http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.4, November 2015, pp.177-191
http://dx.doi.org/10.7838/jsebs.2015.20.4.177

보안관리체계 분석을 통한 산업중심 보안수준평가 모형 설계 방향 연구

A Study on Design Direction of Industry-Centric Security Level Evaluation Model through Analysis of Security Management System

배제민(Je-Min Bae)*, 김상근(Sanggeun Kim)**, 장항배(Hangbae Chang)***

초 록

최근 국내 기업에서 보안사고가 지속적으로 증가함에 따라 기업의 특성과 환경을 고려한 체계적인 보안관리체계의 필요성이 대두되고 있다. 그러나 기업별 보안수준 측정의 대상, 목적, 방법 등이 다름에도 불구하고 현재 다수의 기업이 기존의 정보보호 관리체계인 K-ISMS를 단편 일률적으로 적용하고 있는 것이 실정이며, 이에 따른 보안관리체계 도입에 대한 실효성에 대해서도 많은 문제가 제기되어지고 있다. 본 논문에서 선행연구 분석을 통해 정보보호, 산업보안, 연구보안에 대한 개념을 정립하고, 정보보호 관리체계, 산업보안관리체계, 연구보안관리체계의 통제항목을 비교·분석하여 산업 전반의 보안을 수행할 수 있는 보안수준 평가항목 개발하였다. 또한 세부적으로 기 존재하는 보안수준평가 모형을 분석하여, 산업의 특성을 고려한 산업 중심의 보안수준평가 모형 설계 방향성을 제시하였다.

ABSTRACT

Recently, the necessity of systematic security management system that consider company' character and environment has appeared because of increasing security accident continuously in domestic companies. However, most of companies has applied to only K-ISMS which is existing information security management system, although They are different from object, purpose and way of security level evaluation by companies. According to this situation, Many experts have questioned that there are many problems with effectiveness of introducing security management system. In this study, We established definition of information security management system, industrial security management system and research security management system through analysis of previous study and developed evaluation item which can implement security in whole industry comparing and analyzing the control items of them. Also, we analyzed existing security level evaluation and suggest design direction of industry-centric security level evaluation model considering character of industry

키워드 : 산업보안, 정보보호, 연구보안, 보안수준평가, 산업 중심
Industrial Security, Information Security, Research Security, Security Level Evaluation, Industry-Centric

* First Author, Department of MIS, Catholic Kwandong University(jmbae@cku.ac.kr)
** Division of Computer Engineering, Sungkyul University(sgkim@sungkyul.edu)
*** Corresponding Author, Department of Industrial Security, Chung-Ang University(hbchang@cau.ac.kr)
Received: 2015-10-16, Review completed: 2015-11-10, Accepted: 2015-11-16

1. 서 론

보안인증제도는 기업이 보안활동을 체계적·지속적으로 수행하기 위해 필요한 조치체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도를 말한다. 현재 국내에서 보안사고가 계속적으로 증가함에 따라, 다양한 분야에서 보안인증, 평가 등의 제도가 계속적으로 생겨나고 있다[5, 7]. 이러한 보안인증제도의 증가와 동시에 보안인증을 받은 기업 또한 증가하고 있음에도 불구하고 보안사고는 계속적으로 발생하고 있고, 특히 보안인증을 받은 기업에서도 보안사고가 빈번하게 발생하고 있음에 따라 보안인증을 통해 기업의 보안수준 향상이나 보안사고의 경감 효과를 얻을 수 있다고 보기 어려운 것이 현실이다[1, 3, 8]. 이와 같은 보안인증제도의 실효성에 대한 문제로 인해 정보보호 안전진단, 전자정부 정보보호 관리체계 인증제도 등 많은 보안인증제도가 폐지 및 통합되었다. 보안인증제도에 대한 실효성 문제가 발생하는 이유는 현재 많은 인증제도가 기존의 가장 보편적인 국내 Information Security Management System (이하 K-ISMS)인증제도에서 파생됨에 있다[6]. 하지만 산업의 종류에 따라 보안대상 및 환경의 특징이 모두 다르기 때문에 현재 정보보호만을 중시하고 있는 획일적인 보안체계구축으로는 효과적인 보안을 구현 및 유지하기가 곤란할 것이다. 그렇기 때문에 산업의 보안대상과 환경을 고려하여 각 산업에 최적화 된 보안수준 향상을 위한 보안인증제도를 구축하는 것이 필요하다[2, 9, 10].

그러므로 본 논문에서는 선행연구를 통해 정보보호, 산업보안, 연구보안 등 각 분야의 보안에 대한 개념을 정의하여 보안대상과 환경의 차이를 비교·분석하고, 취약점에 대한 대응방법이 무엇이 있는지에 대해서 알아보고자 한다.

또한 정보보호 관리체계, 산업보안관리체계, 연구보안관리체계 등의 관리항목을 비교·분석하여 각 보안관리체계의 보안조치사항의 공통점 및 차이점 분석을 통해 각 보안관리체계에서 중요시 하는 평가지표가 무엇인지 파악해보고자 한다. 마지막으로 각 보안관리체계의 차이점 분석을 통해 앞으로 산업보안수준 평가 설계 및 운영에 대한 방향성을 제언하고자 한다.

2. 선행개념 정립

2.1 정보보호 개념

정보보호란 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미하며, 정보를 제공하는 공급자 측면과 사용자 측면에서 이해 할 수 있다. 공급자 측면의 정보보호는 내·외부의 위협요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위로서 해석될 수 있으며, 사용자 측면의 정보보호는 개인 정보 유출, 남용을 방지하기 위한 일련의 행위로서 해석될 수 있다[11].

정보보호의 주요목표는 접근, 수정, 노출, 훼손, 파괴 등의 정보에 대한 위협으로부터 정보자산을 방지하는 것으로 크게 기밀성, 무결성,

가용성 등 세 가지 목표로 이루어져 있다. 우선 기밀성은 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것으로 원치 않는 정보의 공격을 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다. 두 번째, 무결성은 허락되지 않은 사용자 또는 객체가 함부로 수정할 수 없도록 하는 것으로, 수신자가 정보를 수신했을 때 혹은 보관돼 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 첨삭되지 않았음을 확인할 수 있도록 하는 것이다. 마지막으로 가용성은 허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것으로 최근 네트워크의 고도화로 대중에 많이 알려진 서비스 거부 공격이 이러한 가용성을 해치는 공격으로 분류되어 진다[4].

이외에도 정보보호의 정의는 국내외적으로 다양하게 해석되어지고 있다. 정보보호를 인가된 사용자만이(기밀성) 정확하고 완전한 정보로(무결성) 필요할 때 접근할 수 있도록(가용성) 하는 인력의 작업으로 해석되며, 인가되지 않은 접근, 사용, 폭로, 붕괴, 수정, 파괴로부터 정보와 정보 시스템을 보호해 기밀성, 무결성, 가용성을 제공하는 것으로 해석된다.

많은 연구에서 보안과 관련된 용어를 엄격히 구분하여 정보보호를 정의하였으며, 정보보호는 「보안업무규정」과 「정보 및 보안 업무 기획조정 규정」 등 국가보안업무를 취급하는 기관에서 주로 사용되는 용어로써 주로 국가 공공기관에서 기밀성을 보장하기 위한 보안수단의 하나로 이용되어 왔다고 해석한다. 또한 정보보호는 정보의 비밀성, 무결성 및 이용가능성을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보, 정보시스템 및 정보통신망을 보호하는 것으로 정의하였다.

정보보호는 시스템 사용자의 실수, 기계적 오류, 불법적 조작, 그리고 자연재난으로부터 정보, 시스템 및 서비스를 보호하여 사고의 가능성과 그 영향을 최소화하는 일련의 노력을 의미한다.

2.2 산업보안 개념

산업보안을 '산업체, 연구소에서 보유하고 있는 기술, 경영상 정보 및 이와 관련된 인원, 문서, 시설, 통신 등을 경쟁 국가 또는 업체의 산업스파이나 전·현직 임직원, 외국인 과학자 등 각종 위해요소로부터 침해되지 않도록 보호하는 활동'으로 규정하고 있다.

국가정보대학원에서 편찬한 산업보안 실무에서는 산업보안 활동에 유용한 기술상, 경영상의 모든 정보나 인원, 문서, 시설, 자재 등을 산업스파이나 경쟁관계에 있는 기업은 물론이고 특정한 관계가 없는 자에게 누설 또는 침해당하지 않도록 보호 관리하기 위한 대응 방안이나 활동으로 해석하고 있다.

현재 산업보안의 의미는 '외부의 침입으로부터 중요한 정보자산을 보호하는 것 또는 중요 정보를 노리는 외부의 침입을 차단하는 활동으로 간략하게 정의하면서 산업보안에서 민간 기업이 추구하는 궁극적인 목적인 기업의 이익 실현을 위해 손실방지와 자산보호 활동을 기본으로 한다'고 해석한다. 따라서 산업보안의 개념은 '산업을 보호하는 활동이며 구체적으로 유·무형의 모든 자산을 지키는 활동을 포함하는 것'으로 해석하고 있다.

산업보안을 국가산업발전의 주체 및 관련

조직들이 경쟁력 확보와 이윤추구에 유용한 기술이나 경영상 필요한 정보 등 유·무형의 자산을 각종 침해요소로부터 보호하는 자율적이고 예방조치로 해석하고 있다. 즉, 기업이 보유한 기술, 지적 재산 영업비밀과 같은 산업기술을 보호하기 위해 목적 외에 사용하려는 내외부인으로부터 보호하는 행동하는 것으로 보고 있다[12].

2.3 연구보안 개념

연구보안의 개념은 아직 학술적으로나 실무적으로 명확하게 정리되어 있지는 않다. 현재 연구보안의 개념은 관련 법률에서 포괄적의미로 제시되어지고 있다. 「산업기술 유출방지 및 보호에 관한 법률」에서 연구보안은 산업기술과 관련된 국가연구개발사업을 수행하는 과정에서 개발성과물이 외부로 유출되지 아니하도록 필요한 대책을 수립 및 시행하는 활동을 말한다. 또한 국가연구개발사업의 관리 등 규정에서는 연구개발과제를 수행하는 과정에서 주요 정보 및 연구개발 결과 등이 무단으로 유출되지 아니하도록 취하는 조치를 말한다.[2]

정부의 지원을 받아 국가연구개발 사업을 수행하는 기관에서 연구내용 및 연구개발 성과물이 외부로 유출되지 않도록 관리하는 제반업무 활동이라고 정의하고 있다.

연구보안은 국가연구개발 성과물을 외부로 유출되지 않도록 관리하는 보안활동으로써, 국가연구개발 성과물은 산업기술이나 국가핵심기술로 지정/고시 될 수 있기 때문에 연구가 진행되는 전 과정에서부터 산업기술이 지정·보호되기 이전까지 발생하는 모든 연구개발 결과물 및 연구개발 성과물을 보호해야 한다[6].

3. 정보보호, 산업보안, 연구보안 관리체계 비교 및 분석

3.1 보안관리체계 비교

본 논문에서는 각 보안체계의 보호대상 및 대응방법 차이점 분석을 위해 정보보호, 산업보안, 연구보안관리체계를 비교하려고 한다. 앞서 말한 바와 같이 보안평가의 기준이 될 수 있는 각 관리체계의 항목들을 정리하여 분류하였다. 본 논문에서는 정보보호 관리체계는 기존에 다수 국내기업에서 보안관리체계로 많이 도입하고 있는 K-ISMS를 사용하였다. 산업보안관리체계는 산업보호 및 기술개발 현황조사 및 수준 측정을 위해 개발되어진 설문지를 참고하여 개발한 산업보안수준평가모형을 이용하였다. 마지막으로 연구보안관리체계는 연구보안 관련 법령 및 지침서들의 조치사항 및 산업기술보호 자가진단의 평가항목을 참고하여 개발한 연구보안수준평가모형을 사용하였다.

정보보호 관리체계인 K-ISMS의 관리항목은 정보보호 관리 과정 5단계의 14개 필수항목과 정보보호 대책 13개 분야 92개 항목으로 구성되어 있다. 정보보호 관리체계 인증제도는 정보보호의 목적인 정보자산의 무결성 및 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화하고 지속적으로 관리·운영하는 시스템에 대하여 제 3자 인증기관이 객관적이고 독립적으로 평가하고 있다.

이 중 정보보호대책은 정보보호 관리체계 인증 심사 시 요구되는 선택 항목으로써 위험평가를 통하여 조직이 수용 가능한 위험 수준을 달성할 수 있도록 관리항목을 선택하는데 이를 요약하여 정리하면 아래 <Table 1>과 같다.

〈Table 1〉 Information Security Management System(K-ISMS)

Security Control Area	Security Control Item
Information Security policies	Approval of Policies; Announcement of Policy; Connection with Top policies; Enforcement of Policy; Review of Policy; Management of Policy Document
Organization of Information Security	Appointment of Chief Information Security Officer; Organization of Working Group; Information Security Committee; Roll and Responsibility
Outsider Security	Requirement of Outsider Contract; Execution Management of Outsider Security; Security After Outsider Contract
Asset Management	Identification of Information Asset; Assignment of Responsibility by Information Asset; Certification and Handling of Information Asset
Information Security Education and Training	Planning of Education; Object of Education; Content and Way of Education; Execution and Assessment of Education
Human Resource Security	Appointment of Main Person in Charge; Job Segregation; Maintenance of Secret; Management of Retirement of Job Change; Reward and Punishment
Physical Security	Appointment of Protection Area; Protection Facilities; Working in Protection Area; Access Control; Mobile Security; Security of Personal Task Environment; Cable Security; Arrangement and Management of System; Public Office Security
System Development Security	Definition of Security Requirement; Certification and Encryption Function; Security Log; Access Authority; Implementation and Test; Separation with Development and Operation Environment; Transfer of Operation Environment; Test Data Security; Source Program Security; Outsourcing Development Security
Cryptography	Cryptography Policies; Creation and Use of Cryptography
Access Control	Establishment of Access Control Policy; User Registration and Authorization; Manager and Management of Special Authority; Review of Access Authority; User Certification; User Identification; Management of Worker Password; Management of User Password; Network Access; Server Access; Application Program Access; Data Base Access; Mobile Device Access; Internet Connection
Operation Management	Operational Procedure and Responsibilities; Change Management; Acquisition of Information System; Operation of Security System; Management of Performance and Capacity; Fault Management; Remote Operation Management; Smartwork Security; Wireless Network Security; Public Server Security; Back-Up Security; Vulnerability Inspection; Electronic Business Security; Information Transmission Policy and Conclusion of Agreement; Management of Information System Storage Device; Management of Portable Storage Device; Control of Malicious Software; Patch Management; Visual Synchronization; Log Record and Preservation; Access and Use Monitoring; Invasion Attempt Monitoring
Emergency Accident Management	Response Plan and System; Establishment of Emergency Accident Response System; Education of Emergency Accident; Report of Emergency Accident; Process and Recovery of Emergency Accident; Analysis and Sharing of Emergency Accident; Recurrence Prevention
IT Disaster Recovery	Establishment of IT Disaster Recovery System; Testing and Maintenance Management; Establishment of Recovery System by Effect Analysis

〈Table 2〉 Industrial Security Management System

Security Control Area	Security Control Items	Presence in K-ISMS
Environment of Industrial Technology Protection	The Type of Industrial Technology Information Being Protected	O
	Ownership of the Business Products (Private or Corporate)	X
	A Budget Allocation of Separate Industrial Technology Management	X
	Investment Accounts for Technology Protection, Investment Accounts for Technology Protection in Comparison with Total Investment Accounts	X
	Investment for Manpower, Budget, Time of Industrial Technology Protection	O
	Assessment of Future Sustainability Concept for Industrial Technology Protection	X
	The Main Purpose of the Budget Use	X
	Absence of Professional Manpower for Industrial Technology Protection	O
	Current State of Security Manpower in Charge	O
	Knowledge for Professional Manpower for Industrial Technology Protection about Industrial Technology Protection Activities	X
	Authorities of Professional Manpower for Industrial Technology Protection	O
Policy of Industrial Technology Protection	Possession of Regulations about Industrial Technology Protection	O
	Periodic Updates of Regulations about Industrial Technology Protection	O
	Knowledge for Employees of Regulations about Industrial Technology Protection Related Business	X
	Distribution of Regulations about Industrial Technology Protection to Employees	O
	Understanding Regulations about Industrial Technology Protection to Employees	X
	Business Requirement of Regulations about Industrial Technology Protection to Employees	X
	Obeying Regulations about Industrial Technology Protection to Employees	X
	Responsibility of Employees when Breach of Regulation about Industrial Technology Protection Occurs	X
	Effectiveness Assessment of Regulations about Industrial Technology Protection	X
	Management Method about Industrial Technology in Force	X
	Cognitive Level of CEO, Willingness to Implement about Industrial Technology Protection	O

Security Control Area	Security Control Items	Presence in K-ISMS
Policy of Industrial Technology Protection	Security Activities of Interior or Exterior Manpower in Force	O
	Effect of Industrial Technology Protection Activities on Task Execution Procedure	X
	Receptivity to Security of Interior or Exterior Employees	X
	Implementation of Education on Industrial Technology Protection to Employees and Target-Specific Training Methods	O
	Education Cycle of Industrial Technology Protection to General Employees	X
	Education Cycle of Industrial Technology Protection to Security Manager	X
	Linkage between Education of Security Manager and Industrial Technology Protection Work	O
Industrial Technology Protection System	Physical Security Activities in Force	O
	Technical Security Activities in Force	O
Incident Response to Industrial Technology Protection	Experience of Leakage during the Past Tree Years	X
	Number and Cost of Technology Leakage during the Past Three years	X
	Detection Time of Industrial Technology Leakage Accident	O
	Type of Leaked Information of Industrial Technology	X
	Route of Industrial Technology Leakage	X
	Response Actions when Industrial Technology Leakage Accident Cccurs	O
	Reasons of No Response when Industrial Technology Leakage Accident Occurs	X
	Recovery Time of Industrial Technology Leakage Accident	O
	Forecast of Industrial Technology Leakage Accident Outlook	X
Difficulties and Policy Recommendations of Industrial Technology Protection	Application in Operation of Information Instrument, Technology Leakage Risk Assessment	X
	Reasons why Industrial Technology Leakage Accident Occurs	X
	Assessment of Management Level about Industrial Technology Protection	X
	Reasons why Industrial Technology is Neglected	X
	Measurement/Management of Industrial Technology Protection Level	X
	Improvement of Industrial Technology Protection Level	X
	Necessity of Industrial Technology Protection Activities for Sustainable Growth	X
	Difficulties when Industrial Technology Manages/Protects	X
	Government-run Issues about Industrial Technology Protection	X
	Government Request	X

〈Table 3〉 Research Security Management System

Security Control Area	Security Control Items	Presence in K-ISMS
Security Management System	Enactment/Establishment of Research Security Rule	O
	Operation of Research Security Council	O
	Appointment of Research Security Manager	O
	Regular Education (More than 2 Times by 1 year)	X
	Publicity of Research Security Contents	X
	Establishment of Response Plan Preparing for fire/flood/disaster	O
	Reward and Punishment about Security Superior/Regulation Violators	O
Researcher management	Management of New Worker	O
	Management of Career Staff Recruitment	X
	Completing Regular Security Education	O
	Completing Prior Security Education before Business Trip	X
	Recognition of Instructional Materials during Business Trip.	X
	Submission of Return Report after Business Trip.	X
	Confirmation of criminal record Certification from Public Safety Agency	X
	A English contract of engagement and security pledge	X
	Implementing Security Measure of Retiree	O
	Grasping trend after retiring	X
	Preparing Guiding Data about Security Compliance	X
	Operating Reception Room	X
	Management of Entry Log (Name, Date, Purpose)	X
Research Contents Management	Providing Security Grade to Research Development Document	X
	Management of Research Development Document	X
	Duplication and Copy Management of Research Development Document	X
	Preparing Security Device of Research Development Document (Fingerprint/Iris Recognizer)	X
	Providing Security Grade to Research Development Accomplishment	X
	Technology Transfer Commercialization	X
	Preparing Acquisition Method of Patent/Intellectual Property Right	X
	Confirmation Prior Security of Research Superintendent of During Foreign Disclosure and Provision	X
	Security Measure During a collaborative research	O
Research Facility /Equipment Security	Management of Research Facility Protection Area	O
	Security Equipment for Research Equipment Management	X
	Control Process of Research Equipment Management	X
	Preparing Disuse and Reuse of Research Equipment about Protection Measure	X
	Management of Insider Researcher	X
	Management Outsider Researcher Which Do Resident Work	X
	Management of Visitor	X
Research Information System Management	System Access Certification/Authority	O
	Management of System Access Record	O
	Approval and Management of Information Asset	O
	Security Management Activity of External Agency	O
	Security Management of Personal Computer	O
	Document System Operation	O
	Access Restriction through User Authentication during Inside Network Access	O
	Operation of DB Security System	O
	Reaction of Cyber Infringement Accident	O
	Preparing Digital Forensic Process for Security Accident	X
	Establishment of Disaster Preventing System for Fault	X

다음의 산업보안관리체계는 산업보안의 보호조치 및 유출사고에 대한 대응체계 등을 조사하여 산업기술보호정책 수립을 위해 개발되어진 「국가핵심기술 보호 및 산업보안 실태」에 관한 설문지, 기술유출 방지 지원방안 및 중장기적인 정책 수립을 목적으로 실시한 「중소기업 기술보호 역량 및 수준조사」의 설문지, 우리기업의 현황을 지속적으로 조사/분석하고 영업비밀의 보호수준을 고양할 수 있는 바람직한 정책방향을 설계하기 위해 개발되어진 「우리기업의 영업비밀 피해 실태조사 보고서」의 설문지 내용을 참고하여 새롭게 구성을 하였다. 새롭게 구성한 산업보안관리체계는 산업기술보호환경, 산업기술보호정책, 산업기술보호시스템, 산업기술보호 사고대응, 산업기술보호 애로사항 및 정책제언 등 크게 5개 영역의 28개 분야로 분류되어지고 총 관리항목은 50개로 구성되어 있다.

산업보안관리체계는 전반적인 산업을 보호하고 기업이 보유한 기술, 지적 재산 영업비밀과 같은 산업기술을 보호하기 위한 관리체계로써 이를 요약하면 <Table 2>와 같다.

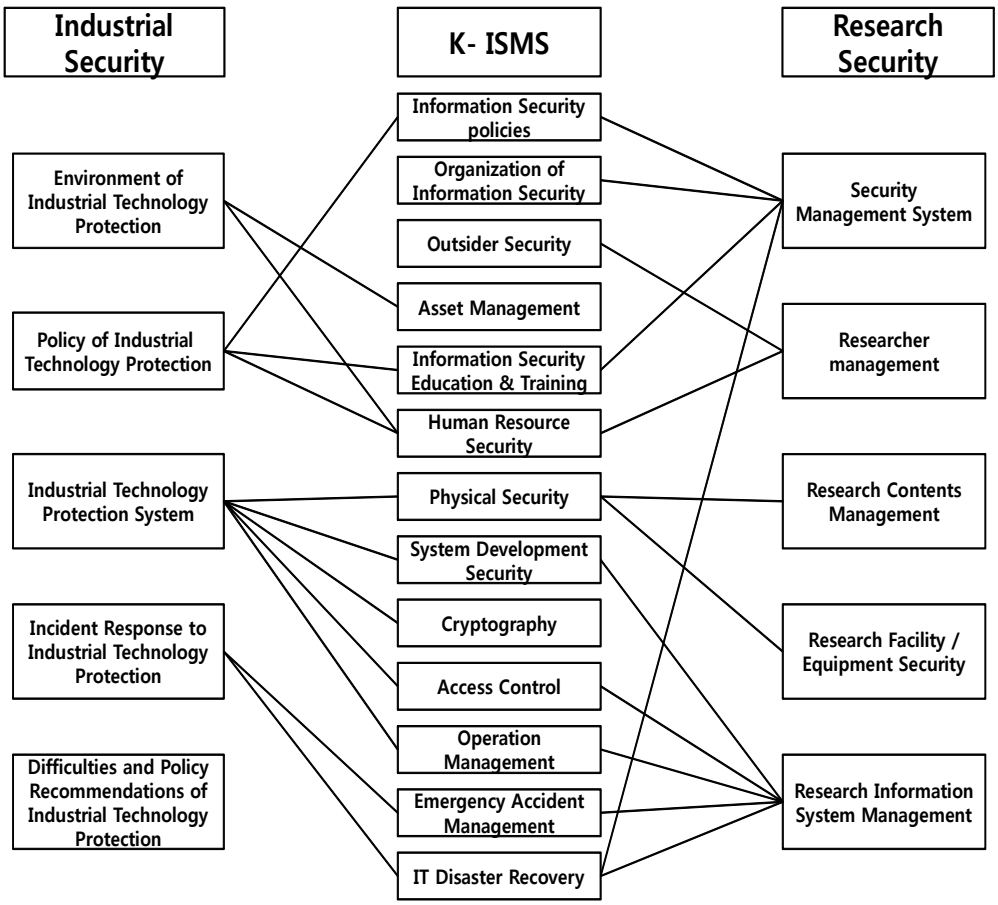
연구보안관리체계는 「국가연구개발사업의 관리 등에 관한 규정」의 각 분야별 세부조치사항과 '산업기술 보호지침'에 근거한 산업기술보호 자가진단 모형의 평가항목을 참고하여 새로운 연구보안관리체계를 만들어 구성하였다. 새로운 연구보안관리체계는 연구가 진행되는 전 과정에서부터 일정 보안수준이 계속적으로 유지되어야 하는 연구보안의 특징을 반영하여 연구개발 전 과정을 보안 관리할 수 있는 관리항목으로 구성되어 있다. 보안관리체계의 관리항목을 요약하면 <Table 3>과 같다.

3.2 산업중심 보안수준평가 모형 설계 방향성 설계

<Figure 1>은 각 보안관리체계의 통제항목이 K-ISMS의 통제항목과 일치 여부를 맵핑을 통해 나타낸 것으로, <Figure 1>의 분석을 통해 알아볼 수 있듯이 산업보안관리체계와 연구보안관리체계의 평가 항목과 기존의 많은 기업에서 도입하고 있는 정보보호 관리체계인 K-ISMS의 평가항목과 많이 상이한 것을 알 수 있다.

정보보호 관리체계는 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립/문서화하고 지속적으로 관리 운용하는 체계를 말하며, 정보통신망의 안정성 및 신뢰성 확보를 위하여 기술적/물리적 보호 조치를 포함한 종합적인 관리체계를 수립/운영하고자하는 기업이 그 대상이다.

산업보안관리체계는 조직의 산업기술을 포함한 산업자산을 체계적으로 보호/관리하기위한 시스템으로, 조직의 근본이라고 할 수 있는 전사적 경영시스템에 대한 만족과 조직의 산업보안 경쟁력을 지속적으로 유지/관리하기 위해 조직이 보유한 산업기술이 외부로 유출되지 않도록 기본 경영시스템 관리체계를 관리적/물리적/기술적 보안 등 다차원적인 관점에서 보완하여 산업자산의 안정적인 보안상태를 유지하기 위한 체계이다. 산업보안관리체계의 대상은 경제 주체의 근간을 이루고 있는 전 산업의 현장 또는 해당 산업의 프로세스 전반에 걸쳐 존재하는 나름대로의 독특한 산업기술을 보유하고 있는 기업이다. 산업기술은 조직 내 설치된 전산시스템에 저장된 정보뿐만



〈Figure 1〉 Connection between Each Security Item of Security Management System

아니라 전산시스템에 저장되지 않고 조직 나름대로의 관리방법에 따라 소유하고 있는 각종 특허기술/도면/제조공법/작업방법 등 조직의 목적달성에 필요한 다양한 경영목표 전략도 포함될 수 있다. 이러한 기술들의 보호 방법은 전산시스템을 통해서 이루어지지 않고 아날로그 방식으로 관리될 수 있기 때문에, 정보보호 관리체계와는 그 관리방법과 관리대상이 달라 전산시스템 위주의 기술적인 관점이 아닌 융합적인 관점에서 조직 전체가 관리대상이 되어야 한다.

이처럼 각 기업의 보안대상 및 보안환경이 다르기 때문에 각 산업에 적용되어야 하는 대응방법도 달라져야한다. 또한 기업을 포함한 조직이 각종위협으로부터 주요자산을 보호하기 위해 수립/관리/운영하는 보안관리체계를 종합적으로 평가할 수 있는 보안인증제도가 구축되어야 하며, 평가지표가 될 관리항목 또한 각 기업 환경을 고려하여 보안이 최적으로 적용되어질 수 있게 구성되어야 한다. 아래 <Table 3>은 모든 산업의 보안관리체계를 종합적으로 평가할 수 있는 산업보안수준평가의 구성요소들이다.

〈Table 4〉 The element of Industrial Security Level Evaluation Model

Evaluation Area	Evaluation Item
Environment of Industrial Technology Protection	Industrial Security Investment accounts; Investment Accounts for Technology Protection; Assessment of Future Sustainability; Concept for Industrial Technology Protection; Main Purpose of the Budget Use; Knowledge for Professional Manpower for Industrial Technology Protection; Knowledge for Employees of Regulations about Industrial Technology Protection Related Business; Publicity of Industrial Security
Information Security Policies	Approval of Policies; Announcement of Policy Connection with Top Policies; Enforcement of Policy; Review of Policy; Management of Policy Document; Responsibility of Employees during Breach of Regulation about Industrial Technology Protection Occurs; Effectiveness Assessment of Regulations about Industrial Technology Protection; Management Method about Industrial Technology in Force; Receptivity to Security of Interior or Exterior Employees
Organization of Information Security	Appointment of Chief Information Security Officer; Organization of Working Group; Information Security Committee; Roll and Responsibility
Outsider Security	Outsider Contract; Execution Management of Outsider Security; Security after Outsider Contract; Preparing Guiding Data about Security Compliance; Operating Reception Room; Management of Access Record
Industrial Asset management	Identification of Information Asset; Assignment of Responsibility by Information Asset; Certification and Handling of Information Asset; Technology Transfer Commercialization; Preparing Acquisition Method of Patent; Intellectual Property Right;
Industrial Security Education and Training	Planning of Education; Execution and Assessment of Education Program; Security Manager Education; Employee Education; Business Trip Employee Education
Human Resource Security	Appointment of Main Person in Charge; Job Segregation; Maintenance of Secret; Management of retirement of Job Change; Reward and Punishment; Management of Career Staff Recruitment; Business Trip Employee Management; Foreign Employee Management; Outsourcing Employee; Visitor Management
Physical Security	Appointment of Protection Area Protection Facilities; Working with Protection Area; Access Control; Mobile Security; Security of Personal Task Environment Cable Security; Arrangement and Management of System; Public Office Security; Security Equipment of Research Development Document; Preparing Disuse and Reuse of Research Equipment about Protection Measure
System Development Security	Definition of Security Requirement; Certification and Encryption Function; Security Log; Access Authority; Implementation and Test; Separation with Development and Operation Environment; Transfer of Operation Environment; Test Data Security; Source Program Security; Outsourcing Development Security
Cryptography	Cryptography Policies; Creation and Use of Cryptography
Access Control	Establishment of Access Control Policy; User Registration and Authorization; Manager and Management of Special Authority; Review of Access Authority; User Certification; User Identification; Management of Worker Password; Management of User Password; Network Access; Server Access; Application Program Access; Data Base Access; Mobile Device Access; Internet Connection

Evaluation Area	Evaluation Item
Operation Management	Operational Procedure and Responsibilities; Change Management; Acquisition of Information System; Operation of Security System; Management of Performance and Capacity; Fault Management; Remote Operation Management; Smartwork Security; Wireless Network Security; Public Server Security; Back-Up Security; Vulnerability Inspection; Electronic Business Security; Information Transmission Policy and Conclusion of Agreement; Management of Information System Storage Device; Management of Portable Storage Device; Control of Malicious Software; Patch Management; Visual Synchronization; Log Record and Preservation; Access and Use Monitoring; Invasion Attempt Monitoring
Incident Response to Industrial Technology Protection	Experience of leakage; Number and cost of technology leakage; Type of leaked information of industrial technology; Reasons of no response when industrial technology leakage accident occurs; Forecast of industrial technology leakage accident outlook
Emergency Accident Management	Response Plan and System; Establishment of Emergency Accident Response System; Education of Emergency Accident; Report of Emergency Accident; Process and Recovery of Emergency Accident; Analysis and Sharing of Emergency Accident; Recurrence Prevention; Digital Forensic
IT Disaster Recovery	Establishment of IT Disaster Recovery System; Testing and Maintenance Management; Establishment of Recovery System by Effect Analysis
Difficulties and Policy Recommendations of Industrial Technology Protection	Application in Operation of Information Instrument; Technology Leakage Risk Assessment; Assessment of Management Level; Reasons of Industrial Technology Neglect; Measurement/Management of Industrial Technology Protection Level; Difficulties when Industrial Technology Manages/Protect; Government-Run Issues about Industrial Technology Protection; Government Request

기존의 많은 기업에서 사용되어지고 있는 정보보호 인증체계인 K-ISMS에 본 연구를 통해 제시되어진 산업보안 인증체계와 연구보안 인증체계의 관리항목 중 K-ISMS의 존재 않는 관리항목을 추가하여, 모든 산업의 보안인증체계를 평가 할 수 있는 산업보안 수준평가항목을 구성하였다. 기존 K-ISMS의 관리항목은 정보보호를 중점으로 만들어졌기 때문에 구성항목의 용어를 산업보안으로 모두 변경시켰고 보호해야할 대상을 정보 및 IT 기기로 국한하는 것이 아니라 모든 산업 자산으로 변경시켰다. 또한 산업보안 환경, 산업보안 사고대응, 산업보안애로사항 및 정책제언 등 K-ISMS와 산업보안 인증체계와 일치하지 않는 영역을 추가하였고, 산업보안에서 중요하게 여기고 있는 산업보안 정책영역 및 인적보안의 평가항목을 좀 더 세부적으로 구분하여 평가항목을 구성하였다.

본 산업보안 수준평가 항목을 통해 기업의 특성을 고려한 산업 전반의 다양한 형태로 저장되어 있는 모든 자산을 체계적으로 보호/관리 할 수 있는 항목을 적용할 수 있을 것이다.

4. 결 론

최근 국내에서 보안사고가 다양한 산업분야에서 계속적으로 발생하고 있음에 따라 이에 따른 보안사고를 방지하기 위해 보안인증, 평가 등의 제도가 생성되고 있음에도 불구하고, 그 수는 줄어들지 않고 있다. 특히 보안인증을

받은 기업에서도 보안사고의 경감과 같은 효과를 찾아보기 어렵기 때문에 보안인증제도의 실효성에 대한 지적이 끊임없이 제기되고 있는 것이 현실이다. 이러한 실효성 문제가 발생하는 이유는 현재 많은 인증제도가 가장 보편적으로 사용되고 있는 보안관리체계인 K-ISMS를 모방하여 만듦에 따라, 유사한 형태의 제도만이 계속적으로 양산되어 기업의 특징을 고려하지 않고 천편일률적으로 적용되고 있기 때문이라는 점이다.

본 논문에서는 정보보호, 산업보안, 연구보안관리체계를 비교하여 각 기업의 보호대상 및 보안환경이 다르다는 것을 확인하고, 이에 따른 대응방법 또한 달라져야 한다는 것을 파악하였다. 그렇기 때문에 기업은 보안수준평가 및 인증을 위해 각 산업의 환경에 적합한 보안관리체계에 따라 보안환경을 구축하고 보안대응조치를 취해야 한다.

본 논문에서는 각 보안관리체계를 비교・분석하여 산업보안 수준평가 모형 설계를 위한 방향성 제시 및 평가항목을 설계하였다. 추후 연구에서는 이러한 방향성을 토대로 산업보안관리 평가 구성요소의 가중치를 산출하여 산업전반의 최적의 보안환경을 구축할 수 있는 산업보안 수준평가 모형을 설계하려고 한다.

References

[1] Bae, S. T. and Kim, J. H., “A Study on Development of the Evaluation Model about Level of Security in National R&D Program,” The Journal of Korean Association of Computer Education, Vol. 16, No. 1, pp. 73-80, 2012.

[2] Chang, S. E. and Ho, C. B., “Organizational factors to the effectiveness of implementing information security management”, Industrial Management and Data Systems, Vol. 106, No. 3, pp. 345-361, 2006.

[3] Choi, J. W. and Jung, J. H., “Study on Building Security Controls Framework for The Industrial Security Management System,” Korean Academy of Public Safety and Criminal Justice, Vol. 22, No. 1, pp. 295-337, 2013.

[4] Choi, J. and Nazareth, D. L., “System Dynamics Model for Information Security Management,” Information and Management, Vol. 52, No. 1, pp. 123-134, 2014.

[5] Jin, C. Y., Kim, A. C., and Lim, J. I., “Correlation Analysis in Information Security Checklist Based on Knowledge Network,” The Journal of Society for e-Business Studies, Vol. 19, No. 2, pp. 109-124, 2014.

[6] Jo, M. K., Kim, S. C., Hwang, J. M., and Kim, S. C., “A Study on the Effect of Institutionalization of the Security Education: Survey of National R&D Projects,” The Journal of Korean Association of Computer Education, Vol. 17, No. 2, pp. 21-29, 2014.

[7] Kang, H. S., “An Analysis of Information Security Management System and Certification Standard for Information Security,” Journal of Security Engineering, Vol. 11,

No. 6, pp. 445-468, 2014.

[8] Kim, C. H. and Yoo, J. H., "Priority of the Government Policy to support Industrial Security-Focus on a companies' demand and efficiency of policy," The Journal of Korean Security Science Association, Vol. 42, pp. 155-178, 2015.

[9] Kim, Y. H. and Chang, H. B., "The Industrial Security Management Model for SMBs in Smart Work," Journal of Intelligent Manufacturing, Vol. 25, No. 2, pp. 319-327, 2012.

[10] Lee, C. S. and Kim, Y. H., "An Analysis of Relationship between Industry Security Education and Capability: Case Centric on Insider Leakage," The Journal of Society for e-Business Studies, Vol. 20, No. 2, pp. 27-36, 2015.

[11] Park, C. S., Lee, D. B., and Kwak, J., "A Study on Enterprise and Government Information Security Enhancement with Information Security Management System," The Journal of Korea Navigation Institute, Vol. 15, No. 6, pp. 1220-1227, 2011.

[12] The Korean Association for Research of Industrial Security, "A Study on the Conceptual Definition of Industrial Security," The Journal of Korean Association for Industry Security, Vol. 2, No. 1, pp. 73-90, 2011.

저 자 소 개

배제민	(E-Mail: jmbae@cku.ac.kr)
1999년	중앙대학교 컴퓨터공학과 (공학박사)
1999년~2013년	관동대학교 컴퓨터교육과 교수
2014년~현재	가톨릭관동대학교 경영정보학과 교수
관심분야	웹 프로그래밍, 임베디드소프트웨어, IoT, 빅데이터

김상근	(E-Mail: sgkim@sungkyul.edu)
1996년	중앙대학교 컴퓨터공학과 (공학박사)
2003년~2004년	Sydney University, 방문교수
1996년~현재	성결대학교 컴퓨터공학부 교수
관심분야	소프트웨어 공학, 클라우드 컴퓨팅, 유비쿼터스 컴퓨팅, 정보보호

장항배	(E-Mail: hbchang@cau.ac.kr)
2006년	연세대학교 정보시스템관리 전공 (박사)
2007년~2011년	대진대학교 경영학과 조교수
2012년~2013년	상명대학교 경영학과 조교수
2014년~현재	중앙대학교 산업보안학과 부교수
관심분야	중소기업 정보보호, 정보 오남용 및 유출방지, 성과분석 체계