성숙도 평가모델에 기반한 정보보호 관리체계 인증에 관한 연구

이진용*, 양선주**, 장형진*
*한국정보통신기술협회 디지털정보보호단
**한국인터넷진흥원 디지털안전단
topjin55@tta.or.kr, sjyang@kisa.or.kr, chj760@tta.or.kr

A Study on Information Security Management System Certification based on Maturity Assessment Model

Jin Yong Lee*, Sun Joo Yang**, Hyoung Jin Jang*
*Digital Infomation Security Department, Telecommunications Technology Association
**Digital Safety Department, Korea Internet & Security Agency

요 약

정부에서는 내·외부 사이버 보안 위협 고도화에 대한 실질적이고 효과적인 대응을 위해 정보보호 관리체계(Information Security Management; 이하 ISMS) 인증에 대한 법령을 시행하고 있다.

ISMS 인증은 컨설팅과 인증심사를 분리하여 독립성을 확보하였으며, 현장심사 비중을 높여 기존 문서심사에 치중되었던 인증·평가제도와의 차별화를 통해 실효성을 증진시켰다.

그러나 최근 ISMS 인증을 받은 대상자임에도 불구하고 개인정보 정보유출 사고, 대규모 서비스 장애가 유발됨으로써, 다시금 ISMS 인증의 실효성 문제가 제기되고 있다. 현재 제기되고 있는 문제의 요인은 인증기준에 적합한 최소한의 요구사항만 심사·심의하는 ISMS 인증의 한계점에 기인한다. 본 논문에서는 이와 같은 ISMS 인증의 실효적 한계점을 개선하고 인증취득 대상자의 실질적 보안역량 강화시키기 위하여 성숙도 평가모델에 기반한 ISMS 인증제도 운영 방안을 제언한다.

1. 서론

첨단화, 지능화, 고도화되고 있는 사이버 보안 위협에 효과적인 정보보호 대응체계를 구축하기 위해 정부에서는 2013년부터 안전진단 제도를 폐지하고 ISMS 인증제도로 일원화하는 작업을 거쳤다. 이와 함께 일정 자격 이상의 대상자에 대해서는 ISMS 인증을 취득하도록 의무화하여 조직 내 정보보호 관리체계가 실질적으로 구축될 수 있는 사회적 환경을 조성하였다[1].

ISMS 인증제도는 기존의 안전진단과 달리 심사기관의 독립성을 기반으로, 현장심사에 대한 비중을 높였다. 이것은 문서중심 심사와 차별화된 방향이며, 이를 통해 현장의 보안운영 환경 수준을 실질적으로 평가하고 개선할 수 있도록 하였다. 또한, 인증취득 대상자 및 정보보호 산업군에 대한 투자를 촉진시켰다. 더 나아가 인증취득 시 조직성과에 긍정적인 영향을 미침으로써 기업의 성과향상, 금융리스크 감소, 보안 투자에 따른 장기적 기업 매출액 증대 및 주가 향상 등에 효과가 있다는 다양한 연구들이 발표되기도 하였다[2]. 그럼에도 불구하고, 최근 ISMS 인증을 취득한 대상자 내에서 대규모 서비스 장애, 개인정보 유출사고 등이 지속적으로 발생하고 있다. 이에 따라, 앞서 서술된 ISMS 인증의 긍정적인 효과에도 불구하고 새로운 측면으로 실효성 문제가 다시금 제기되고 있다[3]. 즉, ISMS 인증이 실제 사건·사고에 대하여 어느 정도까지 유효성을 보장할 수 있는가에 대한 문제이다.

그러나 ISMS 인증심사는 최소한의 인증기준에 대한 적합·부적합만을 심사하기 때문에 실질적 보안운영 수준의 유효성 보장을 위한 측정·관리는 어려운 한계점이 존재한다. 이와 같은 한계점은 다음 두 가지 문제점을 내포하고 있다.

첫째, ISMS 인증취득만을 목표로 하는 대상자에게는 최소한의 보안 요구사항 충족 외 추가 개선의 필요성을 제공하지 않는다.

둘째, 지속적으로 정보보호 수준을 향상시키고자 하는 대상자에게는 개선에 대한 동기부여 및 조직 내 관심을 이끌어 낼 수 있는 기준점을 제시하지 못한다.

본 논문에서는 이와 같은 문제점을 개선하고 정보보호 관리체계의 실질적 효과 및 지속적 정보보호 개선 활동에 대한 관심을 촉진하기 위하여 성숙도 평가모델에 기반한 ISMS 인증제도 구축 방안을 제언한다.

2. 관련 연구

정보보호 성숙도·수준을 측정하는 방법론을 사용하고 있는 국내 대표적 평가·인증 제도로는 정보보호 준비도 평가를 예로 들 수 있다. 정보보호 준비도 평가는 중소기업을 중심으로 전산업 영역군에 적용 가능하다. 평가방법으로는 총 30개 활동 및 선택지표를 대상으로 세부 운영 수준을 측정하여 5단계의 성숙도 수준을 산출한다[4]. 그러나 해당 평가방법은 ISMS 인증제도와 같은 규모와 범위가 큰 환경에서는 적합하지 않은 한계점이 존재한다. 국외에서는 미국 국방성이 발주하기 위한 사업에 참여하기 위한 자격제도로 사이버 보안 성숙도 모델인증(Cybersecurity Maturity Model Certification)이 2020년부터 시행되고 있다. 해당 인증제도는 등급이 상향될수록 평가항목을 추가하여 보다 세밀하게 성숙도를 측정·관리하는 형태를 띄고 있다[5, 6]. 이와 같은 방법은 정보보호 관리체계의 범용적 적용을 위해 인증기준 항목을 고정·정의하고 있는 ISMS 인증제도에 적용하기에는 적합하지 않다.

이외 정보보호 수준 측정 및 목표에 대한 개선과제를 수립하여 ISMS를 효과적 운영하기 위한 방법이 제안되기도 하였으나[7], ISMS 인증절차 운영보다는 개선과제의 효과적 달성·관리에 국한된다.

3. ISMS 성숙도 평가모델 구축방안

본 논문에서는 ISMS 성숙도 평가모델 구축을 위해 다음과 같이 세 가지 목표 달성을 위한 기본 원칙을 수립한다.

첫째, 지속적 인증유지·관리를 위한 동기와 관심을 유발할 수 있도록 하여야 한다.

이를 위해 ISMS 인증의 운영·유지 기간에 대한 유의미한 특성을 고려하여 성숙도 평가항목에 반영하도록 한다.

둘째, ISMS 심사구분(최초·사후·갱신)에 따른 심사기법을 차별화하고 각 심사결과를 연계할 수 있어야 한다.

심사구분 간의 시계열적 연계관리를 통해 전략적 집중관리가 필요한 개선 항목을 도출할 수 있도록 한다.

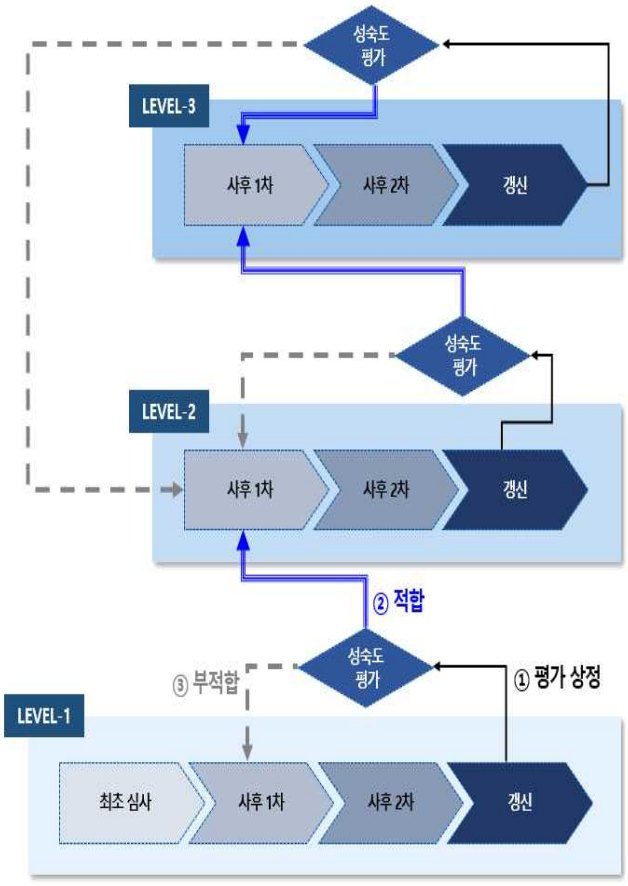
셋째, 성숙도 모델의 평가방법은 간단·명료하여야 한다.

ISMS 인증은 프로세스 평가로 분류될 수 있으며, 기능적 평가보다 주관적 요소가 포함될 가능성이 다분히 높을 수 밖에 없다. 따라서, 객관성을 최대한 보장하기 위해 평가모델을 단순화할 수 있어야 한다.

이와 같이 인증유지·관리 연속성, 심사 구분에 따른 심사기법 차별화를 기반으로 주관적 요소를 최대한 배제할 수 있는 성숙도 평가 방안을 강구하도록 한다.

3.1. ISMS 성숙도 평가모델 운영 절차

(그림 1)은 앞서 제시한 기본원칙에 입각한 성숙도 평가모델 사상을 구현하기 위한 ISMS 인증 운영 절차를 도식화한 것이다.



(그림 1) ISMS 성숙도 평가모델

(그림 1)의 ISMS 성숙도 평가모델의 첫 번째 단계인 “LEVEL-1”은 최초 심사를 수검한 후 갱신심사를 받기 전까지의 기간을 의미한다.

이 단계에서는 최초 구축한 정보보호 관리체계가

두 번의 사후관리를 통해 일정수준 이상의 타당성을 확보하기 위한 것을 목표로 한다. 이를 위해 인증기준의 누락·중복 및 구축 방향의 적절성 등에 중점을 두고 심사를 수행한다.

첫 단계에서 두 번의 사후관리까지 완료한 기업은 갱신 시점에 인증위원회에 상정하여 성숙도 등급 상향에 대한 심의를 받을 수 있다. 인증위원회에서는 정보보호 관리체계 구축의 타당성을 심의하는 것에 중점을 둔다. 이를 위해 최초·사후·갱신심사를 수행하기까지의 발견된 결함의 연계적 관리수준(유사·재발 여부 등)을 중점적으로 심의 할 수 있다. 이때 유사결함이 지속적으로 재발되거나 적절하지 않은 보완대책으로 관리되고 있다고 판단될 경우 등급 상향은 기각되고 기존 등급을 유지하도록 한다. 등급 상향에 실패한 대상자는 차기 심사 시 등급 상향 재심의 혹은 현재 등급으로 인증을 유지하는 방안 중 희망하는 것을 선택할 수 있도록 하여 등급 상향 기각에 대한 부담을 경감할 수 있도록 한다.

다음 단계인 “LEVEL-2”에서는 이전 단계에서 구축된 정보보호 관리체계에 대한 신뢰성 평가에 방점을 둔다. 등급 상향에 대한 인증심의위원회의 심의 절차는 “LEVLE-1”과 동일하다. 이때 인증위원회는 발견된 결함의 타당성 외 실효성 및 효과성에 기반한 품질수준을 심의한다.

최종 단계인 “LEVEL-3”을 유지하기 위해서는 앞선 단계에서 확립된 타당성·신뢰성 외 보안수준 개선 관리·운영에 대해 정성·정략적으로 입증할 수 있어야 한다.

3.2. ISMS 성숙도 등급에 따른 심사 방법

위와 같은 ISMS 인증 운영 절차를 위한 심사 방법은 <표1>과 같이 구성된다.

<표 1> ISMS 성숙도 등급 및 심사 방법

등급	운영기간	심사 목표
LEVEL-1	3년 이하	- ISMS 구축·운영항목의 누락·중복·적절성을 위한 타당성 심사
LEVEL-2	3년 초과	- ISMS 구축·운영항목의 품질·산출물에 대한 신뢰성 심사
LEVEL-3	6년 초과	- ISMS 구축·운영항목의 타당성·신뢰성·보안수준 개선의 측정관리 심사

ISMS 인증 유지·관리 기간을 바탕으로 ISMS 구축의 타당성에서부터 신뢰성 및 지속적 보안 품질 개선의 심사 전략을 수립하고 각 심사 수행의 연계성을 확립하여 인증위원회로부터 적절한 등급 심의를 받을 수 있도록 한다.

4. 결론

본 논문은 최근 제기되고 있는 ISMS 인증제도 실효성에 대한 문제를 개선하고 인증 대상자에게 동기부여와 관심을 지속적으로 촉진하기 위한 ISMS 성숙도 평가모델 구축방안을 제언하였다. 평가방법은 주관성을 최대한 배제하기 위해 인증유지·운영기간, 심사 방법의 차별화와 연계성을 활용하여 타당성·신뢰성·지속적 보안 품질 개선의 단계로 심사·심의하는 방안을 제시하였다.

향후 산업군, 규모, 임직원 성숙도 등을 고려한 심사·심의 방법에 대한 구체적인 추가 연구가 이루어질 때 보다 효과적인 모델이 구축되어 질 것으로 기대된다.

참고문헌

[1] KISA, Available: https://isms.kisa.or.kr/main/

[2] 최동권, 윤형식, “기업의 정보보호관리가 영업성과와 기업가치에 미치는 영향: 정보보호관리체계(ISMS)를 중심으로”, 디지털콘텐츠학회논문지, Vol.20, No.8, pp.1567-1576, 2019.

[3] TECHWORLD, Available: https://www.epnc.co.kr/news/articleView.html?idxno=228638

[4] 김민천, “우리나라의 개인정보 보호제도 분석: 인증 및 평가제도와 개인식별번호를 중심으로”, 정보보호정책, Vol.23, No.4, pp.38-58, 2016.

[5] Vijay Sundararajan, Arman Ghodousi, J. Eric Dietz, “The Most Common Control Deficiencies in CMMC non-compliant DoD contractors”, IEEE International Symposium on Technologies for Homeland Security, 2022 IEEE International Symposium on.:1-7, 2022.

[6] Reginald M. Jones, Mary Mikhaee, “Cybersecurity: How to Successfully Navigate CMMC and the DFARS”, Procurement Lawyer, Vol.55, No.3, pp.1-41, 2020.

[7] 김용선, 민대환, “성숙도 기반 정보보호 수준 측정 시 효과성을 중심으로 한 ISMS 개선 우선순위 도출모델에 대한 연구”, 한국IT서비스학회 학술대회 논문집, pp.802-806, 2020.