Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.541

금융권 정보보호 관리 효율을 제고하기 위한 인증모형 개선방안*

오 은,[1†] 김 태 성,[2‡] 조 태 희[1]
[1]조이 보안컨설팅, [2]충북대학교

Improvement of the Certification Model for Enhancing Information Security Management Efficiency for the Financial Sector*

Eun Oh,[1†] Tae-Sung Kim,[2‡] Tae-Hee Cho[1]
[1]CHO&LEE Security Consulting, [2]Chungbuk National University

요 약

3.20 전산 대란, 카드사 고객정보유출사고 등에서 알 수 있듯 보안이 전제되지 않고서는 그 어떤 편의성과 효율성도 담보할 수 없다. 그뿐만 아니라 금융권은 다른 산업보다 고객 이익의 침해 가능성이 커 보안사고 발생 시 이용자의 정신적·금전적 피해가 발생할 수 있으며, 이로 인해 집단 소송, 고객 이탈, 평판 실추, 대외 신뢰도 하락 등으로 이어져 해당 기업의 비즈니스 연속성에도 큰 영향을 미칠 수 있다. 따라서 금융보안 위험에 대한 효과적인 관리가 필요한 실정이다. 본 연구에서는 정보보호 관리 효율성 개선을 위해 국내 대표 정보보호 인증제도를 통합하고 금융 산업의 특성을 반영한 정보보호 관리체계 인증의 필요성을 밝히고자 한다. 또한 금융권 정보보호 관리체계 인증이 필요하다면 앞으로 어떤 방향으로 개발되어야 할지에 대해 제시하고자 한다.

ABSTRACT

Considering the results of the 3.20 Cyber Attack, leaks of personal information by card companies, and so on, convenience and efficiency cannot be guaranteed without security as a prerequisite. In addition, it is more likely that customers' interests seem to be interfered with in financial institutions than in any other industry. Therefore, when a security accident occurs, users may suffer mental damage and monetary loss, leading to class action, customer defection, loss of reputation, and falloff in international credibility, which all may have a significant effect on the business continuity of corporations. This study integrates the representative information security certification systems in order to improve the efficiency of information security management and demonstrate the necessity of information security management system certification for the financial sector. If the certification is needed, we would like to recommend the desirable development direction.

Keywords: Information Security Management System, Financial Information Security, Finanacial Information Security Management System

Received(03. 07. 2016), Modified(03. 31. 2016), Accepted(04. 06. 2016)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(NRF-2011-0025512)
† 주저자, oeun613@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

I. 서 론

정보보안 사고는 기술의 변화 속도, 새로운 기술의 도입과 발맞추어 함께 진화해 왔다. 따라서 보안사고도 더욱더 고도화되고, 복잡해지고, 발생횟수도 빈번해지고 있다[11]. 외부 해킹뿐만 아니라 내부 직원에 의한 보안사고가 늘어나면서 기업은 정보자산을 보호하고 조직 경쟁력을 강화하기 위한 수단으로 정보보호관리 프로세스 개선활동의 하나인 정보보호 관리체계 구축 및 운용에 지속적인 노력을 기울이게 되었다[13].

2002년 국내 정보보호 관리체계(ISMS: Information Security Management System) 인증 도입 이후 14년 간 10개 이상의 정보보호 인증 및 평가제도가 생겼으며, 2개의 제도(정보보호 안전진단, 전자정부 정보보호 관리체계 인증)는 폐지되거나 통합되었다. 이는 정부의 이중 규제 및 중복 제도, 유사 제도 양산의 한계라는 문제를 가지게 되었다. 가장 대표적인 정보보호 인증제도인 정보보호 관리체계(ISMS), 개인정보보호 관리체계(PIMS: Personal Information Management System), 개인정보보호 인증(PIPL: Personal Information Protection Level)은 법 규제 측면에서 차이는 있지만, 심사기준 및 항목이 겹치거나 비슷한 부분이 적지 않다. 따라서 인증대상 기업들은 인증 획득에 드는 비용 부담도 적지 않아 법적으로 의무화된 ISMS 인증에만 몰리고 있다[15].

국제 정보보호 관리체계 표준인 ISO/IEC 27001이 소속된 ISO/IEC 27000시리즈를 보면, ISO/IEC 27001을 기반으로 한 금융, 의료, 통신 분야 등 산업별 정보보호 관리에 관한 세부적인 가이드라인을 제시하고 있다[5]. 이에 따라 국내에서도 앞으로 모든 기업에 적용 가능한 표준 정보보호 인증제도와 함께 개별 기업이 속해있는 업종의 특성을 반영한 산업별 정보보호 관리표준을 제시해야 할 것이다.

특히 금융권의 경우, 업무 시스템이 해킹 당하거나 고객의 개인정보가 유출되어 막대한 재무적 손실이 발생할 수 있으며, 기업의 대외 신뢰도 하락 등의 비재무적 손실을 야기할 수 있다[14]. 이에 따라 본 연구에서는 금융 산업에 먼저 초점을 두어 금융권에 특화된 정보보호 관리체계 인증의 필요성을 밝히고 개발방향을 제안하고자 한다.

II. 이론적 배경

2.1 정보보호 인증제도

정보보호 관리체계란 정보자산의 비밀성·무결성·가용성을 달리하기 위하여 각종 보호대책을 관리하고, 위험기반 접근방법에 기초하여 구축·구현·운영·모니터링·검토·개선 등의 주기를 거쳐 정보보호를 관리하고 운영하는 체계이다[8].

국제 정보보호 관리체계 표준으로는 ISO/IEC 27001이 있으며 과거 영국의 정보보호 관리표준인 BS7799를 기반으로 하여 정보보호 관리체계를 수립, 구현, 운영, 모니터링, 검토 유지 및 개선하기 위한 요구 사항을 규정하고 있다[5]. ISO/IEC 27015는 금융서비스 조직의 정보보호관리에 관한 문서로 법적인 측면, 추가적인 구현 지침, 추가적 통제 항목 등을 포함하고 있는 문서이다[6,7]. Table 1은 ISO/IEC 27001:2005의 11개 통제분야이며, Table 2는 ISO/IEC 27001:2005와 비교하여 금융서비스 조직에 맞춰 수정, 보완된 ISO/IEC 27015:2012의 통제분야와 통제항목을 정리한 것이다.

국내에서 운영되고 있는 대표적인 정보보호 인증제도로는 ISMS, PIMS, PIPL 등이 있다. ISMS 인증제도란, 어떤 조직이 정보보호 관리체계를 구축·운영하고 있을 때, 그 관리체계가 정보보호 관리체계

Table 1. Areas of ISO/IEC 27001[5]

Areas	
Information protection measures	Security policy
	Organization of information security
	Asset management
	Human resources security
	Physical and environmental security
	Communications and operations management
	Access control
	Information systems acquisition, development and maintenance
	Information security incident management
	Business continuity management
	Compliance

Table 2. ISO/IEC 27015 areas and controls supplemented for organizations providing financial services[6]

Areas
Security Policy(5)
Allocation of information security responsibilities/Contact with special interest groups/Identification of risks related to external parties/Addressing security when dealing with customers/Addressing security in third party agreements
Asset management(2)
Inventory of assets/Acceptable use of assets
Human resources security(3)
Screening/Terms and conditions of employment/Information security awareness, education and training
Physical and environmental security(4)
Working in secure areas/Equipment siting and protection/Equipment maintenance/Secure disposal or re-use of equipment
Communications and operations management(7)
Segregation of duties/Capacity management/Controls against malicious code/Disposal of media/Information handling procedures/Internet banking services/Monitoring system use/
Information systems acquisition, development and maintenance(3)
Security requirements analysis and specification/Policy on the use of cryptographic controls/Control of operational software
Business continuity management(2)
Business continuity and risk assessment/Developing and implementing continuity plans including information security
Compliance(2)
Technical compliance checking/Compliance monitoring

Note : ( )is the number of controls supplemented

의 인증 기준에 적합한지를 인증기관이 객관적이고 독립적으로 평가하여 적합성 여부를 판단해 주는 제도로 2002년에 도입되었다. 2013년에는 주요정보통신서비스제공자를 정보보호 관리체계 인증제도의 인증 의무화 대상자로 지정하여 운영하게 되었다. 인증기준은 크게 '정보보호 관리과정'과 '정보보호 대책'으로 이루어져 있다[9]. PIMS 인증은 기업이 개인정보 보호 활동을 체계적·지속적으로 수행하는 데 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도이다. 인증기준은 '관리과정', '보호대책', '생명주기' 3개 분야로

Table 3. Assessment items for integrated certification of PIMS, PIPL

Areas	Assessment items			
	Public institution	Large companies·Internet communications services providers	Small & medium sized firms	Small enterprise
Personal information management processes	16	16	15	3
Personal information lifecycle and assurance on rights	20	19	19	19
Personal information security countermeasures	50	48	44	22
Total	86	83	78	44

구성되어 있다[10]. PIPL은 개인정보처리자의 개인정보보호 관리체계 구축 및 개인정보 보호조치 사항을 이행하고 일정한 보호수준을 갖춘 경우 인증마크를 부여하는 제도이다. 인증 기준은 크게 '개인정보 보호 관리체계'와 '개인정보 보호대책'분야로 구성되어 있다[12]. 방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 근거로 PIMS를 운영해 왔으며, 행정자치부는 「개인정보 보호법」에 따라 공공기관과 일반 사업자를 대상으로 PIPL 제도를 운영해왔다. 개인정보 보호와 관련된 기업이 양 부처가 유사한 인증제도를 별도로 운영해 혼란을 겪어왔으며, 유사한 규제에 대한 통합 요구가 높아 이를 통합하여 한국인터넷진흥원이 본 제도를 운영하기로 하였고(2016.1.1.), PIMS의 124개 심사항목과 PIPL의 65개 항목을 86개로 통합 및 조정하였다(Table 3참조). 본 연구는 '개인정보보호 관리체계 인증 등에 관한 고시'가 개정되기 이전부터 통합모형을 진행하였기 때문에 기존의 PIMS와 PIPL의 심사항목을 활용한 결과를 제시한다.

2.2 중복규제 관련 연구

미래창조과학부는 ISMS, 방송통신위원회는 PIMS 그리고 행정자치부는 PIPL을 별도로 운영해 왔다. 그러나 각 인증체계가 지닌 유사성으로 인해

인증 대상 기업은 혼란을 겪으면서[4] '개인정보보호 정상화 대책'(2014년 7월)과 규제개혁 일환으로 개인정보보호 인증제도(PIMS, PIPL) 통합이 추진되었고[1], 2016년 1월 1일부터 개인정보보호 관리체계 인증(PIMS)으로 통합 시행되고 있다.

이 같은 중복규제는 부처별로 관할권이 중복되기 때문에 발생하는 현상이다. 모든 부처업무가 상호의존적인 성격을 지니기 때문에 관할권이나 부처업무의 중복을 피할 수 없는 '제도적 현실'로 보여진다[3,8]. 관할권의 중첩은 바람직한 가외성으로 귀결될 수도 있지만, 비효율적인 중복과 소모적인 영역다툼으로 귀결될 우려 또한 크다[16]. 최근 들어 정부조직이나 기능의 중복에 대한 관리적 처방의 대부분은 중복을 단일화하기 위한 통폐합에 초점이 맞추어져 효율성을 중시하는 경향이 많아졌다[8].

국외에서는 대부분 국제표준인 ISO/IEC 27001을 따르는 반면, 국내에서는 많은 유사 인증제도 때문에 인증제도 효과성 분석 연구, 인증제도 간 중복성 문제 관련 연구 등이 이루어지고 있다. 박은엽 외[2]는 ISMS와 PIMS를 모두 고려하여 관리체계를 수립하고 인증을 받는 경우 정보보호와 개인정보보호 모두를 고려하고 유기적으로 관리할 수 있게 되어 기업입장에서 체계적으로 관리할 수 있다는 이점이 있지만, 인증심사를 받는 경우에는 동시에 인증심사를 진행하거나 중복항목에 대한 간편화, 또는 행정절차의 간소화 등은 해결되어야 할 문제라고 지적하였다. 강현선[4]은 국내 정보보호 관리체계는 유사성을 지닌 각종 인증체계로 인해 인증 대상 기업이 혼란과 불편을 겪고 있으며, 정보보호 관리체계의 일관성, 신뢰성을 유지하기 위하여 정보보호 관리체계 시스템의 국제적 표준화 및 국제적인 상호 인증의 필요성을 주장하였다. 전자정부 정보보호 관리체계(G-ISMS)와 ISMS가 통합되어 점검항목이 대폭 조정되면서 그에 따른 인력과 예산의 중복을 줄일 수 있었듯, 현재 운영 중인 정보보호 관리체계를 재정비하여 방만한 인증제도의 확산보다는 유사제도간의 통합을 통한 효율적인 인증제도의 확산이 필요한 시점이다[17].

본 연구는 그동안 많은 연구들에서 지적한 정보보호 관리 인증제도 간 중복성 문제를 해결하기 위해 실제 통합모형을 도출하고, 전문가를 대상으로 한 설문을 통해 적정성을 검증받았다. 더 나아가 하나의 통합모형이 금융 분야에서는 어떻게 활용될 수 있을지에 대한 방향을 모색해 보았다는 점에서 관련 연구들과 차별점을 가진다.

III. 방법론

3.1 연구방법 및 절차

금융 산업의 특성을 고려한 정보보호 관리체계 인증모형을 도출하기에 앞서 기존 정보보호 인증제도의 중복성 문제를 해결하고자 한다. 본 연구에서는 국내 대표 정보보호 인증제도인 ISMS, PIMS, PIPL의 평가 기준을 비교 및 통합한다. ISMS와 PIMS는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의거한 제도이며, PIPL은 「개인정보보호법」에 의거한 제도이다. 정보보호 인증 통합 방법은 Fig. 1과 같다.

정보보호 인증제도 통합 시 먼저 ISMS와 PIMS의 세부 통제항목을 비교하여 '동일', '유사', '다름'을 판단한다. 2차로는 ISMS와 PIPL의 세부 통제항목

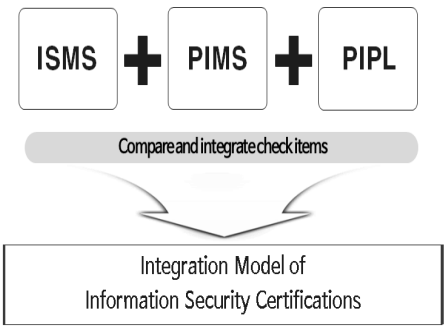


Fig. 1. Methodology and procedure of the study

Table 4. The deduction criteria on same, similar, and different item

Same item	- In case the object, direction and contents of check items are same - In case ISMS check items are included and the contents which aren't included in the items are other ISMS check items
Similar item	- In case the object and direction of check item are same, but one part of contents are different - In case of one part of ISMS check items - In case PIMS/PIPL check items include one part of ISMS check items
Different item	- In case there are no same and similar check items

을 비교하여 '동일', '유사', '다름'을 판단한다. ISMS는 국내 최초로 도입된 정보보호 관리체계 인증제도로 10년 이상 운영되었으며 PIMS, PIPL 또한 ISMS에서 파생되었기 때문에 ISMS를 정보보호 인증제도의 비교 및 통합의 중심축으로 설정하였다. '동일', '유사', '다름' 항목 도출 기준은 Table 4와 같이 결정하였으며, 각 세부 통제항목의 설명과 심사 지침 및 기준을 모두 참고하여 목적, 방향, 내용의

Table 5. Result of redundancy evaluation of information security certifications (Countermeasures)

ISMS			PIMS					PIPL					
Areas		Check items	same	similar	blank[1]	Different	Redundancy[2]	same	similar	blank	PIMS[3]	Different	Redundancy
ISMS	Information security policies	13	13	0	0	0	100%	6	3	4	0	0	69%
	Information security organization	7	7	0	0	3	100%	3	2	2	1	2	71%
	Security of external parties	4	3	0	1	0	75%	2	0	2	0	0	50%
	Information asset classification	7	6	0	1	0	86%	4	1	2	0	0	71%
	Education and training on information security	10	10	0	0	0	100%	5	1	4	0	0	60%
	Personnel security	11	10	1	0	0	100%	2	1	8	0	0	27%
	Physical security	21	13	0	8	4	62%	3	1	17	4	2	19%
	System development security	22	16	0	6	0	73%	11	0	11	0	3	50%
	Cryptography control	8	8	0	0	0	100%	3	1	4	0	0	50%
	Access control	46	44	0	2	5	96%	11	6	29	2	2	37%
	Operations security	56	41	0	15	5	73%	9	4	43	1	1	23%
	Intrusion incident handling	14	13	0	1	0	93%	3	2	9	0	0	36%
	IT disaster recovery planning	6	0	0	6	0	0%	0	0	6	0	0	0%
Total		225	184	1	40	17	82%	62	22	141	8	10	37%

Note: 1) In case there are no check items which can be reconciled.
2) The holding rate of same and similar items in overall check items
3) The second different items which are overlapped with the different item deducted firstly

Table 6. Result of redundancy evaluation of information security certifications (Lifecycle)

PIMS			PIPL				
Areas		Check items	same	similar	blank[1)]	Different	Redundancy[2)]
PIMS (lifecycle)	Collection of personal information	20	15	0	5	1	75%
	Use and provision of personal information	46	29	1	16	4	65%
	Management and destruction of personal information	16	7	2	7	0	56%
Total		84	51	3	28	5	64%

Note: 1) In case there are no check items which can be reconciled.
2) The holding rate of same and similar items in overall check items

일치 여부를 확인하였다. 1, 2차에서 도출된 '동일', '유사' 항목은 ISMS 세부 통제항목에 일치시키고, '다름' 항목은 ISMS에 추가하여 통합한다. 단, 1, 2차에서 도출된 '다름' 항목 중 중복되는 항목은 제외한다.

ISMS의 세부 통제항목을 기준으로 PIMS, PIPL의 '동일', '유사', '다름' 항목을 도출한 결과는 다음 Table 5와 같다. ISMS에 없는 PIMS의 생명주기 통제분야를 기준으로 PIPL과의 '동일', '유사', '다름' 항목도 도출하였다(Table 6참조). 먼저 정보보호대책 파트를 살펴보면 PIMS의 경우 5개의 통제분야가 ISMS와 100% 중복되었으며 'IT 재해복구'를 제외한 나머지 통제분야에서도 높은 중복비율을 보였다. PIPL은 상대적으로 낮은 중복비율을 보였는데 ISMS와의 세부 통제항목 수의 차이에서 기인한 것이다(참고: ISMS의 세부 통제항목 수는 253개, PIMS는 310개 그리고 PIPL은 155개임). PIMS의 생명주기 파트에서도 이러한 점을 감안한다면 상당히 높은 중복비율을 보인다고 할 수 있다.

최종적으로 도출된 32개의 새로운 세부 통제항목 중 ISMS에 추가되는 통제사항을 정리하면 Table 7과 같다(기존 ISMS 통제사항에 추가되는 세부 통제항목은 제외). 기존 ISMS에 32개의 새로운 세부 통제항목과 ISMS에 없는 PIMS의 생명주기 통제분야를 추가하여 정보보호 인증제도 통합모형을 도출하였다.

Table 7. Integration of information security certification systems

Areas		Additional control activities
Information security organization	Organizational system	(PIMS)Appointment of the employee responsible for and in charge of personal information by sections
	Role and responsibility	(PIMS)Report and communication system
Access control	Access control management	(PIMS)The responsibility of employee in charge of personal information
	Access authority management	(PIMS)Authority management of employee in charge of personal information
Operations security	Medium security	(PIPL)Keeping of storage media
	Log management and monitoring	(PIMS)Storage of access records of personal information system
		(PIMS)Designation of output purpose of personal information and protection measure and personal information masking

IV. 통합모형 검증

4.1 설문 대상

본 연구에서는 정보보호 관리체계 통합모형의 적정성을 검증하고 금융권 정보보호 관리체계 인증의 필요성을 밝히기 위해 금융 산업의 업무적 특성을 잘 이해하는 금융 산업에 직접 종사하는 IT·정보보호 전문가, 정보보호 관리체계 인증 컨설팅 경험이 있는 정보보호 컨설턴트 또는 인증심사원을 대상으로 설문조사를 하였다. Table 8은 응답자의 일반적 특성을 나타낸 것이다.

4.2 설문 결과

ISMS에 없는 PIMS, PIPL의 통제사항에 대해 응답자가 금융기관 정보보호 관리수준 평가 시 느끼는 필요 정도를 5점 척도(1: 전혀 필요하지 않다,

Table 8. Descriptive statistics for the respondents

Type		Frequency	Percentage
Type of industry	Public financial enterprise	1	4.8
	Insurance	1	4.8
	Credit card	4	19.0
	Security consulting company	6	28.6
	ISMS auditor	4	19.0
	etc.	5	23.8
Number of employees	Under 100	9	42.9
	100~300	3	14.3
	300~1,000	3	14.3
	1,000~5,000	4	19.0
	5,000~10,000	1	4.8
	Over 10,000	1	4.8
Career	1~5 years	2	9.5
	5~10 years	5	23.8
	10~15 years	9	42.9
	Over 15 years	5	23.8
Certifications acquisition or not (Multiple responses possible)	K-ISMS	8	29.6
	PIMS	3	11.1
	PIPL	0	0.0
	ISO27001	4	14.8
	Not acquired	12	44.4
Ought to acquire ISMS or not	Yes	4	19.0
	No	17	81.0
Total		21	100.0

2: 필요하지 않다, 3: 보통이다, 4: 필요하다, 5: 매우 필요하다)로 평가하도록 하였다. 응답자의 평균값이 3.0 이상이면 통제항목의 적정성을 충족하는 것으로 보았다.

Table 9는 정보보호 관리체계 통합모형에서 ISMS에 추가된 7개의 통제사항에 대한 설문 결과의 평균값이다. 개인정보취급자의 권한관리 분야가 4.57로 가장 높았고, 그다음으로는 개인정보처리시스템의 접속기록 저장분야 4.52, 개인정보취급자 책임 분야 4.38 순으로 나타나고 있다. 상대적으로 낮은 항목은 저장매체의 보관 분야 3.64, 개인정보 출력용도의 특정 보호대책 분야 3.57 등을 들 수 있다. 응답 결과의 평균값은 모두 3.0 이상으로 정보보호 관리체계 통합모형의 적정성을 충족하는 것으로

Table 9. Result of survey on integration model of information security certification systems

Questionnaire items	Mean
1. Appointment of the employee responsible for and in charge of personal information by sections	4.38
2. Report and communication system	4.57
3. The responsibility of employee in charge of personal information	4.05
4. Authority management of employee in charge of personal information	4.05
5. Keeping of storage media	3.57
6. Storage of access records of personal information system	4.52
7. Designation of output purpose of personal information and protection measure and personal information masking	3.67

나타났다. 금융권 정보보호 관리체계 인증 개발을 위해서는 ISMS에 없는 PIMS, PIPL 통제사항을 추가하여 통합하는 단계가 먼저 필요함을 알 수 있다.

추가적으로 ISMS 인증제도가 국내 금융 산업의 특성을 충분히 반영하고 있는지에 대한 설문을 실시하였다. Fig. 2는 응답결과를 나타낸 것이며, '보통이다' 또는 '그렇지 않다'라고 대답한 응답자는 총 19명으로 90%를 차지하였다.

Fig. 3은 국내 금융 산업의 특성이 ISMS 인증제도에 충분히 반영되어 있지 않았다고 생각하는 이유에 대한 응답 결과의 평균이다. '금융 관련 법률에 대한 내용을 ISMS에 반영하고 있지 않다'라는 답변이 3.52로 가장 높았다.

Table 10은 금융권 정보보호 관리체계 도입 시, 더 강화해야 할 ISMS 정보보호대책의 통제분야(13

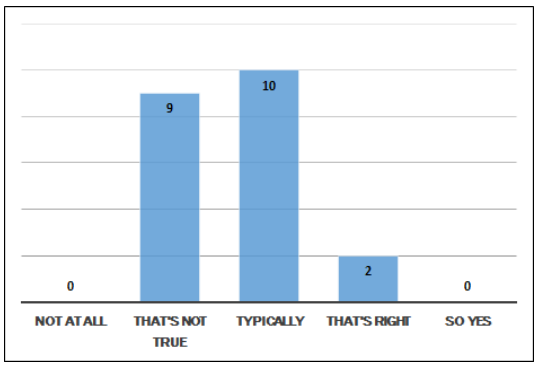
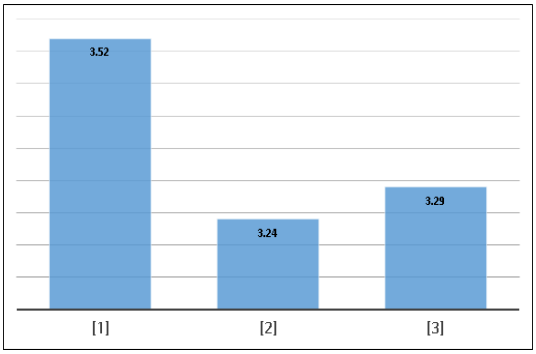


Fig. 2. Opinion on how far ISMS reflects the characteristic of financial industry



Note: [1]As the contents for financial related laws were not reflected on ISMS;[2] As required items on the life cycle which check legal standard on the generation through destruction of personal information are not reflected;[3]As the required items on the protection of information was well reflected on the current criteria, but they don't come out clearly

Fig. 3. Reason to think ISMS does not reflect the characteristic of financial industry

개 분야)에 대한 설문 결과이며 평균값으로 중요도 순위를 정하였다. 가장 높은 평균값을 보인 통제분야는 '접근통제'였으며, 가장 낮은 평균값을 보인 통제분야는 '정보보호 정책' 이었다.

마지막으로 설문 응답자에게 금융권 정보보호 관리체계 도입 시 고려사항에 대해 자유롭게 의견을 제시하도록 하였다. 금융권의 경우 아직 온라인만큼 오프라인에서 필요한 요구사항들이 상당부분 존재하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 근거로 한 ISMS만으로는 모두 충족할 수 없으므로 금융관련 법률 반영이 필요하다는 의견이 다수였다.

Table 10. Opinion on degree of strengthening ISMS areas when introducing information security management system certification for the financial sector

Areas	Mean	Standard Deviation	priority of impor-tance
Information security policies	3.38	0.21	10
Information security organization	3.95	0.19	5
Security of external parties	4.38	0.18	2
Information asset classification	3.57	0.21	7
Education and training on information security	3.52	0.21	8
Personnel security	3.86	0.21	6
Physical security	3.48	0.25	9
System development security	4.38	0.20	2
Cryptography control	4.19	0.16	4
Access control	4.52	0.13	1
Operations security	4.19	0.15	4
Intrusion incident handling	4.19	0.16	4
IT disaster recovery planning	4.24	0.17	3

V. 결 론

그동안 기업에 부담과 혼란을 주었던 PIMS, PIPL이 개인정보보호 관리체계 인증(PIMS)으로 일원화되었다(2016.1.1. 시행). 이에 따라 기업 혼란 해소뿐만 아니라 인증 신청기관 유형별로 심사항목을 차등화해 인증취득 소요기간 단축, 수수료 절감 등의 효과가 있을 것으로 예상되고 있다. 이처럼 단계적 추진을 통해 최종적으로는 ISMS와 PIMS의 통합이 가능할 것으로 보인다.

그러나 PIMS는 ISMS와 달리 인증 취득이 의무사항이 아니며, 여전히 ISMS와 중복되는 통제항목이 존재하여 (통합)PIMS 그 자체의 효과와 실효성 여부는 지켜봐야 할 것이다.

본 연구에서는 유사성을 지닌 정보보호 인증제도의 통합으로 정보보호 관리 업무의 효율성 높이고 금융권에 특화된 정보보호 관리체계 인증모형의 개발방향을 제안하고자 하였다.

정보보호 인증제도 통합 결과는 다음과 같다. ISMS를 기준으로 하여 PIMS와 PIPL을 일치시켜 기존 ISMS에 추가되는 32개의 새로운 세부 통제항목 32개를 도출하였으며, PIMS의 생명주기 통제분야를 추가하여 정보보호 인증제도 통합모형을 도출하였다. ISMS에 새롭게 추가되는 통제사항에 대해서 전문가를 대상으로 한 설문을 통해 금융기관 정보보호 관리수준 평가 시 통합 모형의 적정성을 검증할 수 있었다. 또한 ISMS 인증의 국내 금융 산업 특성

반영 정도에 관한 의견을 통해 금융권 정보보호 관리체계 인증의 필요성을 밝힐 수 있었으며, ISMS 인증이 금융 산업 특성을 반영하고 있지 않다고 생각하는 이유에 대한 답변에서 앞으로 어떻게 금융권 정보보호 관리체계 인증모형이 개발되어야 할지 방향성을 확인할 수 있었다.

본 연구를 보완하기 위해서는 금융 IT, 정보보호 관련 법률을 검토하여 앞서 도출한 통합모형의 통제항목과 일치시키는 작업을 통해 실제 금융권을 대상으로 한 정보보호 관리체계 인증모형을 개발해보는 후속연구가 필요하다. 또한 ISO/IEC 27001:2005와 비교하여 금융서비스 조직에 맞춰 수정, 보완된 ISO/IEC 27015:2012의 통제항목이 속한 통제분야와 금융권 정보보호 관리체계 도입 시 ISMS 통제분야 강화 정도에 관한 설문 결과 높은 중요도 순위를 보인 통제분야를 고려하여 개발되어야 할 것이다.

References

[1] DigitalDaily, "'PIMS, PIPL', integration of the similar personal information security certifications," 2015.11.15.

[2] Eun-yeop Park, Jin-won Choi, and Tae-hee Cho, "A case study on building personal information management System Certification," Review of The Korea Institute of information Security & Cryptology, 21(5), pp. 27-36, Aug. 2011.

[3] F. Gregory Hayden and Kurt Stephenson, "Overlap of organizations: corporate transorganization and Veblen's thesis on higher education," Journal of Economic Issues, 24(1), pp. 53-85, Mar. 1992.

[4] Hyeon-seon Kang, "An analysis of information security management system and certification standard for information security," Journal of Security Engineering, 11(6), pp. 455-468, Dec. 2014.

[5] ISO/IEC27001, Information technology- Security techniques- Information security management systems- Requirements, 2005.

[6] ISO/IEC TR 27015, Information technology-Security techniques-Information security management guidelines for financial services, 2012.

[7] Jung-duk Kim, "Standardization of information security management," Review of KIISC, 21(2), pp. 19-22, Apr. 2011.

[8] Jeong-hae Kim, "A study on the reform of the overlapping regulation in the industrial safety sector," Korean Society and Public Administration, 15(1), pp. 211-233, May. 2004.

[9] Korea Internet and Security Agency, Information Security Management System(ISMS) certification guideline, 2013.

[10] Korea Internet and Security Agency, Personal Information Management System(PIMS) certification guideline, 2010.

[11] Myung-seong Yim, Tae-seog Jeong and Jung-min Lee, "A suggestion for information security awareness of finance firms," Journal of Security Engineering, 11(6), pp. 479-798, Dec. 2014.

[12] National Information Society Agency, Personal Information Protection Level(PIPL) guideline, 2015.

[13] National IT Industry Promotion Agency, Domestic and international research trends on information security management system certification, 2011.

[14] Sung-ju Park and Jong-in Lim, "A study on the development of SRI(Security Risk Indicator)-based monitoring system to prevent the leakage of personally identifiable information," Journal of the Korea Institute of Information Security and Cryptology, 22(3) pp. 637-644, Jun. 2012.

[15] The Boannews, "Visualization of integrating the information security certifications...what are the priorities?," 2014.08.11.

[16] Yong-hun Kim, "Inter-ministration com-

petition in government public key infra-structure," Korean Republic Administration Review, 34(3), pp. 93-109, Nov. 2000.
[17] Yeong-jin Shin, "A study on technological protection measures improvement for personal information security," The Journal of Public Policy and Governance, 8(1), pp. 69-103, Jun. 2014.

〈저자소개〉

오 은 (Eun Oh) 정회원
2013년 8월: 경희대학교 경제학과 졸업
2016년 2월: 충북대학교 정보보호경영학과 석사
2016년 3월~현재: 조이 보안컨설팅 정보보호컨설턴트
〈관심분야〉 금융보안, 정보보호관리체계 인증, 정보보호정책

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수 및 학과장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정

조 태 희 (Tae-Hee Cho) 정회원
1998년 11월: RoyalHolloway, Univ. of London 정보보호학과 석사
1999년 7월~2001년 3월: LG전자 연구원
2001년 4월~2008년 1월: 한국정보보호진흥원, 선임연구원
2008년 1월~2012년 10월: NHN(주), 정보보안팀장
2012년 11월~현재: 조이보안컨설팅 이사, 충북대학교 정보보호경영전공 겸임교수, ISMS 선임심사원, PIMS 심사원, 정보보호 준비도 선임평가사
〈관심분야〉 (개인)정보보호관리체계 인증, 위험관리, 정보보호정책, 클라우드 보안