된 33개의 통제사항 중 평균 중요도보다 높은 중요도를 가지는 통제사항을 도출한다.

먼저 정보보호 전문가 17명을 대상으로 ISMS 104개 세부 통제사항에 대하여 중요도를 기록하도록 하였고 이 중 일부 작성되지 않은 2부를 제외하고 15부를 분석에 활용하였다. 동 설문에 참여한 정보보호 전문가 15명은 컨설턴트가 10명, 기업 보안관리자가 5명이었으며, 경력으로는 5년 이상 10년 미만이 8명, 10년 이상 15년 미만이 5명, 15년 이상이 2명이었다.

그리고 전자금융거래법등에 존재하는 내용이 미리

Table 3. The characteristics of sample

Division	Detailed Division	Respondents
Security Role	Consultant	10
	Corporate Security Manager	5
Security Career	5 ≤ years < 10	8
	10 ≤ years < 15	5
	15 ≤ years	2

설문자들에게 공개될 경우 전자거래의 중요성 때문에 편향적으로 평가할 가능성이 있어서 이를 배제하기 위하여 ISMS 통제항목만을 가지고 중요도에 대하여 평가하도록 하였다.

평가 점수는 0~10점으로 하고 소수점 1자리까지 적용하도록 하였다. 자칫 0~100점 단위로 할 경우 정보보호는 완벽할 수 없다는 점 때문에 100점이라는 심리적 부담감이 있을 수 있다는 판단에 따라 10점 만점 방식을 택하였다.

일정수준 이상이 되는 점수의 기준은 설문조사 결과 104개 각각의 항목별로 15명의 정보보호전문가가 부여한 점수를 평균한 값을 기록하고 기록이 완료된 104개에 대한 평균값을 구하였다. 따라서 평균점수인 기준점수를 $\mathbb{Z}$라고 할 경우

$$\mathbb{Z} = \sum_{j=1}^{104} [\sum_{i=1}^{15} a_{ij}/15]/104,$$

where $1 \le i \le 15,\ 1 \le j \le 104,\ i,\ j \in N$

이다. 따라서 ISMS에는 존재하나 전자금융거래법등에서는 존재하지 않는 33개 통제사항 중 기준점수 $\mathbb{Z}$ 이상은 채택하고 미만은 기각한다.

IV. 통제사항에 대한 중요도 산정 결과

104개에 대한 15명의 정보보호 전문가로부터 구한 기준점수는 8.911점이 나왔다.

ISMS 통제사항에 전자금융거래법등에 포함되지 않은 33개 항목 중 기준점수 이상인 통제사항은 Table 4, Table 5와 같이 모두 19개인 것으로 나타났다.

전자금융거래법등에는 포함되어 있지는 않지만 2014년 3월 10일에 발표한 『금융분야 개인정보 유출 재발방지 종합대책』[6]에는 정보유출 시 대응 매뉴얼 마련 및 비상 대응체계 구축을 반영하고 있으므로 12.1.1, 12.3.1, 12.3.2는 제외하기로 한다.

또한 2014년 7월 31일에 국무총리실 주관으로 발표한 『개인정보보호 정상화대책』[7]에는 주민등록번호의 암호화를 포함하고 있으므로 9.1.1을 제외하기로 한다.

더불어 금융분야에서는 스마트워크센터가 운영되지 않고 있기 때문에 11.2.6도 제외하고, 교육에 관하여 계층별로 받아야 하는 시간을 명시한 규정의 개정에 따라 4.2도 제외한 남은 13개에 대하여 고찰한다.

Table 4. Non-Financial Controls over mean value on security management process of ISMS

Number	Management Process	Control #	Detailed Management Process
1	Establish Security Policy and Scope	1.1	Establish Security Policy
4	Implement Security Controls	4.2	Internal sharing and training

Table 5. Non-Financial Controls over mean value on security controls of ISMS

Contro Clause Number	control clause	Control objective Number	Control Objective	Control number	controls
1	Security policy	1.1	Approve and publish Ssecurity policy	1.1.1	Approve security policy
				1.1.2	Publish security policy
		1.2	Security policy architecture	1.2.1	Consistency of high level policy
		1.3	Maintain security policy	1.3.1	Review security policy
3	Outsourced human resource security	3.2	Implement outsourced human resources	3.2.1	Implement and maintain outsourced human resources
				3.2.2	outsourced human contract timeout
4	Asset management	4.2	Classify information asset	4.2.1	Classify information asset
9	Encryption	9.1	Encryption policy	9.1.1	Establish encryption policy
10	Access control	10.1	Access control policy	10.1.1	Establish access control policy
		10.4	Access control area	10.4.2	Server access
				10.4.3	Application program access
				10.4.4	Database access
				10.4.5	Mobile device access
11	Maintenance	11.2	System and service operation security	11.2.6	Smartwork security
12	Information security incident management	12.1	Incient response procedure and system	12.1.1	Establish Incient response procedure
		12.3	Follow up	12.3.1	Incident analysis and sharing
				12.3.2	Prevent re-accident

4.1 정보보호 관리과정 분야

○ 정보보호 정책 수립 및 범위 설정

정보보호정책은 규제 이전에 동 금융기관에서 정보보호의 최종 목적을 정하는 것이다. 정보보호정책의 수립에 관하여 전자금융거래법 제21조 제4항에서는 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하도록 하고 있다. 따라서 내년 제출하는 계획에는 제출 금융기관이 정한 정보보호 관련 정책이 포함될 가능성이 높다. 그러나 명시적으로 정보보호정책을 작성 규칙 등에서라도 포함하도록 함으로써 당해 금융기관이 추구하는 정보보호의 대 고객 신뢰도를 높이는 것이 바람직하다.

4.2 정보보호대책 분야

○ 정보보호 정책의 승인 및 공표

금융분야에서 정보보호정책에 대해서는 법률에 명시하지 않았으나 자체 보고체계에 따라 승인받고 확정하여 운영하고 있다. 정보보호정책과 대책이 수립될 경우 이를 공유하고자 인트라넷 등을 활용하고 있으나 실질적인 공유를 위해서는 개개인의 정책숙지에 대한 서명, 주기적인 정책 시험시행 등도 필요하다.

○ 외부자 보안

최근의 은행, 카드사 등 대규모 개인신용정보의 유출 사건의 주요 취약점은 외주 직원에 의한 권한 탈취로 인해 발생되었다. 현재 전자금융감독규정 제13조에서는 전산자료 보안대책으로 외부사용자에게 사용자 계정을 부여하는 경우는 최소한의 작업권한만 할당하고 적절한 통제장치를 갖추도록 하고 있다. 그러나 외부직원에 대하여 보안을 이행하는지에 대하여 주기적으로 점검하도록 명시함으써 특별히 상시 탐지할 수 있는 활동이 추가된다면 위험을 더욱 줄일 수 있을 것이다.

○ 정보자산 분류

정보자산의 분류는 정보자산의 중요성을 측정하고 중요도에 상응하는 책임자를 지정하여 보호 책임성을 높이기 위함이다. 정보자산을 모두 중요하다고 생각하여 중요도를 달리하지 않고 획일적으로 적용할 경우 이는 정보보호의 효율성을 떨어뜨릴 수 있기 때문에 비용효과적이지 않다. 따라서 정보자산을 파악하고 중요도를 산정한 후에 담당자를 지정하여 관리하도록 전자금융거래등에서의 보안 통제사항으로 반영이 필요하다.

○ 접근통제

접근통제는 보안에서 가장 기본적이면서 가장 중요한 분야이다. 이에 부응하여 전자금융거래법 제21조의4에서는 누구든지 전자적 침해행위 등의 금지를 다루고 있고, 감독규정에서는 제11조 전산실 출입통제, 제12조 단말기 보호대책, 제13조 전산자료 보호대책에서 접근통제를 비중 있게 다루고 있다.

이러한 접근통제 정책이 비중 있게 다루어지고 있음에도 불구하고 보안사고의 상당 부분이 동 원인에 기인하고 있다. 그러나 여전히 역할기반의 사용자 접근통제, 외부에서의 디바이스 접근통제 등에서 차별화되지 않고 있다. 서버별, 응용프로그램별, 기타 각종 네트워크 장비별 차별화된 접근통제 정책과 구현이 필요하다.

○ 기타

기준점수 이상을 받지는 못했지만 추가적으로 파일 등의 내부공유 금지, 프로그램 개발 시 안전한 코딩을 위한 가이드의 적용, 전송구간에서 암호화, 저장매체의 파기 등도 전자금융거래법등에 포함되어 있지 않은 사항들이나 이들의 적용에 대해서도 고려는 해볼 수 있다.

V. 결 론

2013년 6.25 사이버테러, 2013년 12월 은행권 개인신용정보 유출, 2014년 1월 카드사 개인신용정보 유출 등으로 인하여 전자금융거래에서의 안전성은 더욱 강화되어야 한다는 사회적 합의에 따라 2014년 3월 10일에는 금융분야 개인정보 유출 재발방지 종합대책을 발표하고 이에 따라 전저금융거래법을 보강하는 내용으로 개정을 추진 중에 있다.

또한 2014년 7월 31일에는 국무총리실 주관 관계부터 함동으로 개인정보보호 정상화대책을 발표하여 개인정보처리자의 책임성을 더더욱 강화하고 이용자의 권리를 구제하고 유통되는 개인정보의 최소화와 주민등록번호의 관리제도를 개선하기로 하였다.

이러한 대책들에 부응하여 현재의 전자금융거래법에서 추가로 고려하여야 할 사항들을 분석하였으나 전자금융거래법을 기준으로 분석하였기 때문에 현장

에서 운영되고 있는 사항은 다소 반영하지 못한 부분들이 있을 것이다.

또한 법과 비교한 대상이 일정규모 이상은 의무적용하고 그 이하는 권고사항인 정보보호관리체계(ISMS) 통제사항과 비교하였다는 점에서 위상이 다소 차이가 날 수 있다.

그러나 분석한 내용이 어떠한 방식으로든 필요하다고 판단할 경우 전자금융거래법등에서든지 아니면 다른 방식으로든 반영은 필요하다고 하겠다.

향후에는 전자금융의 안전성을 의무로 채택하고 있는 미국의 금융서비스현대화법안(Gramm-Leach-Bliley Act), ISO/IEC 27015를 분석하여 금융분야의 사실상의 세계적 수준에 맞추기 위한 연구가 필요하고 미국회계사협회(AICPA)에서 발간한 SOC2에 대한 비교 연구 등도 필요하다. 또한 전자금융의 안전성을 위한 다양한 정부기관의 정책에 따라 추가적으로 보완하여야 할 사항들도 필요하다.

References

[1] Dataloss, http://www.datalossdb.org, 2014.

[2] Financial Supervisory Commission, Regulation on Supervision of Electronic Financial Activities (FSC 2013-39), Amended on December 2, 2013.

[3] Financial Supervisory Commission, "Electronic Financial Transaction Act", Amended on May 22, 2013

[4] Ministry of Science, ICT and Future Planning, "Regulation on Information Security Management System"(MSIP 2013-36), August 8, 2013.

[5] ISO/IEC, "ISO/IEC 27014:2013 Information Technology - Security Techniques - Governance of information security", 2013.

[6] FSC et al., "Comprehensive Countermeasures for Preventing Recurrence of Personal Infrmation Leakage in the Field of Finance", March 10, 2014.

[7] Office of the Prime Minister, "Normalization Plan for Protecting Personal Information", July 31, 2014.

〈저자소개〉

이 강 신 (Gangshin Lee) 종신회원
1989년 8월: 한양대학교 수학과 석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
1990년 7월~1992년 6월: (주) 데이콤 종합연구소 연구원
1992년 7월~2000년 8월: 한국정보화진흥원 부장
2000년 9월~2011년10월: 한국인터넷진흥원 단장
2011년11월~현재: 김·장 법률사무소 전문위원
2006년 9월~현재: 건국대학교 정보통신대학원 겸임교수
〈관심분야〉 정보보호관리, 네트워크보안, 개인정보보호