Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1605

전자금융기반시설 정보보호 수준강화 방안 (정보보호 관리수준 분석을 통한)

박 근 덕,[1†] 염 흥 열[2‡]
[1]한국아이티평가원, [2]순천향대학교

Improvements of Information Security Level in Electronic Financial Infrastructure(By Analyzing Information Security Management Level)

Keun-dug Park,[1†] Heung-youl Youm[2‡]
[1]KSEL, [2]Soonchunhyang University

요 약

최근 몇 년 동안 금융회사(은행, 증권사, 신용카드사, 보험사 등)를 대상으로 한 개인정보 유출, 홈페이지 해킹, 분산서비스거부공격(DDoS) 등 보안사고가 꾸준히 증가하고 있다. 본 논문에서는 현행 전자금융기반시설의 정보보호 관리수준의 문제점을 법적 준거성과 정보보호 인증제도 관점에서 분석하고 금융 분야 특성에 적합한 종합적인 관리체계 하에서 높은 수준의 정보보호 활동이 지속 가능하도록 정보보호관리체계, 정보보호 준비도 평가 및 주요정보통신기반시설 취약점 분석·평가 제도를 활용한 개선방안을 제시하고자 한다.

ABSTRACT

In recent years, security incidents - such as personal information leakage, homepage hacking, DDoS and etc. – targeting finance companies(banks, securities companies, credit card companies, insurance companies and etc.) have increased steadily. In this paper, we analyze problems of information security management level in the existing electronic financial infrastructure from perspective of compliance and information security certification system and propose improvements to enable sustainable high level of information security activities under a comprehensive management system for the financial sector characteristics using ISMS, SECU-STAR and CNIVAM system.

Keywords: Electronic Financial Infrastructure, Information Security, ISMS(Information Security Management System), SECU-STAR(SECUriTy Assessment for Readiness), CNIVAM(Critical Network Infrastructure Vulnerability Analysis·Measurement)

I. 서 론

'전자금융기반시설'이란 전자금융거래에 이용되는 정보처리시스템 및 정보통신망(전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제)을 말하고[1][5], 전자금융기반시설의 운영 및 관리 책임은 금융회사에 있다.

최근 몇 년 동안 금융회사(은행, 증권사, 신용카드사, 보험사 등)는 개인정보 유출 및 전산망 마비 등의 보안사고 사례를 통하여 사회적·경제적으로 혹독한 대가를 치룬바 있다. 또한 최근에는 중요 정보를 볼모로 금전적 보상을 요구하는 랜섬웨어(Ransom+Software)가 기승을 부리고 있고, 배드유에스비(BadUSB)와 같이 USB메모리의 펌웨어를 조작하여 해킹 도구로 악용하는 최신 기술이 등

Received(06. 27. 2016), Modified(11. 03. 2016), Accepted(11. 03. 2016)
† 주저자, jacepark926@gmail.com
‡ 교신저자, hyyoum@sch.ac.kr(Corresponding author)

장하고 있어 지속적인 보안사고 예방이 절실히 필요하다.

금융회사에서 운영·관리하는 전자금융기반시설은 대량의 개인정보(주민등록번호, 계좌번호, 신용카드번호 등) 및 중요정보(금융거래정보, 비밀번호, 바이오정보 등)를 처리하는 정보시스템으로 구성되어 있기 때문에 금융회사는 금융 분야 특성에 맞게 자율적으로 종합적인 관리체계를 구축·운영하고, 높은 수준의 정보보호 활동이 지속 가능하도록 전사적으로 노력하여야 한다.

본 논문의 2장에서는 금융 분야에서 수행하고 있는 정보보호 평가 방안, 정보보호 인증제도 등에 관한 현황을 살펴보고, 3장에서는 현행 전자금융기반시설의 정보보호 관리수준의 문제점을 분석하고, 4장에서는 금융 분야 특성에 적합한 개선방안을 제시하고자 한다.

II. 관련 연구

본 장에서는 전자금융기반시설 취약점 분석·평가, 금융회사의 정보기술부문 실태평가, 정보보호관리체계(ISMS) 인증, 주요정보통신기반시설 취약점 분석·평가, 정보보호 준비도 평가 제도에 대하여 설명한다.

2.1 전자금융기반시설 취약점 분석·평가

금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 취약점을 분석·평가하고 그 결과를 금융위원회에 보고하고 있다[1].

○ 법적 근거
- 『전자금융거래법』 제21조의3(전자금융기반시설의 취약점 분석·평가)
- 『전자금융거래법 시행령』 제11조의4(전자금융기반시설 취약점 분석·평가의 내용)
- 『전자금융감독규정』 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)
- 『전자금융감독규정 시행세칙』 제7조의2(전자금융기반시설의 취약점 분석·평가의 내용)

○ 시행 주기
- 매 년 1회 이상

○ 취약점 분석·평가 내용
- 3개 평가 부문의 20개 평가 항목으로 구성 (Table 1. 참조)

Table 1. 『Electronic Financial Supervisory Regulations Detailed Enforcement Regulations』 〈Annex 3〉[4]

Sector	Measurement Item
Managerial Security	- Information Security Policy - Information Security Organization and Human Resource - Internal Control - Information Security Education and Training - Asset Management - Business Continuity Management - Incident Management - Information System Introduction, Development and Maintenance
Physical Security	- Computer Equipment Security - Computer Center Security
Technical Security	- Internet Electronic Financial Security - Mobile Electronic Financial Security - Access Control - Computer Data Security - Server Security - Database Security - Web Service Security - Terminal Security - Network Security - Information Security System Security
3 Sectors	20 Measurement Items

전자금융기반시설 취약점 분석·평가 내용은 『전자금융감독규정 시행세칙』〈별표 3〉에 정하고 있으나, 세부 평가항목은 금융회사가 자율적으로 정하여 시행하고 있다. 반면에 타 주요정보통신기반시설의 관리기관의 경우에는 2.4에서 보는 바와 같이 『주요정보통신기반시설 취약점 분석·평가 기준』(미래창조과학부고시 제2013-37호)에서 정하고 있는 세부 평가항목(기본·선택)을 준용하고 있다.

IBK캐피탈은 전자금융기반시설 취약점 세부 평가항목을 정함에 있어 『전자금융감독규정』의 각 조항에 근거를 두고 있다.

IBK캐피탈의 전자금융기반시설 취약점 평가항목은 아래의 Table 2.와 같다[13].

금융회사는 아래의 'IBK캐피탈의 전자금융기반시설 취약점 평가항목 일부 예시'에서 보는 바와 같이

Table 2. Electronic Financial Infrastructure Vulnerability Measurement Items of IBK Capital

Area	The Number of Measurement Items	Basis [3]
1. Human Resource	3	No. 8
2. Organization	3	
3. Budget	2	No. 5, No. 8
4. Buildings and Facilities	19	No. 9, No. 10
5. Computer Center	17	No. 9, No. 11
6. Terminal	13	No. 12
7. Computer Data	22	No. 13
8. Information Processing System	10	No. 14
9. Information Security System	7	No. 15
10. Open Web Server	22	No. 17
11. Computer Network	1	No. 18
12. IP Address	5	No. 18
13. IT Plan	4	No. 19
14. IT Business	4	No. 20
15. IT Contract	9	No. 21
16. IT Supervision	5	No. 22
17. Capacity and Performance Management	1	No. 25
18. Job Separation	8	No. 26
19. Computer Ledger Control	8	No. 27
20. Transaction Control	2	No. 28
21. Program Control	10	No. 29
22. Batch Job Control	5	No. 30
23. Cryptography Program and Key Management Control	4	No. 31
24. Internal User Password Management	8	No. 32
25. IT Outsourcing	14	No. 60
26. IT Sector Reality Measurement	3	No. 58
27. Compliance of Electronic Financial Transaction	10	No. 34
28. Customer Precaution Notice	5	No. 35
29. Security Review	3	No. 36
30. User Password Management	11	No. 33
31. Vulnerability Analysis and Measurement	2	No. 15
32. Incident Prevention	7	
33. Preventing Malware Infection	5	No. 16
34. Emergency Measures	17	No. 23
35. Disaster Recovery Center	4	
36. Disaster Recovery Training	1	
37. Incident Response Training	2	No. 24
38. IT Sector Electronic Financial Incident Report	8	No. 73
38 Managerial Areas	**307 Items**	-
39. UNIX Server	44	No. 14
40. Windows Server	46	
41. Database	10	
42. Security Equipment	16	No. 15
43. Network Equipment	14	
44. Web Service	28	No. 17
45. Smart Phone Banking	15	No. 15
7 Technical Areas	**173 Items**	-
45 Areas	**749 Items**	-

취약점 평가항목을 '체크리스트' 방식으로 개발하여 적용하고 있다[13].

○ 인력 부문 평가항목(근거: 『전자금융감독규정』 제8조)
- 정보기술(이하'IT"라 한다)부문 인력비율(5%이상)의 적정성
- 정보보호 인력비율(5%이상)의 적정성
- IT외주인력 수행 업무에 대한 적정성 및 검토 여부
- IT인력 및 정보보호인력에 대한 연수 프로그램의 적정성

○ 조직 부문 평가항목(근거:『전자금융감독규정』제8조)
- 정보처리시스템 관련 전담조직 운영 여부
- 전자금융업무 관련 전담조직 운영 여부
- IT 아웃소싱(이하 'IT자회사'포함) 통제·관리 조직(인력포함) 운영 여부

○ 예산 부문 평가항목(근거:『전자금융감독규정』제8조)
- 정보보호 예산 비율(7%)의 적정성
- 전자금융사고 책임이행을 위한 보험, 공제 또는 적립금 규모의 적정성

2.2 금융회사의 정보기술부문 실태평가

금융감독원은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 『전자금융감독규정』〈별표 5〉에 명시된 일부 대형 금융회사에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하고 있다[3].

○ 법적 근거
- 『전자금융감독규정』 제58조(금융회사의 정보기술부문 실태평가 등)
- 『전자금융감독규정 시행세칙』 제9조(정보기술부문 실태평가 방법 등)

○ 시행 주기
- 매 년 1회 이상

○ 실태평가 내용
- 『전자금융감독규정 시행세칙』〈별표 4〉[4]의 내용은 아래의 Table 3.을 참조한다.

○ 평가 등급
- 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험)

Table 3. 『Electronic Financial Supervisory Regulations Detailed Enforcement Regulations』 〈Annex 4〉

Sector	Measurement Item
1. IT Audit	- IT Audit Organization and Staff - IT Audit Conducted Content - IT Audit Ex Post Facto Management and Etc.
2. IT Management	- IT Department Organization and Staff - IT-related Bylaws(Regulations, Guidelines, Procedures, Manuals, Etc.) - IT Plan and Direction Suggest - Emergency Plan - Management Information Systems, Etc. - IT Human Resource and Adequacy of the Budget
3. System Development, Introduction and Maintenance	- Organization and Staff - Bylaws(Regulations, Guidelines, Procedures, Etc.) - Status of System Development, Introduction and Maintenance - Internal Control System, System Integration, Etc.
4. IT Service Delivery and Support	- Organization and Staff - Bylaws(Regulations, Guidelines, Procedures, Etc.) - Facilities and Equipment - Operations Control - Communications Network - End-User Computing - Electronic Financial Transaction, Etc.
5. IT Security and Information Security	- IT Security Procedure - IT Security Risk Measurement - IT Security and Information Security Strategy - IT security control Implementation - IT Security Monitoring
5 Sectors	25 Items

정보기술부문의 실태 평가항목은 『전자금융감독규정 시행세칙』〈별표 4〉에서 정하고 있으나, 세부 평가 항목은 금융감독원이 정하여 시행하고 있다.

2.3 정보보호관리체계(ISMS) 인증

미래창조과학부는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 할 수 있다[5].

○ 법적 근거
- 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제47조(정보보호 관리체계의 인증)
- 『정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령』 제47조(정보보호 관리체계 인증의 방법·절차·범위 등)
- 『정보보호 관리체계 인증 등에 관한 고시』(미래창조과학부고시 제2016-59호)

○ 유효 기간
- 3년(매 년 1회 이상 사후심사)

○ 인증기준 내용
- 『정보보호 관리체계 인증 등에 관한 고시』〈별표 7〉[7]은 아래의 Table 4.를 참조한다.

Table 4. 『Notice Concerning Information Security Management System Certification, Etc.』 〈Annex 7〉

Domain	Control Area	The Number of Control Items
Management Courses	1. Establishment of Information Security Policy and Scope	2
	2. Executives Responsibility and Organization	2
	3. Risk Management	3
	4. Implementation of Information Security Measures	2
	5. ex post facto management	3
	Subtotal	**12**
Protection Measures	1. Information Security Policy	6
	2. Information Security Organization	4
	3. Visitor Security	3
	4. Classification of Information Asset	3
	5. Information Security Training	4
	6. Human Security	5
	7. Physical Security	9
	8. System Development Security	10
	9. Cryptography Control	2
	10. Access Control	14
	11. Operation Security	22
	12. Incident Management	7
	13. IT Disaster Recovery	3
	Subtotal	**92**
2 Domains	**18 Control Areas**	**104**

ISMS 인증 제도는 기업(조직)이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계의 적합성에 대해 인증을 부여하고, '일회성 관리', '부분적 보안'이 아닌 '지속적 관리', '전사적 보안'을 위한 보다 높은 수준의 보안관리 활동을 가능하게 하는 효과적인 수단이다.

2016년 6월 현재 유지되고 있는 ISMS 인증서는 총 407건이고, 그 중 금융회사의 인증서는 농협은행, NH농협은행, KB국민은행, 우리은행, 중소기업은행, 신한은행, 하나은행, 유안타증권, 미래에셋증권, 신한금융투자, HMC투자증권, 한화투자증권, 교보증권, 메리츠종합금융증권, 현대증권, 동부증권, KDB대우증권, SK증권, 하나대투증권, 유진투자증권, 우리투자증권, 키움증권, 한국투자증권, 삼성증권, 대신증권, 동부화재해상보험, 삼성화재해상보험, 비씨카드 등 28건으로 총 발급 건수 대비 15% 수준이다[15].

또한 2016년 6월 현재 인가된 금융회사(각 협회별 정회원 기준) 160개 중 ISMS 인증서를 유지하고 있는 금융회사는 28개이므로 18% 수준에 불과하다.

○ 금융회사 인가 현황(2016년 6월 현재)
- 은행社 : 16개[19]
- 증권社 : 55개[20]
- 보험社 : 23개(생명보험), 15개(손해보험)[21][22]
- 신용카드社 : 8개[23]
- 리스·할부금융社 : 43개[23]

2.4 주요정보통신기반시설 취약점 분석·평가

주요정보통신기반시설을 관리하는 기관은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 관리적·물리적·기술적 대책을 포함한 관리대책을 수립·시행하고 있다[8].

○ 법적 근거
- 『정보통신기반 보호법』 제9조(취약점의 분석·평가)
- 『정보통신기반 보호법 시행령』 제17조(취약점 분석·평가의 시기), 제18조(취약점 분석·평가 방법 및 절차), 제19조(정보공유·분석센터의 취약점 분석·평가)
- 『주요정보통신기반시설 취약점 분석·평가 기준』(미래창조과학부고시 제2013-37호)

○ 시행 주기
- 매 년 1회 이상

○ 취약점 분석·평가 점검 항목
- 『주요정보통신기반시설 취약점 분석·평가 기준』[10]은 아래의 Table 5.를 참조한다.

Table 5. 『Critical Network Infrastructure Vulnerability Analysis and Measurement Criteria』

Area	Category	Vulnerability Checklist	
		Mandatory	Optional
Managerial	Information Security Policy	4	4
	Information Security Organization	1	3

Area	Category	Vulnerability Checklist	
		Mandatory	Optional
	Human Security	2	4
	Visitor Security	2	3
	Asset Classification	3	2
	Media Management	2	3
	Education and Training	1	4
	Access Control	7	14
	Operation Management	13	20
	Business Continuity Management	1	3
	Incident Response	3	10
	Audit	0	5
Physical	Access Control	2	1
	Surveillance and Control	4	4
	Power Protection	1	3
	Environmental Control	0	11
Technical	UNIX	43	30
	Windows	45	37
	Security Equipment	16	10
	Network Equipment	14	24
	Control Systems	16	6
	PC	14	6
	Database	11	13
	Web	28	0
3 Areas	24 Categories	233	220
		453	

주요정보통신기반시설 관리기관은 업무 분야별(교육, 의료, 에너지 등) 특성에 따라 관리적·물리적·기술적 취약점 평가항목을 일부 보완하여 취약점 분석·평가를 시행하고 있고, 기본 평가항목(등급: 상)과 선택 평가항목(등급: 중·하)을 모두 준용하고 있다.

2.5 정보보호 준비도 평가

미래창조과학부는 보안, 인력 조직 확충, 법규준수 등 기업의 보안 역량 강화를 위한 정보보호 준비 수준을 평가함으로서 정보보호 자율규제 문화 정착 및 기업의 자발적 정보보호 역량 강화를 유도하고 있다.

○ 법적 근거
- 『정보보호산업의 진흥에 관한 법률』 제12조 (정보보호 준비도 평가 지원 등)

○ 유효 기간
- 1년

○ 평가기준 내용
- '정보보호 준비도 평가 기준'[14]은 아래의 Table 6.을 참조한다.

○ 평가 등급
- 1등급(AAA), 2등급(AA), 3등급(A), 4등급(BB), 5등급(B)[14]

Table 6. Information Security Readiness Measurement Criteria

Area	Category	Measurement Item	Score
Based Indicator	1. Information Security Leadership	1.1 CISO Appointment	5
		1.2 Information Security Communication and Information Provision	5
		1.3 Information Security Operating Policy	4
	2. Information Security Resource Management	2.1 Information Security Implementation Plan	4
		2.2 Information Security Human Resources and Organization	4
		2.3 Information Security Budgeting and Execution	4
		2.4 Information Security Implementation Inspection	4
Activity Indicator	3. Managerial Protection Activity	3.1 Information Security Training Performance	5
		3.2 Asset Management	4
		3.3 Human Security	4
		3.4 Visitor Security	5
	4. Physical Protection Activity	4.1 Environment Security of Information and Communication Facility	4
		4.2 Access Control of Information and Communication	4

Area	Category	Measurement Item	Score
		Facility	
		4.3 Office Security	4
	5. Technical Protection Activity	5.1 Vulnerability Inspection	5
		5.2 Information Security Incident Detection and Response	5
		5.3 System Development Security	4
		5.4 Network Security	4
		5.5 Information System and Application Authentication	5
		5.6 Data Loss prevention	4
		5.7 System and Service Operation Security	5
		5.8 Backup and IT Disaster Recovery	4
		5.9 PC and Mobile Device Security	4
Optional Indicator	6. Personal Information Security	6.1 Personal Information Collected at least	P
		6.2 Personal Information Treatment Policy	P
		6.3 User Right Protection	P
		6.4 Managerial Protection of Personal Information	P
		6.5 Technical Protection of Personal Information	P
		6.6 Personal Information Destruction	P
3 Areas	6 Categories	29 Items	100

III. 전자금융기반시설 정보보호 관리수준의 문제점

본 장에서는 금융회사가 매년 1회 이상 주기적으로 수행하고 있는 '전자금융기반시설 취약점 분석·평가' 및 '정보기술부문 실태평가'의 평가 항목을 분석함으로서 금융회사가 관리하는 전자금융기반시설의 주요 IT자산인 정보시스템(서버, 보안장비, 네트워크장비, PC, 데이터베이스 등) 및 대량의 정보자산(주민등록번호, 계좌번호, 신용카드번호, 내부비밀정보 등)을 안전하게 보호하기 위한 정보보호 관리수준의 문제점을 설명한다.

3.1 전자금융기반시설 취약점 분석·평가의 한계점

3.1.1 ISMS 통제항목과 전자금융기반시설 취약점 평가항목 비교・분석

ISMS의 통제항목과 전자금융기반시설 취약점 평가항목을 비교·분석한 결과, 아래의 Table 7.에서 보는 바와 같이 ISMS 통제항목 104개 중 전자금융기반시설 취약점 평가항목이 만족하는 통제항목은 67개(64%)로서 특히 관리적 분야에서 매우 부족함을 확인하였다.

Table 7. Mapping of ISMS Control Item and Electronic Financial Infrastructure Vulnerability Measurement Item

ISMS Control Item		EFIVMI*
1.1	Establishment of Information Security Policy	-
1.2	Establishment of Scope	-
2.1	Executives Participation	-
2.2	Configuration of Information Security Organization and Resources Assignment	-
3.1	Risk Management Methods and Planning	-
3.2	Risk Identification and Measurement	9, 29, 31
3.3	Selection of Information Security Measures and Establishment of Action Plan	-
4.1	Effective implementation of Information Security Measures	-
4.2	Internal Shares and Training	-
5.1	Reviewing Compliance with Legal Requirements	-
5.2	Management of ISMS Operation Status	-
5.3	Internal Audit	-
1.1.1	Policy Approval	-
1.1.2	Policy Publication	-
1.2.1	Linkages with the Parent Policy	-
1.2.2	Establishing policy enforcement documents	-
1.3.1	Policy Review	-
1.3.2	Policy Documents Management	-
2.1.1	CISO Appointment	1

ISMS Control Item		EFIVMI*
2.1.2	Configuration of Working-level Organization	2, 3
2.1.3	Information Security Committee	2
2.2.1	Role and Responsibility	1, 2, 16, 26
3.1.1	External Parties Contractually Security Requirements	25
3.2.1	Management of External Party Security Transition	25
3.2.2	Security of External Party Contract End	25
4.1.1	Information Asset Identification	-
4.1.2	Responsibility Assignment about Each Information Asset	-
4.2.1	Security Level and Treatment	-
5.1.1	Training Plan	1, 13
5.1.2	Subject for Training	1, 13
5.1.3	Training Content and Method	1, 13
5.2.1	Training Enforcement and Measurement	1, 13
6.1.1	Major Staff Appointment and Supervisory	18
6.1.2	Job Separation	18
6.1.3	Confidentiality Pledge	-
6.2.1	Retirement and Job Change Management	-
6.2.2	Reward and Punishment Regulations	-
7.1.1	Protection Areas Appointment	4, 5
7.1.2	Protection Equipment	4, 5
7.1.3	Working Inside Protection Area	4, 5
7.1.4	Access Control	4, 5
7.1.5	Mobile Devices In & Out	4, 5
7.2.1	Cable Security	4, 5
7.2.2	System Deployment and Management	4, 5
7.3.1	Security of Private Business Environment	6
7.3.2	Security of Common Business Environment	6
8.1.1	Definition of Security Requirements	14, 15, 25
8.1.2	Function of Authentication and Encryption	23
8.1.3	Function of Security Log	20, 21
8.1.4	Function of Access Privilege	21
8.2.1	Implementation and Test	21
8.2.2	Environment Separation of Development and Operation	21
8.2.3	Transfer to Operation Environment	21
8.2.4	Test Data Security	21
8.2.5	Source Code Security	-
8.3.1	Outsource development Security	-
9.1.1	Establishment of Cryptography Policy	23, 27
9.2.1	Encryption Key Generation and Use	23
10.1.1	Establishment of Access Control Policy	-
10.2.1	User Registration and Authorization	7, 8, 9
10.2.2	Management of Administrator and Special Authority	7, 8, 9
10.2.3	Access Authority Review	7, 8, 9
10.3.1	User Authorization	7, 8, 9
10.3.2	User Identification	7, 8, 9
10.3.3	Administrator Password Management	24, 30
10.3.4	User Password Management	24, 28, 30
10.4.1	Network Access	9, 11, 12, 43
10.4.2	Server Access	8, 39, 40
10.4.3	Application Access	-
10.4.4	Database Access	8, 41
10.4.5	Mobile Device Access	-
10.4.6	Internet Connection	9, 10
11.1.1	Establishment of Operating Procedures	21, 22
11.1.2	Change Management	8, 19, 21, 22
11.2.1	Information System Acquisition	-
11.2.2	Security System Operation	9, 42
11.2.3	Performance and Capacity Management	17
11.2.4	Fault Management	34
11.2.5	Remote Operations Management	9
11.2.6	Smart work Security	-
11.2.7	Wireless Network Security	5, 11
11.2.8	Open Server Security	10, 44, 45
11.2.9	Backup Management	7, 8
11.2.10	Vulnerability Inspection	31
11.3.1	Electronic Transaction Security	-
11.3.2	Establishment of Information Transfer Policy and Agreement	-
11.4.1	Information System Storage Media Management	7
11.4.2	Portable Storage Media Management	7
11.5.1	Malware Control	33
11.5.2	Patch Management	8, 9
11.6.1	Time Synchronization	8
11.6.2	Logging and Preservation	7, 8, 19

ISMS Control Item		EFIVMI*
11.6.3	Monitoring of Access and Use	32
11.6.4	Intrusion Attempt Monitoring	32
12.1.1	Establishment of Incident Response Procedures	-
12.1.2	Establishment of Incident Response System	-
12.2.1	Incident Training	36, 37
12.2.2	Incident Report	38
12.2.3	Incident Handling and Recovery	-
12.3.1	Incident Analysis and Sharing	-
12.3.2	Recurrence Prevention	-
13.1.1	Establishment of IT Disaster Recovery System	35
13.2.1	Establishing Recovery Measures based on Impact Analysis	34
13.2.2	Test and Maintenance	36, 37
104 Items		**67 Items**

(EFIVMI*=Electronic Financial Infrastructure Vulnerability Measurement Item of Table 2.)

3.1.2 주요정보통신기반시설 기술적 취약점 평가항목과 전자금융기반시설 기술적 취약점 평가항목 비교·분석

주요정보통신기반시설 기술적 취약점 평가항목과 전자금융기반시설 기술적 취약점 평가항목을 비교·분석한 결과, 아래의 Table 8.에서 보는 바와 같이 주요정보통신기반시설 기술적 취약점 평가항목 291개 중 전자금융기반시설 기술적 취약점 평가항목이 만족하는 항목은 158개(54%)이고 특히 PC(노트북)에 대한 취약점 평가항목(20개)이 누락되어 있어 주요정보시스템에 대한 취약점 분석이 매우 부족함을 확인하였다.

Table 8. Comparison Critical Network Infrastructure Technical Vulnerability Measurement Item with Electronic Financial Infrastructure Technical Vulnerability Measurement Item

Category	CNITVMI*		EFITVMI*
	Mandatory	Optional	
UNIX	43	30	44
Windows	45	37	46
Security Equipment	16	10	16
Network Equipment	14	24	14
PC	14	6	0
Database	11	13	10
Web	28	0	28
7 Categories	**171**	**120**	**158**
	291		

(CNITVMI*=Critical Network Infrastructure Technical Vulnerability Measurement Item)

(EFITVMI*=Electronic Financial Infrastructure Technical Vulnerability Measurement Item)

3.1.3 체크리스트 방식의 평가항목

전자금융기반시설 취약점 평가항목은 2.1의 'IBK캐피탈의 전자금융기반시설 취약점 평가항목 일부 예시'에서 보는 바와 같이 금융회사가 자율적으로 『전자금융감독규정』에 근거하여 개발한 평가항목은 '체크리스트' 방식으로 구성되어 있기 때문에 아래와 같은 몇 가지 한계점이 있다.

○ 보호 대상 정보시스템 및 정보자산이 누락될 가능성이 높음

○ 다양한 위협에 대응하기 위한 보호대책을 종합적으로 평가하기에 부족함

○ 금융회사에서 개발한 평가항목은 객관성·공정성이 결여될 가능성이 높음

○ 『전자금융감독규정』은 최소한의 보안 수준을 규정한 것임

3.2 정보기술부문 실태평가의 한계점

'정보기술부문 실태평가'는 아래의 법적 근거에서 보는 바와 같이 금융회사의 IT부문 안전성 및 건전성 관리·감독을 위한 평가에 주안점을 두고 있기 때문에 금융회사의 종합적인 정보보호 관리수준을 평가하기 위한 수단으로 활용하기에는 적합하지 않다.

'정보기술부문 실태평가' 법적 근거는 아래와 같다[3].

> 『전자금융감독규정』 제58조(금융회사의 정보기술부문 실태평가 등)
> ① 금융감독원장은 금융회사의 정보기술부문의 건전성 여부를 감독하여야 한다. 〈개정 2013.12.3.〉

② 금융감독원장은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 〈별표 5〉에 규정된 금융회사(이하 이 조에서 '은행 등'이라 한다)에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하여야 한다.

3.3 관리적·기술적 문제점 요약

전자금융기반시설의 관리적 측면의 정보보호 수준의 문제점은 다음과 같이 요약할 수 있다.

전자금융기반시설 취약점 평가항목과 ISMS 통제항목 비교·분석 결과(Table 7. 참조)
- 전자금융기반시설 취약점 평가항목 45개는 ISMS 통제항목 104개 중 67개를 만족함(64%)
- 특히, ISMS 관리과정 통제항목 12개 중 1개를 만족함(8%)

전자금융기반시설의 기술적 측면의 정보보호 수준의 문제점은 다음과 같이 요약할 수 있다.

전자금융기반시설 기술적 취약점 평가항목과 주요정보통신기반시설 기술적 취약점 평가항목(필수·선택) 비교·분석 결과(Table 8. 참조)
- 전자금융기반시설 기술적 취약점 평가항목 158개는 주요정보통신기반시설 기술적 취약점 평가항목의 기본항목(등급: 상) 171개 중 158개를 만족함(92%)
- 또한, 주요정보통신기반시설 기술적 취약점 평가항목의 선택항목(등급: 중·하) 120개는 만족하지 않음

IV. 전자금융기반시설 정보보호 수준강화 방안

본 장에서는 3.1과 3.2에서 확인된 전자금융기반시설 정보보호 수준의 문제점에 대한 개선방안을 관리적 분야와 기술적 분야로 구분하여 제안한다.

4.1 관리적 분야

일정 규모 이상의 금융회사를 대상으로 현행 정보보호관리체계(ISMS) 인증 제도를 확대 적용하여 전자금융기반시설에 대한 관리적 보호 수준을 강화하여야 하고, 금융회사로부터 주요 정보시스템 등의 운영업무를 위탁받은 용역업체는 정보보호 준비도 평가제도를 활용하여 자발적 정보보호 역량 강화를 유도하여야 한다.

전자금융기반시설의 관리적 정보보호 수준강화 방안 예시를 금융회사(위탁사)와 용역업체(수탁사)로 구분하여 제안함으로서 금융회사의 중요 정보시스템 운영 및 유지보수 업무를 수행하는 용역업체(수탁사)의 정보보호 수준도 강화할 필요가 있다.

전자금융기반시설 관리적 정보보호 수준강화 방안의 예시는 아래와 같다.

4.1.1 금융회사(위탁사)

○ 적용제도 : 정보보호관리체계 인증(2.3 참조)
○ 세부 내용
- 대상 : 매출 1,500억 원 이상의 금융회사
- 통제항목 개선 : 현행 104개 통제항목을 유지하되, 금융 분야 특성에 적합한 세부 통제항목을 개발하여 적용[18]
- 중복완화 : 현행 전자금융기반시설 취약점 평가항목 중 관리적 평가항목(Table 1. 및 Table 2. 참조)을 ISMS 통제항목으로 대체

4.1.2 용역업체(수탁사)

○ 적용제도 : 정보보호 준비도 평가(2.5 참조)
○ 세부 내용
- 대상 : ISMS 인증 미보유 중소기업
- 평가항목 개선 : 현행 29개 평가항목을 유지하되, 금융 분야 특성에 적합한 선택지표를 추가 개발하여 적용(Table 9. 참조)
- 최소 요구 등급 : 5등급(B) + 금융 분야 선택지표(Pass)
- 중복완화 : 금융회사(위탁사)에서 주기적으로 시행하는 용역업체(수탁사) 대상 보안지도·점검을 대체

『전자금융감독규정 시행세칙』〈별표 3의2〉정보보

Table 9. Example of Financial Sector Optional Indicator and Measurement Item

Area	Category	Measurement Item	Score
Optional Indicator	F. Financial Sector Protection Activity	F.1 Computer Center Access Control	P
		F.2 Terminal Security	P
		F.3 Computer Data Security Management	P
		F.4 Information Processing System Connection Control	P
		F.5 Hacking, Etc. Prevention Measures	P
		F.6 Malicious Code Control Measures	P
		F.7 Open Web Server Security Management	P
		F.8 Internal User Password Management	P
		F.9 Customer Password Management	P
		F.10 Customer Precaution	P
		F.11 Electronic Financial Incident Report	P

안 점검항목을 고려한 금융 분야 선택지표 및 평가항목의 예시는 아래의 Table 9.와 같다.

4.2 기술적 분야

금융회사는 소관 전자금융기반시설의 주요 정보시스템을 식별 및 분류하고, 현행 주요정보통신기반시설 취약점 평가항목(기본항목+선택항목) 뿐만 아니라 금융 분야 특성에 적합한 평가항목을 추가로 개발하여 적용함으로서 기술적 보호 수준을 강화할 필요가 있다.

전자금융기반시설 기술적 정보보호 수준강화 방안의 예시는 아래와 같다.

○ 적용제도 : 주요정보통신기반시설 취약점 분석·평가(2.4 참조)

○ 대상 정보시스템
- 현행 : 유닉스·윈도우즈서버, 보안장비, 네트워크 장비, 데이터베이스, 웹서비스, 스마트폰뱅킹
- 개선방안 : 현행 + PC·노트북 (Table 2. 및 Table 5. 참조)

○ 평가항목
- 현행 : 기본항목(171개) + 스마트폰뱅킹(15개)
- 개선방안 : 현행(186개) + 선택항목(120개) (Table 2. 및 Table 5. 참조)

○ 추가 평가항목(금융 분야 특성 고려)
- 목적 : 개인정보(고유식별정보, 비밀번호, 바이오정보 등)를 처리하는 대국민 웹서비스 경우, 전송구간 암호화(HTTPS) 보안강도 및 SSL 통신 안전성 평가를 통하여 개인 정보 유출 등을 예방
- 근거: 『개인정보의 안전성 확보조치 기준』제6조(개인정보의 암호화)
- 전송구간 암호화(HTTPS) 보안강도 및 SSL 통신 안전성 평가항목의 예시는 아래의 Table 10.과 같다.
- 전송구간 암호화(HTTPS) 보안강도 및 SSL 통신 무료 진단도구 : 웹기반 SSL 서버 테스트 (https://www.ssllabs.com/ssltest/)[17]

Table 10. Measurement Items about Transmission Section Encryption(HTTPS) Security Strength and SSL Communication Safety[17]

Division	Categories	Measurement Item
Authent-ication	Server Key and Certificate	Subject
		Common names
		Alternative names
		Valid from
		Valid until
		Key
		Weak key (Debian)
		Issuer
		Signature algorithm
		Extended Validation
		Certificate Transparency
		Revocation information
		Revocation status
		Trusted
	Additional Certificates (if supplied)	Certificates provided
		Chain issues
		Subject
		Valid until
		Key

Division	Categories	Measurement Item
		Issuer
		Signature algorithm
	Certificati on Paths	1
		2
		3
Config- uration	Protocols	TLS 1.2
		TLS 1.1
		TLS 1.0
		SSL 3
		SSL 2
	Cipher Suites	-
	Handshake Simulation	Android 2.3.7
		Android 4.0.4
		Android 4.1.1
		Android 4.2.2
		Android 4.3
		Android 4.4.2
		Android 5.0.0
		Baidu Jan 2015
		BingPreview Jan 2015
		Chrome 48 / OS X
		Firefox 31.3.0 ESR / Win7
		Firefox 42 / OS X
		Firefox 44 / OS X
		Googlebot Feb 2015
		IE 6 / XP
		IE 7 / Vista
		IE 8 / XP
		IE 8-10 / Win 7
		IE 11 / Win 7
		IE 11 / Win 8.1
		IE 10 / Win Phone 8.0
		IE 11 / Win Phone 8.1
		IE 11 / Win Phone 8.1 Update
		IE 11 / Win 10
		Edge 13 / Win 10
		Edge 13 / Win Phone 10
		Java 6u45
		Java 7u25
		Java 8u31
		OpenSSL 0.9.8y
		OpenSSL 1.0.1l
		OpenSSL 1.0.2e
		Safari 5.1.9 / OS X 10.6.8
		Safari 6 / iOS 6.0.1
		Safari 6.0.4 / OS X 10.8.4
		Safari 7 / iOS 7.1
		Safari 7 / OS X 10.9
		Safari 8 / iOS 8.4
		Safari 8 / OS X 10.10
		Safari 9 / iOS 9
		Safari 9 / OS X 10.11
		Apple ATS 9 / iOS 9
		Yahoo Slurp Jan 2015
		YandexBot Jan 2015
	Protocol Details	DROWN (experimental)
		Secure Renegotiation
		Secure Client-Initiated Renegotiation
		Insecure Client-Initiated Renegotiation
		BEAST attack
		POODLE (SSLv3)
		POODLE (TLS)
		Downgrade attack prevention
		SSL/TLS compression
		RC4
		Heartbeat (extension)
		Heartbleed (vulnerability)
		OpenSSL CCS vuln. (CVE-2014-0224)
		Forward Secrecy
		ALPN
		NPN
		Session resumption (caching)
		Session resumption (tickets)
		OCSP stapling
		Strict Transport Security (HSTS)
		HSTS Preloading
		Public Key Pinning (HPKP)
		Public Key Pinning Report-Only
		Long handshake intolerance
		TLS extension intolerance
		TLS version intolerance
		Incorrect SNI alerts
		Uses common DH primes
		DH public server param (Ys) reuse
		SSL 2 handshake compatibility
	Miscellaneous	Test date
		Test duration
		HTTP status code
		HTTP server signature
		Server hostname
2 Divisions	**8 Categories**	**109 Items**

V. 결 론

현행 전자금융기반시설의 정보보호 관리수준의 문제점은 크게 2가지로 요약할 수 있다. 첫 번째로 금융회사는 '전자금융기반시설 취약점 분석·평가'를 매

년 주기적으로 수행하고 있으나, 그 평가내용이 기술적인 측면에 집중되어 있기 때문에 관리적인 측면이 매우 부족하다(3.3 참조). 두 번째로 금융감독원이 주기적으로 수행하는 '정보기술부문 실태평가'는 금융회사의 IT부문 안전성 및 건전성 관리·감독을 위한 평가에 주안점을 두고 있기 때문에 금융회사의 종합적인 정보보호 관리수준을 평가하기 위한 수단으로 활용하기에는 적합하지 않다.

따라서 대량의 개인정보 및 중요정보를 처리하는 전자금융기반시설의 경우, 정보 유출 및 시스템 마비 등 보안사고 발생시 사회적인 파급효과가 매우 심각하기 때문에 금융회사는 금융 분야 특성에 맞는 관리체계 구축 및 정보보호 운영을 자율적으로 수행하되, 현행 제도화 되어 있는 정보보호관리체계(ISMS) 인증, 정보보호 준비도 평가 등을 적극 도입하여 높은 수준의 정보보호 활동을 전사적·지속적으로 보장하여야 한다.

References

〔1〕 Financial Services Commission, "『ELECTRONIC FINANCIAL TRANSACTIONS ACT』," Jan. 2016

〔2〕 Financial Services Commission, "『ELECTRONIC FINANCIAL TRANSACTIONS ACT DECREE』," Dec. 2015

〔3〕 Financial Services Commission, "『ELECTRONIC FINANCIAL SUPERVISORY REGULATIONS』 (Financial Services Commission Notice No. 2015-18)," Jun. 2015

〔4〕 Financial Supervisory Service, "『ELECTRONIC FINANCIAL SUPERVISORY REGULATIONS DETAILED ENFORCEMENT REGULATIONS』," May. 2016

〔5〕 Korea Communications Commission, "『ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.』," Dec. 2015

〔6〕 Korea Communications Commission·Ministry of Science, ICT and Future Planning, "『ENFORCEMENT DECREE OF THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.』," May. 2016

〔7〕 Ministry of Science, ICT and Future Planning, "『Notice Concerning Information Security Management System Certification, Etc.』(Ministry of Science, ICT and Future Planning Notice No. 2016-59)," Jun. 2016

〔8〕 Ministry of Science, ICT and Future Planning, "『ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE』," Jun. 2015

〔9〕 Ministry of Science, ICT and Future Planning, "『ENFORCEMENT DECREE OF THE ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE』," Dec. 2015

〔10〕 Ministry of Science, ICT and Future Planning, "『Critical Network Infrastructure Vulnerability Analysis and Measurement Criteria』(Ministry of Science, ICT and Future Planning Notice No. 2013-37)," Aug. 2013

〔11〕 Ministry of Science, ICT and Future Planning, "『ACT ON PROMOTION OF INFORMATION SECURITY INDUSTRY』," Jun. 2015

〔12〕 Korea Internet & Security Agency, "ISMS Certification System Guide," pp. 5-9, Mar. 2016

〔13〕 IBK Capital, "Request for Proposal of Electronic Financial Infrastructure Vulnerability Inspection," pp. 11-23, May. 2014

〔14〕 Korea Security Evaluation Laboratory Co., Ltd., "http://www.ksel.co.kr/secu_star_summary.php)," Jun. 2016

[15] Korea Internet & Security Agency, "http://isms.kisa.or.kr/kor/issue/issue01.jsp?certType=ISMS)," Jun. 2016
[16] Ministry of the Interior, "『Ensure Safety Criteria of Personal Information』 (Ministry of the Interior Notice No. 2014-7)," Dec. 2014
[17] Qualys Inc., "https://www.ssllabs.com/ssltest/," Jun. 2016
[18] Keun-Dug Park, "Improved measurements of information security management based on compliance in financial companies," Soonchunhyang University, pp. 88-110, Sep. 2015
[19] Korea Federation of Banks , "http://www.kfb.or.kr/cms.html?S=AC," Jun. 2016
[20] Korea Financial Investment Association, "http://www.kofia.or.kr/member_status/m_15/sub0202.do," Mar. 2016
[21] Korea Life Insurance Association, "http://www.klia.or.kr/aklia/aklia_090101.do," Jun. 2016
[22] General Insurance Association of Korea, "http://www.knia.or.kr/about/partner/partner01/," Jun. 2016
[23] The Credit Finance Association Of Korea, "https://www.crefia.or.kr/portal/company/membership/membershipIntroduction.xx?coCodeSubId=1#," Jun. 2016

〈저자소개〉

박 근 덕 (Keun-dug Park) 종신회원
1992년 2월: 동아대학교 전산공학과 학사
2015년 8월: 순천향대학교 대학원 정보보호학과 석사
2015년 9월~현재: 순천향대학교 대학원 정보보호학과 박사과정
2012년 2월~현재: 정보보호관리체계(ISMS) 인증 심사원
2016년 2월~현재: ㈜한국아이티평가원(KSEL) 수석컨설턴트
2016년 4월~현재: ISO/IEC JTC1/SC27/WG5 Expert
〈관심분야〉 정보보호관리체계, 개인정보보호, 정보보호 국제표준, IoT 보안, 클라우드 컴퓨팅 보안, 블록체인

염 흥 열 (Heung-youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2016년~현재: ITU-T SG17 의장
2016년 5월~현재: 개인정보보호표준포럼 의장
〈관심분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜