https://doi.org/10.33778/kcsa.2024.24.2.039

사이버보안관제센터 운영 및 제도 개선에 관한 연구

이 후 기*

요 약

공공분야의 사이버보안관제는 정보시스템 및 정보통신망의 자원 손실이나 정보 침해를 사전에 방지하여 대국민 행정서비스의 안전성을 확보하는 것을 목적으로 한다. 보안관제 체계는 시스템 취약점 분석과 보안시스템 탐지 패턴 최적화를 통한 실시간 탐지, 분석, 대응 및 보고 업무를 수행하는 절차이다. 본 연구는 현재 운영 중인 사이버보안관제센터와 이를 위탁 운영할 수 있는 보안관제 전문업체 간의 수급 미스매치 현황을 객관적으로 파악하고, 실질적, 제도적 개선방안을 도출, 제안하는 것을 목적으로 한다. 향후 공공부문의 보안관제센터 운영이 증가할 것으로 예상되는 점을 고려하여, 보안관제센터 운영 프로세스에 필요한 실무적 보완과 보안관제 전문기관 지정제도 개선에 대한 연구는 근본적이고 시의적절하다. 국가 전략적 산업화 측면에서 지속적인 연구가 필요한 분야이다.

A Study on the Operation and System Improvement of Cyber Security Center

Hoo-Ki Lee*

ABSTRACT

The purpose of security control in the public sector is to secure the safety of administrative services for the public by preventing resource loss or information infringement in information systems and information and communication networks. The security control system is a process that performs real-time detection, analysis, response, and reporting through system vulnerability analysis and security system detection pattern optimization. This study aims to objectively identify the current situation of the mismatch between the supply and demand of cyber security control centers currently in operation and specialized security control companies that can be entrusted to operate them, and to derive and propose practical and institutional improvement measures. Considering that the operation of security control centers in the public sector is expected to increase in the future, research on the practical supplementation required for the operation process of security control centers and the improvement of the designation system of security control specialized organizations has fundamental and timely significance, and it is an area that requires continuous research in terms of strategic industrialization.

Key words : Cyber security, specialized cyber security control companies, SOC

접수일(2024년 04월 03일), 수정일(1차: 2024년 04월 11일), 게재확정일(2024년 04월 22일)

* 건양대학교/스마트보안학과(주저자)

1. 서 론

디지털 전환의 증진은 산업의 패러다임 변화와 함께 국민의 생활 기반이 사이버공간과의 결합과 융합을 촉진하고 있다. 이에 따라 편의성과 효율성이 증대되는 동시에 사이버 공격에 노출되는 영역 이 증가하는 문제점도 대두되고 있다. 즉, 국민의 보편적인 일상 생활과 경제와 사회를 구성하는 기반 전체가 사이버위협의 대상이 되었다.[1] 국가 핵심기술에 대한 지식재산의 탈취와 주요 기반시설 마비 등 사이버공격이 전세계적으로 급증하고 공격기법이 고도화되는 등 위협으로부터 보안성과 복원력 향상 전략이 요구 되고 있다.[8]

보안관제는 기관의 정보시스템망을 보호하는 정보시스템을 운영·관리하고 사이버공격 및 위협을 즉시 탐지하고 대응하는 것을 의미한다. 보안관제센터를 중심으로 이루어지는 보안관제는 24시간 365일 무중단으로 사이버 위협을 모니터링, 탐지, 분석, 조사하여 조직을 보호하는 역할을 수행하며, 국가차원의 사이버안전관리체계에 유기적인 대응을 유지하는 역할을 수행한다. 즉, 네트워크, 서버, 컴퓨터, 엔드포인트 디바이스, 운영 체제, 애플리케이션 및 데이터베이스에서 사이버 보안 사고의 징후가 있는지 지속적으로 검사하며, 피드를 분석하고, 규칙을 수립하고, 예외를 식별하고, 대응을 강화하고, 새로운 취약점을 계속 감시한다. 새로운 위협에 신속하게 대응할 수 있도록 교대근무로 24시간 운영되는 것이 일반적이며, 다른 부서 및 직원과 협업과 협력을 수행한다.[2]

본 연구는 현재 운영 중인 보안관제센터와 이를 위탁운영 할 수 있는 보안관제 전문기업 간 수요공급 간 불일치가 나타나는 현황을 객관적으로 파악하고, 이에 대한 실무적이고 제도적인 개선방안을 도출하여 제안하고자 한다. 공공부문에서 보안관제센터의 운영은 앞으로도 증가하는 추세를 감안한다면, 보안관제 운영 과정의 현실적인 보완과 보안관제 전문기관의 지정 제도의 개선에 관한 연구는 근본적이고 시기적인 측면에서 의미와 중요성을 갖으며, 향후에도 전략산업화 측면에서 지속적인 연구가 필요한 분야라고 할 수 있다.[6]

1-2. 연구 방법

현재 운영 중인 보안관제센터와 이를 위탁운영할 수 있는 보안관제 전문기업 간 수요공급 현황을 파악하고자 조달청 나라장터에서 2022년~2023년 간 사이버보안관제 용역 자료 중 입법부, 사법부, 지방자치단체를 포함한 행정부에서 발주한 내역을 검색해서 데이터로 변환하였다. 나라장터에서 검색을 통해 수집한 데이터는 '공고일, 개찰일, 수요기관, 공고명, 계약방법, 사업금액, 개찰결과, 유찰사유' 등 총 8개의 변수를 구성하였다. 검색과정에서 일부 누락은 있을 수 있겠으나 총 154건의 보안관제 용역의 발주 자료를 구축하였다. 용역의 내용은 해당년도의 보안관제 용역이 있고, 23년~24년 혹은 24년~25년의 다년도 보안관제 용역이 있으며, 지방자치단체의 경우 보안관제와 유지보수 용역을 통합하여 발주하는 용역도 포함되어 있다. 무응찰 및 단독응찰인 경우 유찰되어 일정기간 경과 후 재발주하는 경우가 있고, 단독응찰인 경우 기획재정부 계약예규 특례에 따라 재발주 없이 수의계약을 진행하거나, 재발주 후에도 단독응찰일 경우 수의계약으로 진행한다. 계약방법은 '제한협상에 의한 계약', '일반협상에 의한 계약', '수의계약' 등으로 구분되어 진행한다.

2. 국가기관 보안관제 현황

2-1. 우리나라 국가기관의 보안관제 일반현황

우리나라는 민간기업들이 보안관제를 1999년부터 시작한 이후, 정부 및 공공부문은 2003년부터 보안관제센터를 운영하기 시작했고, 지방자치단체는 사이버침해대응센터를 2009년부터 본격적으로 구축되기 시작하여 현재 17개 광역지방자치단체와 일부 기초지방자치단체에서 운영하고 있다.[5]

공공부문의 사이버보안은 「전자정부법」과 대통령훈령인 「국가사이버안전관리규정」에 따라 이루어지고 있으며, 국가 전체적인 차원에서 사이버보안을 규율하는 일반법은 현재까지 입법화되지 않았다. 따라서 각 부문별로 개별법에 근거를 두고 사이버공격에 대응하는 보안관제를 수행하며,

중앙행정기관과 지방자치단체의 보안대책 및 사이버침해 대응지원체계 구축에 관한 사항은 「전자정부법」 제24조와 같은 법 시행령 제20조 제4항에 규정하여 연계체계가 마련되어 있는 상황이다.[2]

「국가사이버안전관리규정」 제10조는 국가정보원과 중앙행정기관 및 지방자치단체의 사이버공격 관련한 정보의 통보와 통지 등의 협력을 규정하고 있다. 또한 같은 규정 제10조의2는 중앙행정기관, 지방자치단체 그리고 공공기관의 보안관제센터의 설치·운영을 규정하고 있으며, 사이버공격 정보를 국가정보원 및 관계 기관에 제공하고, 과학기술정보통신부에서 지정하는 보안관제 전문기업에서 인원을 파견받아 보안관제업무를 수행할 수 있게 하는 내용 등을 포함하고 있다.

「사이버안보 업무규정」(대통령령) 제14조제1항은 정부 차원에서 사이버공격과 위협을 즉시 탐지하고 대응하기 위해 정부보안관제체계를 구축하여 운영해야 함을 규정하고, 같은 규정 제14조제2항에 따라 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격을 실시간으로 탐지하고 분석하여 즉시 대응조치를 수행할 수 있도록 보안관제센터를 구축·운영해야 함을 명시하고 있다.

2-2. 보안관제 체계

국가·공공분야의 보안관제는 정보시스템 및 정보통신망의 자원 손실이나 정보 침해를 사전에 방지하여 대국민 행정서비스의 안전성을 확보하는 것을 목적으로 한다. 보안관제 체계는 시스템 취약점 분석과 보안시스템 탐지 패턴 최적화를 통한 실시간 탐지, 분석, 대응 및 보고 업무를 수행하는 일련의 절차이다. 일반상황에서 사이버위협에 대한 대응 프로세스는 사이버위협 보안관제, 네트워크 트래픽 모니터링 등을 통하여 사이버위협 유형을 분석한다. 그리고 공격 IP, 유해 사이트 차단 및 악성코드 치료 등을 통해 예방활동을 수행한다. 또한 긴급상황에서 침해사고 발생 시 피해확산 방지를 위해 공격차단 및 피해시스템 격리 등 초동대응을 실시한다. 이후 유관기관 등에 침해사고를 신속히 전파하고, 긴급대응반을 편성하여 피해 시스템 분석, 침해사고 원인분석, 복구, 재발방지 대책을 수립한다.[4]

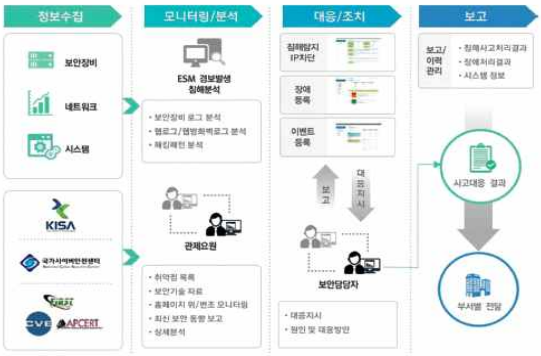
보안관제센터는 일정한 수준의 시설과 장비 및 이를 운영하기 위한 전문인력과 전담인력을 갖추고 보안관제업무를 수행하는 조직이라고 볼 수 있다. 국가·공공분야의 보안관제는 『단위보안관제(각급기관) → 부문보안관제(중앙행정기관) → 국가보안관제(국가사이버안보센터)』의 3단계 보안관제 체계를 구축하고 있다.[7] 17개 광역지방자치단체의 '사이버침해대응센터'는 단위보안관제센터이며, 한국지역정보개발원(KLID)의 '사이버침해대응 지원센터'가 17개 광역지방자치단체의 부문보안관제센터에 해당한다.[6] 최상위 국가보안관제센터인 '국가사이버안보센터'는 부문·단위보안관제센터에 사이버공격을 탐지할 수 있는 기술을 배포하고, 국가안보를 위협하는 사이버공격을 탐지·대응하는 역할을 수행한다.[2]

부문보안관제센터에서는 해당 기관 및 소속·산하기관 정보통신망을 대상으로 보안관제를 실시하고 있다. 중앙행정기관은 사이버침해대응 지원센터를 포함하여 한국인터넷진흥원(KISA) 침해사고대응센터, 국가정보자원관리원, 금융보안원 등 '42개 부문보안관제센터'를 운영하고 있다.[2]

단위보안관제센터는 중앙행정기관이 아닌 각급기관의 장이 자체 및 소관분야 정보통신망에 대한 사이버공격을 1차적으로 탐지·대응하기 위해 구축·운영하는 보안관제센터이다.[2]

또한 2009년 광역지방자치단체에 사이버침해대응센터 구축이 완료되고, 관제가 시작되었으나, 관제기술 부족 등 문제점에 대응하여 지방자치단체를 지원하기 위해 2009년 3월에 한국지역정보개발원(KLID)에 '사이버침해대응 지원센터'를 구축하였다.[8] 따라서 17개 시·도 사이버침해대응센터는 단위보안관제센터로 소관 본청 및 시·군·구 관제 및 상황관리를 하며, 해킹 시도를 탐지하여 대응 및 조치를 취하고 침입시도를 차단하는 역할을 수행한다. 한국지역정보개발원(KLID)은 17개 광역지방자치단체를 통합관제하며 해킹시도 탐지 및 탐지규칙을 배포하며, 지방자치단체 침해사고를

분석·지원하고 관련 정보를 공유한다. 행정안전부는 지방자치단체 사이버보안 총괄 관리 역할을 하며 지방자치단체의 사이버침해대응 정책을 수립하고 유관기관 간 정보를 공유한다.[2]



<그림 1> 보안관제 프로세스[3]

2-3. 보안관제 전문기업 현황

보안관제 업무는 사이버위협의 특성상 24시간 교대근무 체계로 운영되어 일부 내부 직원을 제외하고는 용역사업을 통해 위탁하고 있다. 우리나라는 2011년 7월1일부터「보안관제 전문기업 지정 등에 관한 공고」 따라 '보안관제 전문기업 지정 제도'를 운영하므로, 각 기관은 용역 발주를 통해 보안관제 전문기업 선정을 진행한다.

「보안관제 전문기업 지정 등에 관한 공고」 제2조(정의) 2에 제시된 '보안관제 전문기업'이란,「국가사이버안전관리규정」 제10조의2에 따라 중앙행정기관, 지방자치단체 및 공공기관의 보안관제 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 과학기술정보통신부에서 지정하는 기업을 말한다. 2024년 현재 21개 기업이 보안관제 전문기업으로 지정되어 있으며 그 현황은 <표. 1>과 같다. 공공부문의 보안관제센터에 관제요원 등 인력을 파견 받을 경우에는 반드시 보안관제 전문기업의 직원이여야 한다.

보안관제 전문기업은 보안관제 전문인력 15명 이상, 자기 자본 20억 이상, 보안관제 업무수행능력 평가 통과시(70점 이상) 지정될 수 있다. 또한 사후관리를 통하여 보안관제 전문기업으로 지정된 이후에 역량이 일정 수준 이하인 기업은 지정을 취소함으로써 공공부문 보안관제 전문기업들의 질적 수준을 유지하도록 제도가 마련되어 있다.[4]

<표 1> 보안관제 전문기업 지정 현황(2024년 3월 현재)[10]

No.	기업명	최초지정일
1	㈜에스케이쉴더스	2011.10.31.
2	한전KDN(주)	2011.10.31.
3	㈜싸이버원	2011.10.31.
4	㈜이글루코퍼레이션	2011.10.31.
5	한국통신인터넷기술(주)	2011.10.31.
6	㈜안랩	2011.10.31.
7	㈜윈스	2011.10.31.
8	㈜시큐어원	2012.04.27.
9	㈜케이티디에스	2016.01.12.
10	㈜삼성에스디에스	2016.08.05.
11	㈜파이오링크	2017.10.18
12	㈜가비아	2017.10.18
13	㈜에이쓰리시큐리티	2018.04.25.
14	롯데정보통신(주)	2018.07.13.
15	㈜엘지씨엔에스	2018.07.13.
16	㈜시큐아이	2019.03.19.
17	씨엘정보통신(주)	2020.11.10.
18	㈜피디정보통신	2021.06.14.
19	㈜신한DS	2021.10.18.
20	㈜엔아이티서비스	2022.04.18.
21	㈜메타넷티플랫폼	2023.12.15.

이와 같이 보안관제 전문기업은 보안관제센터와 긴밀한 관계가 있으며 보안관제센터 운영은 보안관제 수행에 충분한 역량을 지닌 보안관제 전문기업과의 협업에 많은 영향을 받을 수 밖에 없다. 근본적으로는 보안관제센터의 운영에 있어서 적절한 역량을 보유한 보안관제 전문기업을 확보하는 것이 우선적으로 요구된다.[8]

3. 수요 대비 보안관제 전문기관의 공급 불일치 현황

3-1. 조달청 나라장터 보안관제 용역 발주 자료 분석결과(2022년~2023년)

조달청 나라장터에서 2022년~2023년 간 사이버보안관제 용역 자료 중 입법부, 사법부, 행정부, 지방자치단체, 광역시도 교육청을 포함한 발주한

내역을 검색을 통해 데이터로 변환하였다. 나라장터에서 검색을 통해 수집한 데이터는 '공고일, 개찰일, 수요기관, 공고명, 계약방법, 사업금액, 개찰결과, 유찰사유' 등 총 8개 변수로 구성하였다.

검색과정에서 일부 누락은 있을 수 있으며, 총 154건의 보안관제 용역이 발주된 것을 확인하였다. 다만, 예산규모는 'S/W 대가 산정 가이드'의 보안관제 비용 산정에 준하여 편성되며, 본 연구에서 논하는 범위가 아니므로 이에 대한 별도 논의는 제외한다. 용역 내용은 해당년도의 보안관제 용역이 있고, 23년~24년 혹은 24~25년의 다년도 보안관제 용역이 있으며, 지방자치단체의 경우 보안관제와 유지보수 용역을 통합하여 발주하는 용역도 포함되어 있다. 무응찰 및 단독응찰인 경우 유찰되어 일정 기간 경과 후 재발주하는 경우가 있고, 단독응찰인 경우 기획재정부 계약예규에 따라 재발주 없이 수의계약을 진행하거나, 재발주 후에도 단독응찰일 경우 수의계약으로 진행하였다. 2021년도에 유찰되어 2022년도에 재발주한 자료는 포함하였으나, 2023년도에 유찰되어 2024년 재발주된 자료는 포함하지 않았다. 계약방법은 '제한협상에 의한 계약', '일반협상에 의한 계약', '수의계약' 등으로 진행된다.

2022년도 및 2023년도 조달청 나라장터를 통해 보안관제 용역을 발주한 현황을 분석한 결과는 <표. 2>과 <표. 3>에 제시하였다.

	낙찰기업(용역수)	씨엠티정보통신(1) 에스케이쉴더스(1) 윈스(1) 이글루코퍼레이션(2) 파이오링크(2)	시큐어원(2) 윈스(1) 이글루코퍼레이션(4) 파이오링크(1)	씨엠티정보통신(1) 윈스(2) 파이오링크(1) 한국통신인터넷기술(1)	시큐어원(2) 싸이버원(1) 에스케이쉴더스(4) 윈스(1) 이글루코퍼레이션(3) 파이오링크(1)	이글루코퍼레이션(3)	씨엠티정보통신(2) 시큐어원(4) 싸이버원(1) 에스케이쉴더스(5) 윈스(5) 이글루코퍼레이션(12) 파이오링크(5) 한국통신인터넷기술(1)

보안관제 전문기업으로 2022년 이전에 지정받은 20개 기업 중 입법부, 사업부, 행정부, 지방자치단체 및 광역 교육청의 용역에 입찰한 기업은 9개 기업으로 45%의 참여율을 보였다. 이는 대기업 입찰참여 제한으로 입찰에 참여하지 않았거나, 모기업 계열사의 보안관제만을 수행하는 보안관제 전문기업이 전체 보안관제 전문기업의 55%에 해당한다고 볼 수 있다. 입찰에 참여한 9개 기업 중 8개 기업이 최종 낙찰을 받은 것으로 나타났다. 최종 낙찰 상황에서 수의계약의 비중이 32%~35% 수준으로 분석되었다.

<표 2> 2022년 조달청 나라장터 보안관제 용역 발주 현황

기관구분		광역지방자치단체	광역교육청	기초지방자치단체	행정부	입/사법부	전체
기관수		11	9	5	15	5	45
발주횟수		18	20	13	26	8	85
평균발주횟수		1.6	2.2	2.6	1.7	1.6	1.9
유찰	무응찰	1	1	0	2	1	5
	단독응찰	10	11	8	12	4	45
	계	11	12	8	14	5	50
	유찰율(%)	61.1	60.0	61.5	53.8	62.5	58.8
낙찰	수의계약	4	8	3	12	3	30
	경쟁낙찰	3	0	2	0	0	5

<표 3> 2023년 조달청 나라장터 보안관제 용역 발주 현황

기관구분		광역지방자치단체	광역교육청	기초지방자치단체	행정부	입/사법부	전체
기관수		10	10	3	11	4	38
발주횟수		17	18	6	19	9	69
평균발주횟수		1.7	1.8	2.0	1.7	2.3	1.8
유찰	무응찰	2	0	0	3	0	5
	단독응찰	9	9	3	9	6	36
	계	11	9	3	12	6	41
	유찰율(%)	64.7	50.0	50.0	63.2	66.7	59.4
낙찰	수의계약	4	8	1	6	3	22
	경쟁낙찰	2	1	2	1	0	6

	낙찰기업 (용역수)	시큐어원(1) 윈스(1) 이글루코퍼레이션(3) 한국통신인터넷기술(1)	시큐어원(1) 윈스(3) 이글루코퍼레이션(4) 파이오링크(1)	씨엘티정보통신(1) 시큐어원(1) 파이오링크(1)	싸이버원(1) 씨엘티정보통신(1) 에스케이쉴더스(4) 이글루코퍼레이션(1)	에스케이쉴더스(2) 이글루코퍼레이션(1)	씨엘티정보통신(2) 시큐어원(3) 싸이버원(1) 에스케이쉴더스(6) 윈스(4) 이글루코퍼레이션(9) 파이오링크(2) 한국통신인터넷기술(1)

보안관제 용역을 발주한 기관별 평균 횟수는 2022년 1.9회, 2023년 1.8회로 평균 약 2회의 발주 과정을 진행하였다. 특히, 일부 지방의 광역교육청은 2022년도에 총 6회에 걸쳐 발주 및 재발주가 진행되었다. 무응찰은 5회, 단독응찰 36~45회로 인해 유찰이 발생했으며, 유찰율은 모두 50% 이상으로 분포되었다. 낙찰이 되었다고 하더라도 수의계약인 경우에는 단독입찰에 기인한 것으로 볼 수 있다. 따라서 수의계약인 경우까지 포함하여 유찰율을 산정하면, 2022년도 광역지방자치단체 83.3%, 광역교육청 100%, 기초지방자치단체 84.6%, 행정부 100%, 입/사법부 100%, 연평균 94.1%의 유찰율이 나타났고, 2023년도 광역지방자치단체 88.2%, 광역교육청 94.4%, 기초지방자치단체 66.7%, 행정부 94.7%, 입/사법부 100%, 연평균 91.3%의 유찰율을 산정할 수 있었다. 2개 이상의 복수 기업이 입찰을 통하여 경쟁한 사례는 2022년 5건(5.9%), 2023년 6건(8.7%)으로 나타났다. 따라서 유찰율이 높은 반면, 정상적인 기술 경쟁을 통한 낙찰은 상대적으로 낮게 나타나는 현상을 보였다.

3-2. 보안관제 수요 대비 보안관제 전문기업의 공급 불일치 분석 결과

본 연구의 진행 과정에서 수집한 자료를 통해 파악한 결과, 2022년에 45개 기관이 총85회의 보안관제 용역 발주를 진행하였고, 2023년에는 38개 기관이 총69회의 용역을 발주했지만, 총 9개의 보안관제 전문기업만이 입찰에 참여하여 보안관제 수요에 비해 공급 측면에서 상당한 불균형이 나타났다. 공공기관까지 포함하여 수요와 공급 상황을 고려한다면 불균형 정도는 더욱 심각한 상황임을 알 수 있다. 물론 개별 보안관제 용역이 2~3년의 기간 동안 다년계약으로 진행하는 부분이 있다고 하더라도, 수요와 공급의 불일치 문제는 정부 및 지방자치단체와 공공기관에서 법률에 따라 진행하는 보안관제 업무에 비해 보안관제 전문기업의 양적측면과 질적측면 모두 현저히 미비된 상황이라고 볼 수 있다. 아울러 보안관제 전문기업을 지정하는 취지에 비해 공공부문의 용역에 미참여하는 기업이 절반 이상이라는 상황이 파악되었다. 이러한 수요와 공급의 불일치 문제는 발주와 재발주 과정을 반복적으로 수행할 수 밖에 없는 입법부, 사법부, 지방자치단체를 포함한 행정부의 담당 공무원 및 행정행위에 부담을 주는 요인이 될 수 있다.[4]

4. 결론 및 제언

국가기관 보안관제센터의 운영과정에서 보안관제 전문기업의 활용은 불가피한 상황이다. 그러나 보안관제센터를 운영하는 국가기관들의 수요에 보안관제 전문기업 공급 부족이 나타나는 현상을 조달청 나라장터 데이터를 통해 전술한 바와 같이 소개하였다. 이와 같은 문제를 개선하기 위해서는, 전문기업의 양적 및 질적 수준의 향상, 전문인력의 양성, 용역발주 과정의 효율성을 제고하는 방안 등을 추진하는 것을 제안한다. 이를 제도적 측면과 실무적 측면에서 요약하면 다음과 같다.

제도적 측면에서의 개선 방안은 첫째, 보안관제 전문기업을 양적으로 확충해야 한다. 이를 위해 한시적으로 보안관제 전문기업 지정 요건의 자본금 등 진입장벽을 낮추되, 기업의 채산성을 높일 수 있는 신기술 기반의 보안관제 전문기업을 지정할 수 있는 요건을 마련하는 방향의 개선을 제안

한다. 둘째, 보안관제 전문기업의 질적 측면에 대한 개선이 필요하다. 갱신심사에서 지방의 지사를 운용하는 부분을 포함하는 심사 기준 및 평가체계를 개발·적용하여, 원격관제를 허용하되 침해사고 대응을 위한 현장출동이 가능한 방향으로 개선해야 한다. 셋째, 실무에 바로 투입할 수 있는 보안관제 전문인력의 양성에 대해 관련학과가 설치된 대학과의 협약을 통해 직무 훈련(OJT; On the Job Training) 등 방법으로 실무와 취업이 연계되는 인력 양성 제도를 마련해야 한다.

실무적 차원에서 조달청의 나라장터를 통해 용역을 발주할 때 제도적으로 보장하고 있으나 제한적으로만 활용하는 계약 방법을 최대한 이용하면서 효율성을 극대화해야 한다. 첫째, 현재 기관별로 분산하여 보안관제 용역을 발주하기 보다는 보안관제센터가 인접해 있는 지역의 경우에는 보안관제 용역을 통합하여 발주하도록 국가기관 간 협의하는 것이 바람직 하다. 둘째, 보안관제 용역이 대부분 단년도 사업으로 진행되고, 실무에서 다년도 계약은 제한적으로 진행되고 있다. 따라서 보안관제 용역을 발주하는 실무차원에서 다년도 계약을 활성화해야 한다.

참고문헌

[1] 2030 미래사회 변화 및 사이버위협 전망 연구, 한국인터넷진흥원, 2021.12.
[2] 최정민, 사이버침해대응센터 운영실태와 개선과제, 국회입법조사처, 2021.12.15.
[3] 보안관제프로세스, https://www.igloo.co.kr/service/security-control/, 이글루코퍼레이션, 2024.2.
[4] 박상돈, 공공부문 보안관제 전문기업 관리제도 개선에 관한 연구Law, 동아법학 제84호, pp.177-206, 2019.8.24.
[5] 2023 연례보고서, 국가사이버안보센터, 2023.5.
[6] 2023 국가정보보호백서, 국가정보원 외, 2023.5.
[7] 권수진 외, 데이터로 보는 국가사이버안보, 국회도서관 2023-4호(통권 제4호), 2023.5.10.
[8] 국가 사이버안보 전략, 대통령실 국가안보실, 2024.2.
[9] 이후기, 공공보안관제업무 동향 및 과제, 국회입법조사처 전문가간담회, 2021.8.4.
[10] 보안관제 전문기업, 정보보호산업진흥포털, https://www.ksecurity.or.kr/kisis/subIndex/470.do, 2024.3.

〔저자소개〕

이 후 기 (Hoo-Ki Lee)
건양대학교 스마트보안학과 교수
숭실대학교 공학박사
산학협력부단장, 정보보호영재교육원 부원장, 사이버미래혁신융합연구회 회장
관심분야 : 사이버보안 침해지표 연구, 제로트러스트 보안, 보안관제시스템
email : hk0038@konyang.ac.kr