*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1585

# 보안성숙도 모델을 활용한 정보보호 관리수준 점검방법에 관한 연구

이 상 규,† 김 인 석‡
고려대학교 정보보호대학원

# A Study on the Method of Checking the Level of Information Security Management Using Security Maturity Model

Sang-kyu Lee,† In-seok Kim‡
Graduate School of Information Security, Korea University

## 요 약

데이터 주도 시대가 형성되면서 경제적 활용가치가 높은 정보의 수집과 분석, 생산과 유통에 관한 안전성 확보를 위한 정보보호 관리의 중요성이 날로 높아지고 있다. 이러한 환경에서 기업은 정보보호 관리체계(ISMS) 인증을 통해 정보보안에 대한 신뢰를 보장받고 있으나 관리체계를 구성하는 세부영역에 대한 수준 평가와 활용은 제한적이다. 이에 반해 보안 성숙도 모델은 기업의 정보보호 수준을 단계적으로 진단할 수 있고 시급히 개선해야 할 영역을 판단할 수 있음은 물론 기업의 특성과 수준에 맞는 목표 설정을 지원하는 도구가 된다. 본 논문에서는 성숙도 모델을 바탕으로 정보보호 분야에 특화되어 개발, 활용되고 있는 보안 성숙도 모델의 사례인 C2M2를 국내 ISMS인증과 비교, 분석하여 정보보호 관리 수준을 점검하기 위한 모형을 벤치마크 하고 ISMS인증의 정보보호대책 세부영역을 구성하는 점검항목 간 우선순위를 도출하여 단계적으로 정보보호 관리수준을 점검하고 구축을 지원할 수 있는 방법을 살펴본다.

## ABSTRACT

In recent years The importance of information security management for securing information collection and analysis, production and distribution is increasing. Companies are assured of confidence in information security through authentication of information Security Management System. However, level assessment and use of domains that make up the management system is limited. On the other hand, the security maturity model is able to diagnose the level of information protection of the enterprise step by step. It is also possible to judge the area to be improved urgently. It is a tool to support goal setting according to the characteristics and level of company. In this paper, C2M2, which is an example of security maturity model, is compared and analyzed with Korea Information Security Management System certification. Benchmark the model to check the level of information security management and derive the priority among the items that constitute the detailed area of information security measures of ISMS certification. It also look at ways to check the level of information security management step by step.

**Keywords:** Information Security, Information Security Management System, ISMS, Security Maturity Model, C2M2

Received(06. 01. 2018), Modified(1st: 09. 28. 2018 2nd: 10. 16. 2018), Accepted(10. 16. 2018)

† 주저자, sk239@shinhan.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

## I. 서 론

금융위원회는 2018년 3월 금융분야 데이터 활용 및 정보보호 종합방안을 발표한 바 있다. 인공지능, 사물인터넷과 함께 4차 산업혁명의 핵심기술로 손꼽히는 빅데이터의 안전한 활용을 보장하기 위한 보호조치로 정보활용과 관리 실태에 대한 상시평가 제도를 도입하겠다는 취지가 담겨있다[1]. 금융업뿐만이 아니라 전통적인 산업군에 속하는 다양한 기업에서도 이른바 '디지털 트렌스포메이션'을 지향하며 비즈니스 모델의 전환을 준비하고 있다. 이와 같이 다양한 산업에서 디지털화가 급격히 진행되면서 기업은 더욱 많은 정보보호 위협에 직면하게 되었다.

기업들은 정보보호 관리체계(Information Security Management System; 이하 ISMS)인증을 받음으로써 고객에게 보안관리 체계 구축과 정보보호 활동에 대한 신뢰를 보장받고 있다. 국제적으로는 ISO/IEC27001과 같은 표준인증을 통해 정보보호 관리체계를 구축, 운영하고 있으며 국내에서는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제47조, "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령" 제50조에 의거 평가 및 인증제도를 운영하고 있다[2].

이러한 인증제도는 기업의 정보보호 활동 강화를 위한 준비와 대응을 가능하게 하는 한편 인증제도 특성상 결과가 인증 또는 미인증으로 제한됨으로 관리체계를 구성하는 세부 영역에 대한 수준별 평가 결과 도출에 한계를 가진다[3]. 또한 이를 통한 세부적인 보안 수준측정과 분석이 어렵고 기업에서 투자를 결정하는 경영진과의 의사소통을 위한 도구로써의 활용성이 부족함에 따라 효과적인 정보보안 투자를 이끌어 내는데에 한계가 될 수 있다.

이에 반해 성숙도 모델에 기반하여 정보보호 분야에 특화되어 개발, 활용중인 정보보호역량 성숙도 모델(Cyberspace Capability Maturity Model : C2M2)은 기업의 정보보호 수준을 단계별로 진단할 수 있고, 기업 전반의 정보보호 역량 강화를 위해 시급히 개선해야 할 영역을 판단할 수 있음은 물론 각 기업의 특성과 수준에 맞는 목표 설정을 지원하는 효과적인 도구가 될 수 있다.

본 연구에서는 성숙도 모델을 기반으로 하는 C2M2 프레임워크와 국내 ISMS인증 제도를 비교 분석하여 정보보호 관리수준을 점검하는데 참조 가능한 모형을 선정하고, ISMS 정보보호대책 영역을 구성하는 점검항목의 우선순위를 결정하여 관리체계 세부 영역별 수준을 측정, 점검할 수 있는 방법을 제안한다. 정보보호 관리수준 점검 방법을 통해서 기업은 우선순위에 따른 정보보호 관리수준을 단계적으로 평가할 수 있으며 점진적으로 이를 보완하여 효과적인 대책을 수립하고 발전시켜 나갈 수 있을 것이라 기대한다.

따라서 본 연구의 목적은 첫 번째, ISMS 세부영역을 구성하는 점검항목에 대한 우선순위를 결정하고 이를 통해 단계적으로 관리수준을 점검할 수 있는 방법을 마련하는 것이고, 두 번째 중소기업 등 관리체계 구축과 운영에 어려움을 겪는 기업들에게 있어서 관리항목의 시급성과 용이성을 기준으로 단계적 적용을 통한 점진적 관리체계 구축을 지원할 수 있는 베이스라인을 제공하는 것이다.

본 논문의 구성은 다음과 같다. 제1장은 서론으로 연구의 배경과 목적, 범위를 기술하였고, 제2장에서는 선행연구 및 문헌자료 분석을 통해 정보보호 관리체계와 인증제도, 성숙도 모델의 개념과 보안성숙도 모델 사례를 정리하였다. 제3장은 관리수준 점검 모형과 점검항목 평가의 기준, 제4장, 5장에서는 실증연구를 위한 분석방법과 결과를 도출하였다. 제6장에서는 실증연구를 통해 도출한 정보보호 관리수준 점검과 활용방안을 제시하고, 제7장에서는 본 연구의 결과 요약과 시사점을 기술하였다.

## II. 이론적 배경

### 2.1 정보보호 관리체계(ISMS) 및 인증제도

정보보호 관리체계란 조직이 보존해야 할 정보자산의 기밀성, 무결성, 가용성을 확보하기 위한 보호대책을 마련하고 위험기반 접근 방법에 기초하여 구축, 운영, 모니터링, 검토, 개선 등의 주기를 거쳐 정보를 체계적으로 관리하고 운영하는 전반적인 체계를 말한다[4]. 국제적으로는 ISO/IEC 27001:2013이 표준인증으로 인정받고 있으며 국내에서는 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 개정을 통해 2001년 7월부터 정보보호 관리체계 인증 제도를 도입한 후 현재까지 ISMS 인증 제도를 운영하고 있다. ISMS 인증체계는 5단계 정보보호 관리과정과 13개 분야 정보보호 대책 총 104개의 통제항목으로 구성된다. ISMS 인증은 정보보호 관리체계의 구축과 유지, 지속적인 개선을 위한 요구사항을 제공하기 위해 개발되었으며 상세적인 항목의 점검을 통해 기업은 정보보

호 정책과 활동의 일관성을 확보하여 보다 효과적인 정보보호 체계를 구축할 수 있다[5].

ISMS 인증을 획득한 기업은 지속 가능한 정보보호 관리와 운영을 위해 필요한 경영진의 지원을 이끌어 낼 수 있고 보유한 자산과 특정 상황에 적합한 통제수단을 도입하여 상황을 개선시킬 수 있다. 무엇보다 인증을 통해 얻을 수 있는 가장 큰 이점은 이해관계자들에게 신뢰성을 제공할 수 있다는 것이다. 이러한 이해관계자 신뢰를 바탕으로 정보보호 투자에 대한 효과적이고 경제적인 관리가 가능해 질 수 있다. Fig. 1은 ISMS 인증의 효과성을 보여주는 그림이다.

ISMS 인증은 상세항목의 점검을 통해 기업의 정보보호 정책과 활동의 일관성을 확보하여 효과적으로 정보보호 체계를 구축할 수 있다는 장점을 가지지만, 선행연구 문헌을 분석한 결과 ISMS 인증제도가 가지는 몇 가지 한계점도 도출할 수 있었다. 이권석[7]은 상당수 기업이 인증을 위해서 컨설팅 업체에 의존하고 있고, 이는 수검기관의 참여도를 낮추어 실질적인 관리체계 구축을 저해한다는 점과 조직 고유의 특성과 규모 그리고 경제적 현실에 대한 고려가 부족하여 효과적인 관리체계를 구축하는데 한계가 있다고 하였고, 손승식[3]은 인증제도 특성상 결과가 인증 또는 미인증으로 제한됨으로 관리체계 수준을 판단하는데 한계를 가진다고 평가하였다. 이에 대한 해결방법으로 김태달[8]은 인증제도가 정보보호 관리체계 목적을 달성하는데 바람직한 도구이지만 단기간에 ISMS 요구사항을 충족시키기 어렵다는 것에 착안하여 점진적인 방법론을 제시하였다. 또한 서동호[9]는 대기업에 비해 자원이 부족한 중소기업은 정보보호 수행을 위한 정책과 시스템을 도입하는 과정에서 다양한 어려움이 존재한다고 지적하였고 2018년 7월 진행된 정보보호 준비도 평가 세미나에서는 기업 내 정보보호 수준을 진단하고 평가하고자 미래창조과학부(현 과학기술정보통신부)에 의해 도입된 정보보호 준비도 평가 인증제도에 대해 정보보호에 취약한 중소기업 등을 위해 기본적인 보안원칙을 수립하고 이를 필요로 하는 기관에게 베이스라인이 되어 보안 수준을 보증할 수 있는 제도로 발전시켜야 한다고 지적하였다[10].

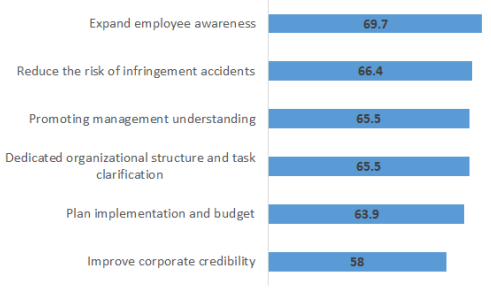


Fig. 1. ISMS Certification effectiveness[6]

## 2.2 성숙도 모델 개념 및 활용

성숙도 모델이란 특정 분야의 능력과 발전 정도를 나타내는 특성, 속성, 지표들의 집합이다. 성숙도 모델에서 제공하는 내용은 일반적으로 우수사례의 기준이 되어 실제 구현 및 적용에 참고가 될 수 있으며 다른 표준이나 실무 규칙과 접목되어 통합될 수 있다. 또한 성숙도 모델을 통해 기업의 업무 내용, 절차 및 방법에 대한 현재 수준을 진단하고 개선을 위한 목표와 우선순위를 설정할 수 있는 가이드를 제공한다. 보안성숙도 모델은 조직에서 일관된 정보보호 관리 수준을 진단하고 이를 의미 있는 방식으로 전달하며 정보보호 관리를 위한 투자의 우선순위를 선정하기 위해 사용된다. Fig 2는 성숙도 모델 사용을 위한 접근방법을 요약한 그림이다. 정보보호 성숙도 목표 수준을 설정한 기업은 세부영역에 대한 수준 점검을 수행하고, 평가 결과를 활용하여 목표한 수준과의 차이를 파악한다. 이후 차이를 극복하기 위한 계획을 수립하고 실행한다. 사업의 목표가 변경되고 위험 환경이 진화되면 이 프로세스를 다시 반복한다.

성숙도 모델은 적용 방식과 표현 방법에 따라 단계적(Staged) 또는 연속적(Continuous)방법으로 구분 가능하다. Fig 3은 단계적 방법과 연속적 방법의 특징을 비교한 그림이다. 단계적 방법은 조직차원

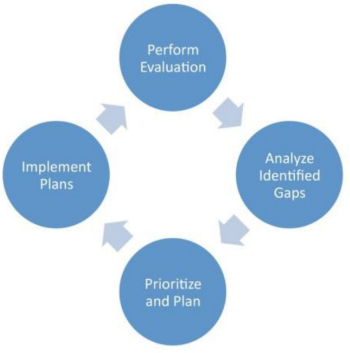


Fig. 2. Approach for Using the Maturity Model[11]

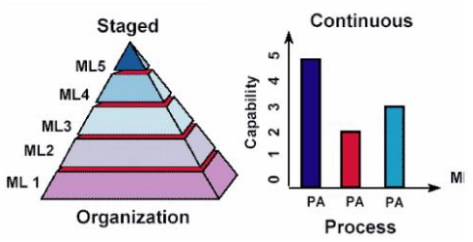


Fig. 3. Staged vs. Continuous Representations〔12〕

의 성숙도를 평가하는데 적합하며 각 성숙도 단계별로 달성해야 할 프로세스 영역이 별도로 정의된다. 전체 영역에 대한 종합적인 성숙도 수준을 중심으로 조직간 비교가 가능하다. 연속적 방법은 영역별 성숙도를 평가할 수 있으며 모든 프로세스 영역별로 각각의 수준이 존재한다. 각 영역을 개별적으로 측정, 개선할 수 있는 장점이 있고 사업 목표와 개선의 순서를 결정한 후 이를 지속적으로 보완해 나갈 수 있다.

### 2.3 C2M2(Cybersecurity Capability Maturity Model)

정보보호 역량 성숙도 모델(C2M2, Cyber security Capability Maturity Model)은 지속되고 있는 모든 형태의 조직에 대한 정보 위협을 감소시키기 위해 2014년 2월 미국 국토안보부(DHS)와 에너지부(DOE)에 의해 개발되었다〔13〕. C2M2는 정보기술 및 운영기술에 필요한 자산과 운영환경과 관련한 정보보호 관리체계의 구현과 관리에 중점을 두고 있다.

Fig 4는 C2M2 모델과 모델을 구성하는 영역 및 요인들 간의 관계를 나타내는 그림이다.

C2M2모델은 10개의 영역으로 구성되어 있고 각 영역은 정보보호 관리 수준과 기업이 해당 영역에서 갖춰야 할 능력, 그리고 이를 성숙시키기 위해 필요한 수행 활동으로 정의된다. 각 영역이 달성해야 하는 목표는 수행 활동을 포함하며 MIL(Maturity Indicator Level)을 기준 지표로 하여 성숙도 수준이 정의된다. 모델을 구성하고 있는 영역은 Fig 5와 같이 위험관리(RM), 자산구성 및 변경관리(ACM), 계정 및 접근 관리(IAM), 위협 및 취약점 관리(TVM), 상황인식(SA), 정보공유 및 의사소통(ISC), 이상징후 탐지 및 사고대응과 업무연속성 관리(IR), 공급망 및 외부 의존성 관리(EDM), 인력관리(WM), 정보보안 프로그램 관리(CPM)로 구성된다.

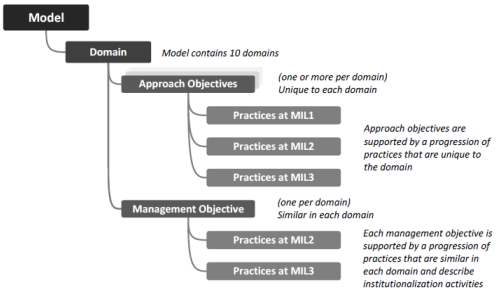


Fig. 4. C2M2 Model and Domain Elements〔9〕

C2M2 모델의 성숙도 단계는 아무런 정보보호 관리 활동이 진행되지 않음을 의미하는 MIL0에서부터 필수적이지만 임시로 수행 가능한 초기 활동을 의미하는 MIL1, 관리영역내 활동을 제도화하는 단계를 의미하는 MIL2, 정보보호 관리활동이 정책과 같은 지침에 따라 진행이 되고 체계적으로 성과가 지속될 수 있는 MIL3까지의 단계로 정의된다.


Fig. 5. Domains of C2M2〔14〕

## III. 관리수준 점검 모형 및 평가기준

### 3.1 정보보호 관리수준 점검모형과 항목 분류 기준

이론적 배경을 통해 살펴본 바와 같이 보안 성숙도 모델 C2M2는 정보보호 관리체계에 대한 수준별 평가 및 관리가 가능하도록 개발된 프레임워크임을 확인하였다. 평가방법 역시 관리체계를 구성하는 영역별로 수준을 측정하고 성숙도 수준을 결정하는 연속적(Continuous) 방법을 채택하고 있음에 따라 관리체계 세부영역을 구성하는 점검항목에 대해 우선순위를 결정하고 이를 통해 점진적으로 관리체계를 구축하고 점검하기 위한 방법을 제안하고자 하는 본 연구의 목적과도 부합한다. 또한 C2M2에 정의된

실무활동과 국내 정보보호 관리체계 인증(ISMS) 통제항목을 비교분석한 결과를 나타내는 Fig 6과 같이 C2M2 의 구성영역은 ISMS 인증에서 요구되는 대부분의 정보보호 대책분야를 구현하고 있다. 따라서 보안성숙도 모델 C2M2 프레임워크를 참조하고 국내 정보보호 관리체계 평가 실정이 잘 반영되어 있고 이미 효과성이 검증된 ISMS 인증 통제항목을 적용한다면 효과적이고 신뢰성있는 단계별 정보보호 관리수준 점검방법으로 활용 가능하다.

ISMS 인증의 통제항목 적용을 위해서는 ISMS 정보보호대책 분야를 구성하는 세부영역에 대하여 점검항목의 우선순위를 결정하여 정의할 필요가 있다. 점검항목의 순위 결정 기준은 C2M2의 성숙도 수준별 수행활동의 특징을 나타내는 Fig 7을 참조할 수 있으며 정보보호 전문가 의견을 기초로 실시한 실증연구를 통해 추출된 ISMS 점검항목의 특징을 기준으로 단계별 수행 항목을 결정한다.

보안 성숙도 모델 C2M2에 정의된 성숙도 수준별 수행활동의 정의 기준 MIL1은 기본적인 실무활동에 속하며 임시적으로 수행될 수 있다는 특징을 가진다. MIL2의 특징은 실무활동이 문서화 되어 있고, 이해관계자가 존재하며 실무 처리를 지원할 수 있는 적절한 자원이 제공된다. 또한 실무 적용을 위한 지침이나 가이드가 존재한다. MIL3은 실무활동이 정책이나 거버넌스에 의해 가이드 되고 있으며 정책에는 표준 및 컴플라이언스 요구사항이 포함되어 있어야 한다. 또한 준수 여부가 주기적으로 검토되어야 하며 실무 수행에 대한 책임과 권한이 배정되어야 한다. 또한 실무를 수행하는 인력은 적정한 기술과 지식을 갖추고 있어야 한다.

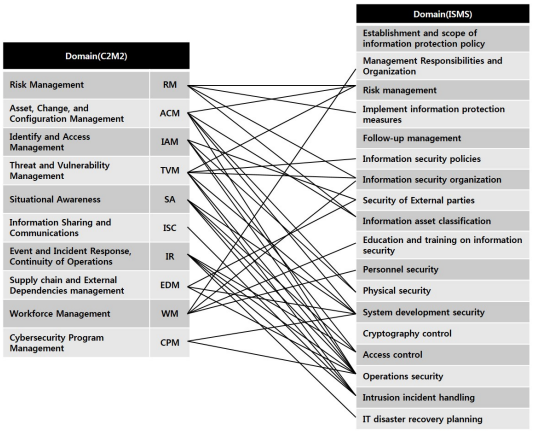


Fig. 6. Comparison of C2M2 & ISMS

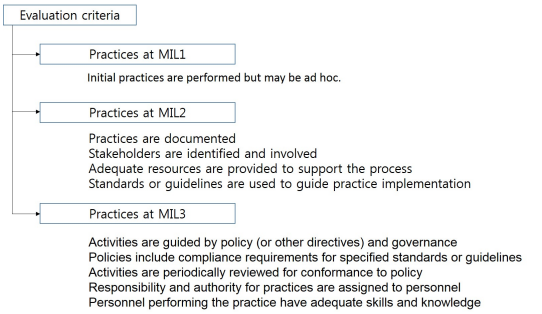


Fig. 7. Characteristics of Maturity Level

## IV. 점검항목 우선순위를 결정을 위한 실증연구

### 4.1 연구범위

보안성숙도 모델 프레임워크를 활용한 정보보호 관리수준 점검방법을 개발하기 위해서는 첫째, 점검을 수행할 관리체계 영역을 구성하고 둘째, 각 영역에 대한 단계별 분류 기준에 따른 점검항목의 반영이 필요하다. 본 연구에서는 정보보호 전문가를 대상으로 AHP(Analytic Hierarchy Process)기법을 통해 ISMS 인증의 13개 정보보호대책 영역에 대한 중요도를 선행 연구한 이중정외 2인의 '정보보호관리체계(ISMS)항목의 중요도 인식과 투자의 우선순위 비교연구' 결과를 바탕으로 중요도가 가장 높게 분석된 침해사고 관리영역에 대해 점검항목의 우선순위를 결정하고 단계를 분류하여 정보보호 관리수준 점검방법의 예시로 활용하였다.

선행된 정보보호대책 항목에 대한 중요도 연구에서는 관리체계를 구성하는 세부 영역을 기술적/물리적 보안, 사전 관리적 보안, 사후 관리적 보안으로 구분하고 관리영역을 재구성하여 평가기준을 구분하였다. 중요도 평가 실험결과 기술적/물리적 보안 측면에서는 접근통제가 29.3%, 사전 관리적 보안측면에서는 인적보안이 23.3%, 사후 관리적 보안 측면에서는 침해사고 관리가 54.1%로 확인되었다[15].

### 4.2 표본 추출 및 자료 수집

정보보호 관리수준 점검방법을 마련하기 위해서 정보보호 업무를 담당하는 기업 실무자 25명을 대상으로 의견조사를 진행하였다. 조사결과의 신뢰성을 확보하기 위하여 정보보호 관리체계 운영 또는 평가

경험이 있는 16명의 응답자를 선별하였고 그 중 일관된 답변을 응답한 2명을 제외한 14명에 대한 결과를 분석에 활용하였다. 응답자에 대한 표본 특성은 Table 1과 같다.

Table 1. The characteristic of sample

| Division | Detail | The number of respondent | Rate |
|---|---|---|---|
| Information security career | 3 ~ 5 years | 4 | 29% |
| | 5 ~ 10 years | 5 | 36% |
| | more than 10 years | 5 | 36% |
| Experience (Operation/ Evaluation) | Experienced | 14 | 100 % |
| ISMS Certification | Qualified | 4 | 29% |
| Academic background | Bachelor's degree | 6 | 43% |
| | Master's degree | 8 | 57% |

### 4.3 연구 및 분석 절차

본 연구는 다음과 같은 순서로 진행과 분석을 실시하였다.

1단계 : 의견조사는 ISMS 인증의 정보보호대책 분야 중 침해사고 관리 분야 점검항목을 조사문항으로 활용하였다.

2단계 : 정보보호 실무자 25명에게 의견조사를 실시하였으며, 조사는 정보보호를 위해 우선적으로 적용해야 하는 시급성과 단계별 필요항목을 빠르게 적용할 수 있는 용이성을 종합적으로 판단하여 1점부터 5점까지를 평가하도록 하였다.

3단계 : ISMS 인증 또는 ISO27001 운영 및 평가 수행 경험이 있는 응답자와 관리체계 인증심사 자격 보유자를 전문가 그룹으로 판단하고 선별하였다.

4단계 : 각 항목에 대한 응답결과의 평균값을 통해 최종 결과 값을 산출하였고 이를 바탕으로 각 항목이 포함되는 수준 단계를 구분하였다.

## V. 실증분석 결과

ISMS 인증 대책분야 중 침해사고 관리 영역 점검항목 우선순위에 대한 정보보호 전문가 의견 결과는 Table 2와 같다. 점검항목의 중요성과 구축 용이성에 따라 1부터 5까지 척도를 선택할 수 있게 하였고 전문가의 평균 응답값에 따라 항목의 최종 분류 단계를 3단계로 결정하였다.

침해사고 관리영역의 1단계에 속하는 관리항목은 침해사고 징후 또는 발생 인지시 보고절차에 따라 보고가 이루어지는지 여부와 침해사고 보고서에 사고 날짜, 내용 등 필요사항을 모두 포함하고 있는지에 대한 여부가 평균 응답 값 1.50으로 나타났다. 또한 최고 경영층까지의 신속한 보고가 1.57, 침해사고 종결 후 원인분석과 결과 보고여부가 1.64로 나타났다. 이상의 항목은 보고서, 보고절차, 보고유무에 관한 것으로 보고에 관한사항들은 정보보호를 위해 가장 우선적으로 관리해야할 특징으로 평가되었다. 또한 침해사고 대응절차 수립여부와 침해사고 발생시 법규와 규정에 따라 신고 및 통지 절차를 수행하고 있는지에 대한 항목은 평균 응답 값 1.64로 나타났다. 두 개 항목은 대응 및 통지의 절차에 관한 것으로 관리절차의 수립과 이를 통한 대응도 우선적으로 관리해야 할 항목으로 판단할 수 있다. 침해사고 처리 및 복구 수행에 대한 기록여부는 1.86, 침해사고 유형 및 중요도에 따른 분류와 보고체계 정의 평균 응답 값은 1.93으로 문서화 및 기록에 관한 사항과 정의/분류와 연관된 사항도 우선적으로 적용되어야 할 항목이라고 판단할 수 있다.

침해사고 관리영역 2단계에 해당되는 항목은 외부 관제시스템 등 외부 기관을 통해 침해사고 대응체계를 구축, 운영하는 경우 대응절차 세부사항을 계약서에 반영하고 있는가에 관한 항목이 2.07, 침해사고 정보와 발견된 취약점을 관련조직 및 인력과 공유하고 있는가에 대한 항목이 동일하게 2.07로 나타남에 따라 조직내부 및 외부의 협조가 필요한 사항들은 2단계에 속하는 관리항목으로 분류하였다.

마지막 최고 단계인 3단계에 해당되는 항목은 침해사고 모니터링 및 대응방법, 절차, 대응 조직 및 인력, 보고 및 승인 방법 등을 포함한 중앙 집중적 대응체계 수립여부가 2.14로 거버넌스 관점의 항목에 해당되며 침해사고 대응을 위한 모의훈련의 주기적 실시 여부가 2.29, 침해사고 분석 정보를 활용하여 대응절차를 변경하고 있는지 여부의 응답 값 또한 2.29로 도출된 것과 같이 주기적으로 변경 및 관리가 필요한 사항들이 3단계에 속하는 항목들로 평가되었다. 또한 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는지에 관한 항목의 결과 값이 2.50으로 나타남에 따라 침해사고 관리 분야에서는 대외

협력 등에 관한 사항이 가장 구축하기 어려운 항목으로 결정되었다.

그 밖에 정보보호 관리체계의 단계적 구축과 평가 방안에 대한 효과성 질문에 대해서 응답자 전원이 정보보호 관리체계를 구성하는 세부분야에 대한 단계적 구축, 평가와 이를 통한 점진적 수준향상을 통해서 전반적인 정보보호 관리수준을 향상시킬 수 있다고 응답하였고, 이러한 "단계적 방법을 통해 관리체계 세부 분야를 구축하고 운영한다면 컨설팅 등 외부 의존도보다 내부인력의 참여와 활동이 증대될 수 있을 것이다."라고 판단한 응답이 85.7%로 나타났다. 또한 "통제항목의 우선순위를 정하여 단계별로 제시된다면 인력, 예산 등 자원이 부족한 조직의 관리체계 구축과 운영에 도움이 될 것이다."라고 응답한 비율은 92.9%로 전문가 의견 수렴 결과 효과성을 기대할 수 있다고 판단된다.

## VI. 정보보호 관리수준 점검방안

5장의 실증연구 조사결과와 같이 정보보호 관리체계의 구축과 평가에 대해 이미 국내에서 효과성이 충분히 검증된 ISMS 인증제도의 통제항목과 연속적(Continuous) 방법의 보안성숙도 모델인 C2M2 프레임워크를 활용하면 기업의 정보보호 관리수준을 효과적으로 점검할 수 있다.

정보보호 관리수준 점검체계는 ISMS 정보보호 대책분야의 13개의 영역으로 구분된다. 해당 영역의 하위에는 개별 점검항목들이 존재하며 각각의 점검항목은 1단계부터 3단계까지로 분류된다. 1단계는 체계정의와 목록, 문서화 및 기록에 관한 항목들이 포함되며 보고와 절차의 수립과 같은 기본적인 실무활동들이 포함된다. 2단계는 이해관계자 존재와 내·외부 협조, 적절한 자원제공과 같은 상위수준의 항목들이 포함된다. 마지막 3단계는 거버넌스의 수립과 주기적 변경관리 등과 같이 정보보호 관리의 지속성을 확보하기 위한 항목들이 해당되며 대외적인 협력활동과 같은 수준 높은 활동들이 포함된다.

Table 2는 침해사고 관리 영역에 대해 항목을 재분류한 단계별 점검항목의 예시이다.

Table 2. Intrusion incident handling Domain

| Step | Practices | Response value |
|---|---|---|
| Step 1 | In case of an incident, report it promptly according to the reporting procedure. | 1.50 |
| | Incident reports should include all necessary information. | 1.50 |
| | If the impact is serious, report to top management quickly. | 1.57 |
| | Analyze the cause of the incident and report the result. | 1.64 |
| | Procedures for response to infringement incidents are established and include necessary items. | 1.64 |
| | In the event of an infringement incident, follow the procedures for notification and notification in accordance with relevant laws and regulations. | 1.64 |
| | Records an infestation incident. | 1.86 |
| | Identify the types of infringement and define the reporting system accordingly. | 1.93 |
| Step 2 | In case of establishing and operating an infringement incident response system through an external agency, the infringement incident procedure shall be reflected in the contract. | 2.07 |
| | Share infringement information and discovered vulnerabilities with related organizations and personnel. | 2.07 |
| Step 3 | Establish a centralized response system. | 2.14 |
| | Training plans and train them periodically. | 2.29 |
| | Change the response procedure using the information of the infringement analysis. | 2.29 |
| | Establish a cooperation system with external experts, professional companies, professional organizations. | 2.50 |

정보보호 업무를 담당하는 관리자는 관리체계를 구성하는 세부 영역에 대한 단계별 관리 항목들을 점검하여 기업이 위치한 현재수준을 파악할 수 있다. 이때 각 항목을 평가하는 기준은 시행여부에 따라 미시행, 부분시행, 완전시행으로 평가할 수 있으며 영역별 각 단계에 포함되는 모든 평가 항목이 완전시행인 경우 해당 단계를 달성했다고 판단할 수 있다. 예를 들어, 침해사고 관리영역의 단계별 평가방법을 요약한 Fig 8의 예시와 같이 침해사고 관리 영역의 1단계에는 8개의 관리항목이 존재한다. 2단계의 경우에는 1단계 관리항목을 포함하여 10개의 항목으로 구성되어 있고 그 중 1개 항목이 미시행 상태이고 나머지 9개 항목이 완전 시행되고 있는 상태임을 의미한다. 또한 1단계를 포함하고 있는 2단계의 모든 점검 항목 중에 1개 항목이 미시행 중임으로 해당영역에 대한 최종적인 관리단계는 1단계로 평가된다.

관리체계를 구성하는 모든 영역에 대한 단계별 수준 점검이 완료되면 세부 영역에 대한 관리수준을 포함한 정보보호 관리체계 전체 수준을 판단할 수 있다.

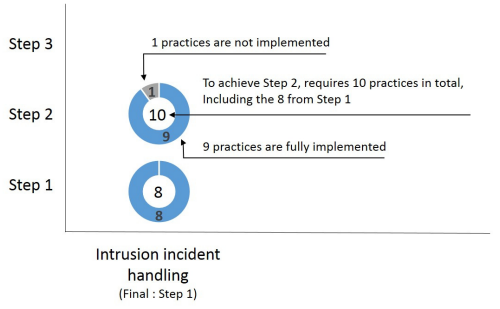


Fig. 8. Example of evaluation method

## VII. 결 론

기업의 성공적인 운영은 각 조직이 가지는 고유한 위험이 효과적으로 관리될 때에야 비로소 달성될 수 있다. 따라서 기업의 위험관리 전략에 부합하는 정보보호 관리체계의 수립과 운영이 필요하다. 이를 위해 기업은 정보보호를 위해 시행중인 보안활동과 현재의 역량 상태를 세밀히 평가하고, 달성해야할 목표수준을 설정한 후 목표까지의 격차를 식별하여 투자 우선순위를 결정해야 한다. 보안 성숙도 모델과 이를 활용한 정보보호 관리수준 점검방법의 목적은 조직 내부 역량을 최대한으로 활용하여 단계적으로 정보보호 관리수준을 점검하고 또한 새롭게 관리체계를 구축하고자 하는 기업의 점진적 체계구축을 지원하고자 함이다. 이를 위해 점검항목의 중요성과 구축의 용이성을 기준으로 특징을 파악하여 우선순위를 결정하였고, 순위별로 정의된 항목에 대한 단계적 구축이 완수되면 정보보호 관리수준 역시 향상되는 효과를 얻을 수 있다.

이를 위해 정보보호 관리수준 점검방법의 기본적인 구조와 특징은 정보보호역량 성숙도 모델 C2M2를 기반으로 하였으며 일반적인 국내 기업의 실정에 맞는 수준별 기준의 특징 정의를 위해 ISMS 구성영역 중 침해사고 관리영역에 대한 전문가 의견조사를 실시하여 반영하였다. 따라서 특정 산업 및 기업에서는 조직 내부의 기준을 새롭게 정의하여 점검방법을 보완하고 이를 확대하여 활용할 수 있다. 예를 들어 해당 산업에 적용되는 법규에서 요구하는 최소한의 보안 요구사항 또는 기업이 가지는 고유의 특징과 점검항목의 중요성 및 이를 바탕으로 도출해낸 위험분석 결과를 점검단계의 기준으로 결정하는 것도 하나의 방법이 될 수 있다.

정보보호 관리수준 점검방법은 이러한 결정을 실행하기 위한 유용한 도구로 활용될 수 있고 최종적으로 기업의 리스크 관리 전략 및 활동에 반영되어 실제적인 도움이 될 수 있을 것이라 기대한다. 앞으로의 연구를 통해 ISMS 정보보호 대책분야 세부영역의 점검항목 특징과 연관성을 추가적으로 분석하여 단계별 관리항목 분류를 더욱 정교화하고 추가적으로 적용 가능한 항목들을 새롭게 개발하여 정의할 수 있다. 더 나아가 특정 산업이 가지는 고유한 특성이 반영될 수 있도록 적합한 영역과 단계별 점검항목을 개발하여 관리체계 수준점검방법을 더욱 발전시킬 수 있을 것이다.

## References

[1] FSC, "Comprehensive plan for data utilization and information protection in Financial sector", Mar 2018

[2] Su-min Sin, "A study on the impact of the project management knowledge area on the ISMS Project Performance : The Case of ISMS project", Dongguk University, 2016

[3] Seng-sik Son, "The Study on the Improved Assessment Methodology for Information Security Level Using 27001", Sungkyunkwan university, 2014
[4] Young-Sik Bae, "A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance", *Korea Academy Industrial Cooperation Society*, 13(9), pp.4224-4233, 2012
[5] KISA, Information Security Management System Certification Guide, 2017
[6] KISA, Information Security Management System Certification Plan, 2017
[7] Kwon-suk Lee, "A Information Security Management Model using Balanced Scorecard", Dongguk University, 2013
[8] Tai-dal Kim, "The ISO the research also the ISMS security maturity of 27001 regarding a measurement modeling", *Journal of The Korea Society of Computer and Information*, 12(6), pp. 153-160, Dec. 2007
[9] Dong-ho Seo, "A Study on Reclassification the Information Security Management System(ISMS) control Items by Company Type", Korea University, 2017
[10] http://news.mt.co.kr/mtview.php?no=2018070916531927530, Money Today, 2018. 7. 9
[11] U.S Department of Energy(DOE), Cybersecurity capability maturity model, 2014
[12] http://www.tutorialspoint.com/cmmi/cmmi-representations.htm, 2018. 5. 30
[13] Sung-moon Kwon, "Cyber Security Framework for Critical Infrastructure", *Journal of The Korea Institute of information Security & Cryptology*, 27(2), Apr. 2017
[14] Katie Stewart, Evaluating and Improving Cybersecurity Capabilities of the Electricity Critical Infrastructure, Carnegie Mellon University, 2015
[15] Choong-Cheang Lee, Jin Kim, ChungHun Lee, "A comparative study on the priorities between perceived importance and investment of the areas for Information Security Management System", *Journal of the Korea Institute of information Security & Cryptology*, 24(5), pp. 919-929, Oct. 2014

## 〈저자소개〉

이 상 규 (Sang-kyu Lee) 정회원
1999년 2월: 명지대학교 컴퓨터소프트웨어학과 졸업
2017년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 금융보안, 정보보호 관리체계, 보안성숙도

김 인 석 (In-seok Kim) 정회원
2008년: 고려대학교 정보경영공학과 박사
2011년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 금융보안, 전자금융 정책, 전자금융 법규