국내환경에 적합한 정보보호관리체계 평가 방법론에 대한 연구

Study on Information Security Management System Evaluation Methodology

홍성혁*, 박종혁*, 서정택**

Sung-Hyuk Hong*, Jong Hyuk Park* and Jungtaek Seo**

요 약

정보화 사회가 진행되면서 오늘날 정보의 가치가 기업의 발전 및 연속성을 결정할 수 있는 중요한 요소로 떠오르고 있으며 이러한 중요한 정보를 보호 및 관리하는 정보보호관리체계에 대한 중요성 또한 대두되고 있다. 본 논문에서는 정보보호관리체계 평가방법론을 연구하기위해 국내·외 정보보호관리체계 평가방법론에 대하여 관리 지침, 평가 기준 산정 방법, 통제 항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분 등을 기준으로 국·내외 정보보호관리체계를 비교·분석하며 국내환경에 적합한 정보보호관리체계 평가 방법론을 제안한다.

Abstract

These days, along with the information society, the value of information has emerged as a powerful factor for a company's development and sustainability, and therefore, the importance of the Information Security and Management System (ISMS) has emerged and become an integral part of all areas of business. In this paper, ISMS evaluation methods from around the world are compared and analyzed with the standards of various management guidelines, definitions, management of threats and vulnerability, approaches to result calculations, and the evaluation calculation indexes for domestic to propose the best method to evaluate the Information Security Management System that will fit the domestic environment.

Key words : Information Security Management System, ISMS, ISMS Evaluation Methodology

I. 서 론

정보통신망의 발전과 함께, 사회 전반의 정보화가 진행되면서 정부, 공공기관 및 민간기관 등 국가 사회 각 분야의 업무들이 오프라인 환경에서 온라인 환경으로 전환되었지만 보안 대책 미비로 인한 해킹이나 바이러스 등에 의한 보안 위협도 증가하였다. 또한 정보의 가치가 기업의 발전 및 연속성을 결정할 수 있는 중요한 요소로 대두 되었지만 단순히 기술적 대응만으로는 기업의 정보보호 관련 사고를 줄일 수 없었다. 또한 보안 사고의 가장 큰 비율이 내부자의 기밀 유출에서 발생함에 따라, 기업 내부의 보안 정

* 경남대학교 컴퓨터공학부 (Department of Computer Science and Engineering, Kyungnam University)
** 한국전자통신원 부설연구소 (The Attached Institute of ETRI)
· 교신저자 (Corresponding author) : 박종혁
· 투고일자 : 2008년 8월 1일
· 심사(수정)일자 : 2008년 8월 4일 (수정일자 : 2008년 8월 18일)
· 게재일자 : 2008년 8월 30일

책과 관리 측면의 중요성이 부각되어 정보보호관리체계 (ISMS: Information Security Management System)의 중요성이 대두되고 있다. ISMS의 국내 활성화를 위한 다양한 노력이 진행되고 있지만, 표준화된 평가 방법론이 존재하지 않고, 국제 표준과 국내 인증제도 간의 연계가 이루어지지 않는 문제로 인하여 ISMS가 활성화 되지 않고 있다.

본 논문에서는 국·내외 정보보호관리체계에 대하여 관리 지침, 평가 기준 산정 방법, 통제 항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분 등을 기준으로 국·내외 정보보호관리체계를 비교·분석하며 국내환경에 적합한 정보보호관리체계 평가 방법론을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 국·내외 정보보호관리체계 연구동향에 대해 살펴보며, 3장에서는 정보보호관리체계 평가방법론 연구를 위한 고려사항에 대해 논의한다. 4장에서는 정보보호관리체계 평가방법론에 대해 비교·분석하며, 5장에서 정보보호관리체계 평가방법론 연구 방안에 대해 제안하고, 6장에서 결론 및 향후 연구계획을 제시한다.

Ⅱ. 국·내외 정보보호관리체계 연구동향

ISMS는 조직의 전반적인 관리시스템의 일부로서 비즈니스 위험에 기반하여 정보보호를 계획, 구현, 운영, 검토 및 개선시키기 위해 조직체계 및 정책, 정보보호 프로세스 및 절차, 정보보호통제 등으로 구성된 관리체계이다.

ISMS의 요구사항을 포함하는 ISO 27001 (BS 7799 part 2: 2002 수정판)과 ISMS의 기초적인 통제수단을 수록한 ISO 27002 (ISO 17799:2005)가 국제표준화에 성공하여 최근 전세계적으로 ISMS에 대한 인증 노력이 빠르게 확산되고 있다 [1, 2, 3].

본 장에서는 BS7799, SSE-CMM, KISA-ISMS, NIST-FISMA 등 국·내외 ISMS의 연구 동향에 대해 간략히 살펴본다.

2-1 BS7799

BS7799 는 영국 BSI (British Standard Institute)에서 정보보호 관리를 위한 표준화된 실무 규약으로서 1995년 처음 개발되었으며, 1998년에는 실무규약은 Part 1 (code of practice for information security management), 인증요건은 Part 2 (Specification for information security management)로 만들어졌다. 1999년 BS 7799 Part 2는 ISMS인증을 위한 규격으로 사용되었고, 2002년 9월 ISO 9001 및 ISO 14001 등의 관리시스템과 규격의 조화를 위하여 개정되었다. 2000년에는 Part 1이 ISO/IEC JTC 1/SC27 WG1을 통하여 ISO 17799로 제정되었다. ISO는 ISMS에 대한 국제표준화 요구에 대응하여 BS 7799 Part 2: 2002년 버전을 약간의 수정을 거쳐 국제표준 (ISO 27001)으로서 제정하였다 [2][4]. BS7799 Part 1에서는 10개의 관리 통제 영역과 36개 통제 목적, 127개의 보안 지침을 제공하며, BS7799 Part 2에서는 ISMS에 대한 규격으로 ISMS의 문서화 수립·실행에 대한 요구사항과 개별 조직의 필요성에 따라 실행될 수 있는 정보보호관리 요건을 규정하고 있다. BS7799 Part 1과 2는 노르웨이, 네덜란드, 브라질, 스웨덴, 아이슬란드, 아일랜드, 핀란드, 호주, 뉴질랜드 등에서 국가표준으로 사용하고 있다 [5][6].

2-2 SSE-CMM

Capability Maturity Model (CMM)은 미국 카네기멜론 대학의 소프트웨어공학연구소 Software Engineering Institute(SEI) 주관으로 개발한 능력성숙도 모델로서 미국, 유럽, 인도 및 호주 등을 중심으로 43개국에서 적용되어 인증을 받고있다. 초기 CMM은 품질 및 공정 개념을 소프트웨어 개발과 유지보수에 적용한 모델이었으나 현재는 CMM for S/W (SW-CMM), S/W Acquisition CMM (SA-CMM), Systems Engineering CMM (SE-CMM), Integrated Product Management CMM (IPM-CMM), People CMM (P-CMM)의 5가지 모델로 세분화 된다. SSE-CMM은 SE (Systems Engineering)-CMM을 기반으로 하며 1996년 10월에 Version 1.0, 1999년 4월에 Version 2.0이 제안되었다. SSE-CMM은 다섯 단계의 수준을 포

함하고 있으며 공통 요소(common features)들로 분할된다 [9][10].

2-3 KISA-ISMS 인증 제도

KISA-ISMS 인증 제도는 정보통신망이용촉진 및 정보보호 등에 관한법률' (이하'망법') 제47조에 의해 정립되었으며, 조직내 정보자산의 보호를 위한 관리체계가 정통부에서 고시한 정보보호관리체계의 인증심사 기준에 적합한지를 제 3자가 객관적이고 독립적으로 평가하여 적합성 여부를 인증해 주는 것이다. KISA-ISMS 인증제도의 목적은 종합적 관리체계수립을 지원하고, 정보보호 관리에 대한 인식을 제고하여 보호되어야할 정보통신망 및 정보자산의 안전, 신뢰성을 강화하고 국제적 신뢰도를 향상시키기 위한 것이다.

KISA-ISMS 인증대상은 2006년까지는 정보통신서비스와 관련된 사업자였으나, 2007년 정보보호관리체계를 수립·운영하고 있는 자는 모두 인증을 받을 수 있도록 개정되었다. KISA-ISMS 인증기준은 ISO/IEC 27001 국제표준을 모두 포함하고 있고, 이에 더하여, 국내 상황에 맞게 개인정보보호, 침해사고예방, 암호화, 전자거래 등의 보안요건을 강화하였으며, 국내 TTA 표준 (표준번호 TTAS.KO-12.0036)으로 2006년 12월 개·제정 되었으며 정보보호 관리과정, 문서화 요구사항 및 정보보호대책등 3가지 요구사항으로 구성된다 [7][8].

2-4 NIST-FISMA

2002년에 연방 정보보호 관리법으로 제정된 미국의 Federal Information Security Management Act (FISMA)는 전자정부법 중 3편에 속하며 FISMA 구현 프로젝트는 2003년부터 정부기관의 운영과 자산을 지원하는 정보와 정보시스템 보호를 위한 핵심 보안 표준과 가이드라인의 개발을 목표로 연구가 실시되었다. FISMA는 인증을 받지는 않지만, 중요 기반구조 보호 (Critical Infrastructure Protection: CIP)를 개선하기 위한 목적으로 만들어진 NIST 내의 컴퓨터 보안 전문가 지원팀(Computer Security Expert Assist Team: CSEAT)에서 활용되며, 17종의 보안통제(Control)를 관리적·운영적·기술적 통제로 분류한다 [11][12].

Ⅲ. 정보보호관리체계 평가방법론 연구를 위한 고려사항

정보보호관리체계의 국내 활성화를 위한 다양한 노력이 진행되고 있지만, 표준화된 평가 방법론이 존재하지 않으며, 국제 표준과 국내 인증제도 간의 연계가 이루어지지 않는 문제가 남아 있다. 국내 방법론 중 대표적인 한국정보보호진흥원 (KISA)의 정보보호관리체계는 인증 취득에 따른 홍보 효과가 부족하며, KISA의 인증을 받더라도 ISO 27001 인증을 받는 것이 아니기 때문에 국제 인증을 필요로하는 기업은 다시 ISO의 인증을 받아야 하는 불편성과 중복성이 존재한다. 또한, 평가 방법론 개발, 평가 수행 기관, 심사원 양성, 인증 혜택 등 국내 모든 기능을 KISA에서 담당하므로 인증의 신뢰성이 저하될수 있으며, 개발 당시의 기대 효과보다 활성화가 이루어지지 않고 있는 상황이다 [7][8]. 따라서 국제 표준과 국내 인증제도 간의 연계와 국내 실정에 적합한 정보보호관리체계 평가를 위한 방법론의 연구가 필요하다.

국내 환경에 적합한 정보보호관리체계 평가방법론을 연구하기 위해서는, 먼저 각 평가 방법론에 대하여 관리 지침, 위협과 취약성의 정의와 처리, 등급 구분, 결과 산정 접근법, 평가 산정 척도 등에 대해 비교하고 이에 대해 적절한 방법론을 도출해내야 한다. 각 방법론들은 기본 개념, 방법론의 개발 철학, 적용대상 등이 상이함으로 수평적인 비교가 엄밀히 이루어질 수 없지만, 유사점을 개괄적인 비교를 통해 평가 방법론을 도출해야 한다.

Ⅳ. 정보보호관리체계 평가방법론 비교 분석

본 장에서는 관리 지침, 평가 기준 산정 방법, 통제항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분 등을 기준으로 국·내외 정보보호관리체계에 대해 비교·분석한다.

4-1 관리 지침

각각의 정보보호관리체계 방법론은 개발된 국가 조직 관리체계에 적합하도록 문화적, 법적, 제도적인 환경을 고려하여 개발되었다. 따라서 방법론의 개발 목적과 전체적인 내용은 동일하더라도 관리 지침의 구성은 다른 방식을 취하고 있다. 다음 표는 이러한 관리 지침들을 비교한 내용을 보여준다. SSE-CMM은 관리 지침이 아닌 보안 공정 분야로 정의되지만, BS 7799를 비롯한 ISMS와 서로 연관성을 지니고 있음을 볼 수 있다. SSE-CMM과 관리 지침의 가장 큰 차이점은 활용 목적에 있다. 관리 지침은 사용자가 보안 정책을 수립하는데 도움을 주고 적절한 방안을 확인하는데 초점을 두지만, SSE-CMM의 주요 목적은 조직에 의해서 구현된 보안 공정의 성숙도 수준을 평가하는 것이다. 이러한 관점에서 ISMS의 관리 지

표 1. SSE-CMM 보안 공정과 정보보호관리체계 관리 지침 비교
Table 1. Comparisons of the Management Guidelines of SSE-CMM Security Process and ISMS

SSE-CMM	GMITS	NIST 편람	BS7799
PA01-보안통제를 관리한다	17절, 후속조치	10장, 직원/사용자 이슈 14장, 컴퓨터 지원 운영에서의 보안 고려사항	5절, 인적 보안 6절, 통신 및 운영 관리 8절, 시스템 개발 및 유지보수
PA02-영향을 평가한다	10절, 위험분석 전략 대안 : GMITS 3부	7장, 컴퓨터 보안 위험 관리	개요
PA03-보안위험을 평가한다	10절, 위험분석 전략 대안 : GMITS 3부	7장, 컴퓨터 보안 위험 관리	개요
PA04-위협을 평가한다	10절, 위험분석 전략 대안 : GMITS 3부	7장, 컴퓨터 보안위험 관리 4장, 보편적인 위협	개요
PA05-취약성을 평가한다	10절, 위험분석 전략 대안 : GMITS 3부	7장, 컴퓨터 보안 위험 관리	개요
PA06-보증논거를 구축한다	14절, 보안대책 구현	9장, 보증	10절, 준거성
PA07-보안을 조정한다	13절, IT 보안 계획	6장, 컴퓨터 보안 프로그램 관리	2절, 보안 조직 6절, 통신 및 운영 관리
PA08-보안상태를 감시한다	17절, 후속 조치	18장, 감사 증적 12장, 컴퓨터 보안 사고 처리	10절, 준거성
PA09-보안입력물을 제공한다	8절, IT 보안 정책 11절, IT 보안 권고안 12절, IT 시스템 보안 정책 13절, IT 보안 계획 15절, 보안 인식	5장, 컴퓨터 보안 정책 13장, 인식, 교육 및 훈련 15장, 물리적 및 환경적 보안	1절, 보안 정책 3절, 자산 분류 및 통제 5절, 물리적 및 환경적 보안
PA10-보안필요성을 명시한다	8절, IT 보안 정책 11절, IT 보안 권고안 12절, IT 시스템 보안 정책 13절, IT 보안 계획	8장, 컴퓨터시스템 수명주기에서의 보안 및 계획수립 11장, 비상사태 및 재해에 대한 준비 16장, 식별 및 인증 17장, 논리적 접근통제 19장, 암호	1절, 보안 정책 7절, 접근 통제 8절, 시스템 개발 및 유지보수 9절, 업무 지속성 계획 수립
PA11-보안을 검증하고 확인한다	17절, 후속 조치 14절, 보안대책 구현	8장, 컴퓨터 시스템 수명주기에서의 보안 및 계획수립 18장, 감사 증적	10절, 준거성

침과 SSE-CMM은 상호 보완적인 성격을 지닌다 (표1 참조).

4-2 관리 지침

평가 기준의 선택에 있어서 평가 대상을 구체적으로 어떻게 설정하는지에 따라 다음과 같이 상향식 접근법과 하향식 접근법으로 구분할 수 있다. 상향식 접근법은 개별적인 세부 통제대책의 적절성을 평가하고 이들을 종합함으로써 전체 정보보호 수준을 결정하는 방법이고, 하향식 접근법은 조직의 정보보호 필요성에서 출발하여 정보보호 정책과 요구사항을 도출하고, 이를 충족시킬 수 있는 정보보호 대책들이 얼마나 잘 구현되어 운영되고 있는지를 평가하는 방법이다. SSE-CMM는 상향식 접근법이며 BS 7799와 SSAG는 하향식 접근방법이다.

4-3 통제 항목과 점검 분야

정보보호관리체계의 통제 항목과 각 상위 분야는 다음 표와 같이 항목의 개수와 분야가 다양하다. 각각의 방법론에 대해 비교해보면, BS 7799는 통제 항목과 분야를 비교적으로 체계적으로 분류하였지만 SSE-CMM는 관리 분야를 기본, 프로젝트, 조직과 같이 단순히 3개로 분류하였다 (표2 참조).

4-4 위험 분석 측정 범위

위험 분석 측정 범위는 각각의 측정 대상 및 구간 등이 다르므로, 서로 비교해서 평균값을 기준으로 각 특장점을 취합할 필요가 있다. 따라서 BS 7799, SSE-CMM, NIST's SSAG 이외에 위험 관리와 관련된 평가방법론을 추가해서 데이터를 비교하였다. 추가한 위험관리 평가방법론은 NIST 보안 관리 지침 SP-800-30, 캐나다의 위험관리 기준인 CSE, ETRI 의 위험분석관리 도구 PRAM, 보안관리표준(GMITS) 중 네트워크 보안 관리 지침인 ISO-13335-5이다. 이러한 각각의 방법론에서 사용하능 위험 분석의 측정 대상에 대한 측정치 구간 범위는 다음과 같다. 표 3은 자산, 표 4는 위협, 표 5는 취약성, 표 6은 위험에 대한 구간 범위를 나타낸다.

표 3. 자산에 대한 측정 대상별 측정 범위
Table 3. Measurement Scope for Assets by Object

자산		
기준	측정 대상	구간
BS-7799	자산가치	5
CSE	자산민감도	5
ISO-13335-5	자산가치	5
ETRI-PRAM	자산가용성, 금전손실, 법적 책임	5

표 2. 정보보호관리체계 평가방법론의 각 통제 항목 비교
Table 2. Comparisons of the Control Items from ISMS evaluation methods

평가 방법론	통제 항목 분류				분야
	클래스	패밀리	컴포넌트	엘리먼트	
BS 7799	10	36	127	550	정책, 조직, 자산, 인사, 물리/환경, 통신/운영, 접근통제, 개발/유지보수, 연속성 준수
한국 정보보호관리기준	12	-	130	-	정책, 조직, 아웃소싱/제3자 접근, 자산, 인사, 교육/훈련, 접근통제 ,물리적 운영 개발, 연속성, 사고대응/복구 준수
GMIT	2	12	63	N/A	관리/정책, 준수, 사건 처리, 인사, 웅영, 연속성, 식별/인증, 접근통제/감사, 악의적 코드 보호, 망관리 암호
BSI IT Baseline	6	-	544	N/A	기반 구조, 조직 ,인사, H/W, S/W, 통신, 비상계획
SSE-CMM	3	22	128	744	기본, 프로젝트, 조직

표 4. 위협에 대한 측정 대상별 측정 범위
Table 4. Measurement Scope for Threats by Object

위협		
기준	측정 대상	구간
BS-7799	위협 수준	3
	위협의 빈도	5
CSE	위협원 능력, 위협원의 동기	3
	위협원 등급	5
ETRI-PRAM	위협 발생 가능성	5
	위협 심각성	3
	위협 수준 (1)	3
	위협 수준 (2)	7

표 5. 취약성에 대한 측정 대상별 측정 범위
Table 5. Measurement Scope for vulnerability by Object

취약성		
기준	측정 대상	구간
BS-7799	취약성 평가	3
	취약성 수준	5
CSE	취약성의 심각성, 취약서의 노출성	3
	취약성 수준	5
ETRI-PRAM	취약성 수준	3
NIST-SSAG	취약성 수준	3
ISO-13333-5	취약성 수준	3

표 6. 위험에 대한 측정 대상별 측정 범위
Table 6. Measurement Scope for Risks by Object

위험		
기준	측정 대상	구간
BS-7799	위험 수준	8
ETRI-PRAM	위험 수준	9
NIST-보안관리	위험 수준	3
ISO-13333-5	위험 수준	9

4-5 위험 분석 프로세스 모델

위험 관리에서 정보시스템의 보호가 필요한 항목을 자산 (A)이라 부르고, 자산에 가해질 수 있는 공격을 위협 (T), 이러한 위협의 대상이 되는 취약성 (V) 그리고 결과적으로 이러한 위험 (R)은 이들의 확률적 함수에 의해 수치적으로 계산된다. 이러한 일련의 과정을 위험 평가 프로세스라 정의한다. 각 평가방법론은 각각 위험을 평가할 수 있는 프로세스 모델이 있으며 서로 다른 특징을 갖는다 (표7 참조).

표 7. 위험 프로세스 모델과 ISMS
Table 7. Risk Process Models and ISMS

모델	해당 평가방법론	특징
AVR: 자산 → 취약성 → 위험	ISO 13335-3	위협 없음
ATVR: 자산 → 위협→ 취약성 → 위험	FIPS-65, 191, PRAM	
ATR: 자산 → 위협 → 위험	CSE	취약성 없음
TVR: 위협 → 취약성 → 위험	NISTSP-800-30, SSE-CMM	자산 없음
자료없음	BS 7799	N/A

4-6 등급 구분

NIST-SSAG는 ISMS의 구축을 위한 단계적 측면을 강조한다. 세부적인 수준을 기준으로 살펴보면 수준 1에서 수준 3까지는 보안절차와 통제의 도출 과정을 대표하고 수준 4와 5는 ISMS의 성숙도를 나타낸다. SSE-CMM의 경우는 조직에서 수행되는 비즈니스 프로세스들이 어떤 형태로 존재한다는 것을 전제로, 각 프로세스가 얼마나 합리적으로 수행되느냐에 따라서 조직의 능력 수준을 구분한다. BS7799는 조직의 수준을 여러 단계로 구분하지 않고 적합/부적합으로 구분한다 (표8 참조).

표 8. 평가 방법론의 등급 구분 비교
Table 8. Comparisons of ISMS evaluation methods

NIST-SSAG	SSE-CMM	BS 7799
수준 1: 문서화된 정책	수준 1: 비공식적으로 수행됨	부적합
수준 2: 문서화된 절차		

수준 3: 구현된 절차와 통제	수준 2: 계획되고 추적된	적합
수준 4: 시험되고 평가된 절차와 통제	수준 3: 잘 정의됨	
	수준 4: 계량적으로 통제됨	
수준 5: 완전히 통합된 절차와 통제	수준 5: 지속적으로 향상됨	

Ⅴ. 정보보호관리체계 평가방법론 연구 방안

국내 환경에 적합한 정보보호관리체계 평가 방법론을 개발하기 위해서 국제 표준 BS 7799 (ISO/IEC 27000X)를 기반으로 하며, 세부적인 평가 방법은 SSE-CMM과 같은 소프트웨어 공학 및 보안 공학 관점에서 등급을 평가하는 기존의 평가 방법론의 장단점을 서로 상호보완해주는 표준화된 평가방법론이 필요하다. 따라서 본 장에서는 Ⅲ장에서 비교·분석한 연구를 바탕으로 관리 지침, 평가기준 산정 방법, 통제 항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분에 대해 국내환경에 적합한 정보보호관리체계 평가 방법론을 제안한다.

관리 지침은 BS 7799의 대상 기관에 정책 수립이 편리한 점과 SSE-CMM의 체계적인 평가 방법을 상호 보완한 지침이 가장 효과적이라 판단된다.

평가기준 산정 방법은 계속해서 변화하고 발전해 가는 보안 위협에 대처하기 위해서는 각각의 세부 통제 항목에 대한 정보보호 대책과 관리를 실시하는 상향식 접근법이 필요하며, 관리적 측면에서는 BS 7799의 하향식 접근법이 필요하다고 판단된다.

통제 항목과 각 평가 분야는 BS 7799와 같은 정책중심의 표준화를 접근법이 필요하다고 판단된다. 각각의 방법론에 대해 비교해보면, BS 7799 는 통제 항목과 분야를 비교적으로 체계적으로 분류하였지만 SSE-CMM의 경우는 기본, 프로젝트, 조직과 같이 단순히 3개로 분류하였다.

위험 분석 측정 범위는 대부분 평가 방법론은 동일한 범위를 가지는 경우가 있으므로, 각 평가 방법론의 구간을 평균/통일화하고, 측정 대상의 명칭의 통일과 속성을 표준화하는 방안이 필요하다.

위험 분석 프로세스 모델은 FIPS-65, 191, ETRI-PRAM과 같이 일반적인 위험관리 모델이 모두 적용된 자산 → 위협→ 취약성 → 위험 프로세스가 좀 더 체계적이라 판단된다. SSE-CMM의 경우 위협 → 취약성 → 위험에서 자산에 대한 항목이 없어, 기업의 영업활동에 꼭 필요한 서버 시스템의 가치나, 기업 비밀 연구 자료 등과 같이 특정 통제 항목에 대한 평가가 불가능하다. 또한 BS 7799의 경우는 위험 프로세스 모델에 대한 언급 자체가 없다.

등급 구분은 SSE-CMM 이나 NIST's SSAG 등과 같이 항목별 등급산출 방법이 효과적이라 판단된다. BS 7799의 이분법적인 방법은 대상 기관의 평가를 일목요연하고 정확하게 판별 가능하나, 부적합 평가를 받은 대상 기관은 통과하지 못한 통제 항목을 체계적으로 관리 받기는 힘들다. 반면, SSE-CMM과 NIST's SSAG 등과 같은 각 항목별 등급산출 방법은 보안 공정에 대한 평가 수준을 산출하고 각각에 대해, 등급을 판정하며, 부적합 판정을 받은 기업에 대한 사후관리를 순환적으로 할 수 있다.

Ⅵ. 결 론

본 논문에서는 BS7799, KISA-ISMS, NIST-FISMA 등 국·내외 정보보호관리체계 연구동향에 대해 간략하게 살펴보았다. 또한, 정보보호관리체계 평가방법론 연구를 위해 관리 지침, 평가 기준 산정 방법, 통제 항목과 점검 분야, 위험 분석 측정 범위, 위험 분석 프로세스 모델, 등급 구분 등을 기준으로 국내·외 정보보호관리체계를 비교·분석하였으며, 이를 기반으로 국내 환경에 적합한 정보보호관리체계 평가 방법론을 제안하였다. 향후 연구계획으로는 본 연구에서 도출한 평가 방안을 바탕으로 관리 지침, 평가 항목, 평가 수행 방법, 기관 등급 분류 등에 대한 연구를 수행하여 정보보호관리체계 평가방법론의 표준화 방향을 제시하고자한다.

참 고 문 헌

[1] A.Plate and O.Weissman, "ISO/IEC FCD 17799", ISO/IEC JTC 1/SC27 NC394, 2004.6

[2] John Snare and Eva Kuiper, " ISO/IEC Final DIS 27001", ISO/IEC JTC 1/SC27 NC4472, 2005.4

[3] 홍기향, 김정덕, "ISO에서의 정보보호관리 국제표준화 동향", *정보보학회지, 14권, 2호,* 2004년 4월

[4] ISO, "ISO/IEC 17799:2000 Code of Parctice for Information Security Mnangement", May 2003

[5] BS7799 Part 1 "Information Security Management - Code of practice for information security management", BSI, 1999

[6] BS7799 Part 2 "Information Security Management - Specification for information security management", BSI, 1999

[7] 한국정보보호진흥원, "정보보호관리 체계 인증 동향", *한국정보보호진흥원 최종 연구 보고서,* 2002년 12월

[8] 김재성, 장상수, 고규만, "정보보호관리체계(ISMS) 구축 시 일반적으로 나타나는 결함사례에 관한 분석" *정보보호학회지,* 17권, 4호, 2007년 8월

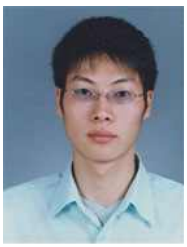
[9] SSE-CMM Project & ISSEA Team, "SSE-CMM version 3"

[10] http://www.sse-cmm.org

[11] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[12] FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

홍 성 혁 (洪成赫)



2008년 2월 : 경남대학교 컴퓨터공학부 (공학사)

2008년 3월 ~ 현재 : 경남대학교 컴퓨터공학부 석사과정

관심분야 : ISMS, 정보보증, DRM, RFID

박 종 혁 (朴鍾爀)

2001년 2월 : 순천향대학교 컴퓨터공학부 (공학사)

2003년 2월 : 고려대학교 정보보호대학원 정보보호학과 (공학석사)

2007년 2월 : 고려대학교 정보보호대학원 정보보호학과 (공학박사)

2002년 12월 ~ 2007년 7월 : 한화에스앤씨(주) 기술연구소 선임연구원

2007년 9월 ~ 현재 : 경남대학교 컴퓨터공학부 전임강사

관심분야 : 디지털포렌식, DRM, 접근제어, 유비쿼터스 컴퓨팅 & 보안, 지능형 홈 서비스, 멀티미디어 보안 및 서비스, ISMS

서 정 택 (徐正澤)

1999년 2월 : 충주대학교 컴퓨터공학과 (공학사)

2001년 2월 : 아주대학교 컴퓨터공학과 (공학석사)

2006년 2월 : 고려대학교 정보보호대학원 정보보호학과 (공학박사)

2000년 11월 ~ 현재 : 한국전자통신연구원 부설연구소 선임연구원

관심분야 : 침입탐지, 침입방지, 정보보호컨설팅, 유비쿼터스 보안