2024년 4/4분기

정보보호 인적자원개발위원회(ISC)

ISSUE REPORT

| 보안관제 업계현황 및 인력양성 방향 (공공기관 보안관제 중심으로)

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

CONTENTS

정보보호 인적자원개발위원회 사무국 02-6748-2011, 2039 | mhr0327@kisia.or.kr

본 이슈리포트는 건양대학교 스마트보안학과 이후기 교수가 작성하였습니다.

요약

□ 공공분야 보안관제 현황

○ 우리나라의 사이버보안과 보안관제를 규율하는 일반법은 없으며, 각 분야별 개별법에 근거하여 사이버공격에 대응 중임

○ 보안관제센터의 설치 및 운영에 관해 「국가사이버안전관리규정」 제10조의2, 「사이버안보 업무규정」 제14조, 「국가정보보안기본지침」 제131조~제138조에서 전반적인 사항을 규정하고 있으며, 「보안관제 전문기업 지정 등에 관한 공고」에 일정 기준과 운영방식을 명시함

○ 공공분야의 보안관제센터는 현재 과학기술정보통신부장관이 고시하는 23개의 지정된 보안관제 전문기업에 의해 위탁운영되고 있으며, 44개의 부문보안관제센터 및 약 50여개의 단위기관 보안관제센터에 보안관제 운영 인력이 파견됨

○ 각급 기관에서 보안관제센터의 구축과 운영을 위한 운영규정의 수립 및 세부사항을 규정하고 있으며, 업무 위탁 시 이를 기반으로 세부 과업내용이 고려됨

□ 공공분야 보안관제 용역 사업 분석

○ 보안관제센터의 효과적 운영에 있어 적절한 역량을 보유한 보안관제 전문기업의 확보가 우선적으로 요구됨

○ 향후 공공분야의 보안관제 시장은 더욱 확대되고 보안관제센터의 위탁운영이 대폭 증가할 것으로 예상됨

○ 대부분의 관제센터는 고급, 중급, 초급 인력을 골고루 요구하고 있으나, 모든 기술 등급별 인력 수급이 어려운 상태이며, 24시간 365일 주야간 교대근무를 요하는 업무 특성상 인력 수급이 가장 어려운 문제로 확인됨

□ 보안관제 용역 사업 인력 수급 개선

○ 공공분야 보안관제 용역 대부분은 '보안관제 전문기업 지정 등의 관한 공고'에 별첨인 '기술인력의 자격기준'에 의거함

○ 실시간 보안관제 모니터링과 초동대응 수행, 주/야 교대 근무하는 보안관제요원은 대부분 초급기술자를 요청하고 있어 신규 초급인력의 수급이 중요함

○ 그러나, 일부 발주사업에서 '기술인력의 자격기준'에 따른 초급기술자 기준 외 특수 경력이 있는 초급인력 편성을 요구하고 있어 신입인력의 투입이 어려운 실정임

□ 결론

○ 보안관제 초급기술자의 경력 요건을 최소화하고 관련 학위와 자격을 보유한 인력이 원활하게 투입될 수 있도록 기준을 완화할 필요성이 있음

○ 정부의 사이버보안인력 양성계획과 부족문제 등을 개선하기 위해 정부와 민간의 협력이 필요할 것으로 보임

정보보호 인적자원개발위원회(ISC)

ISSUE REPORT

Ⅰ.

공공분야 보안관제 현황

I 공공분야 보안관제 현황

1. 사이버보안 법령

보안관제는 일반적으로 사이버보안의 범주에 포함되어 있으며, 이를 기반으로 사이버보안과 관련된 법제가 제·개정되어 왔다. 관련 법제로 공공부문은 「지능정보화기본법」, 「국가사이버안전관리규정」을 기준으로, 민간 및 금융 부문은 「정보통신망법」, 「전자금융거래법」 등을 기준으로 하며, 사이버보안의 목적으로 구분된 국가기밀보호는 「군사기밀보호법」 및 「보안업무규정」, 사이버보안은 「국가사이버안전관리규정」, 기반시설보호는 「정보통신기반보호법」, 그리고 개인정보보호는 「개인정보보호법」을 기준으로 각각 따르고 있다. 따라서, 우리나라의 사이버보안과 보안관제를 규율하는 일반법은 없으며, 각 분야별 개별법이 존재하고 그 개별법에 근거하여 사이버공격에 대응하고 있다.

보안관제센터를 설치하고 운영하는 전반적인 사항을 규정한 근거는 「국가사이버안전관리규정」과 「사이버안보 업무규정」 등 대통령 훈령에 제시되어 있으며, 「국가정보보안기본지침」은 보안관제센터의 구성과 인원 구성, 탐지규칙 정보 개발, 공격 정보의 탐지 및 보안관제 업무 직원에 대한 교육 등의 세부적인 사항을 명시하고 있다. 즉, 중앙행정기관, 지방자치단체 및 공공기관의 장은 「국가사이버안전관리규정」 제10조의2(보안관제센터의 설치·운영) 및 「사이버안보 업무규정」 제14조(사이버공격·위협의 탐지·대응)에 의거하여, 보안관제센터를 설치·운영하여야 하며, 「국가정보보안기본지침」 제131조~제138조에 따라 사이버공격을 효과적으로 대응할 수 있는 보안관제센터 인원 구성, 탐지규칙 정보 개발, 공격 정보의 탐지 및 보안관제 업무 직원에 대한 교육 등을 수행하도록 명시되어 있다.

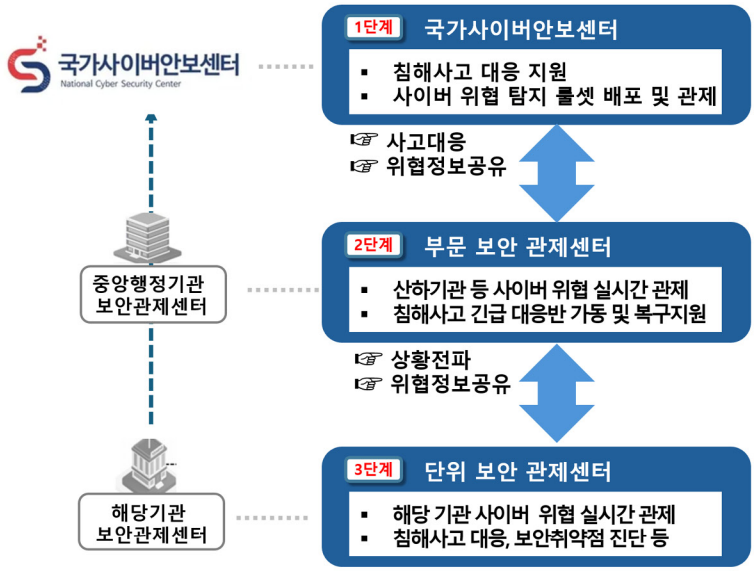
「국가정보보안기본지침」의 내용 중 보안관제센터와 관련된 세부사항을 살펴보면, 보안관제센터를 운영하는 기관의 장은 사이버공격의 탐지·분석·대응 등 보안관제 업무의 책임 있는 수행을 위해 정규직 직원으로 구성된 보안관제 전담 조직을 구성·운영하도록 운영조직을 명시하고 있다. 보안관제센터 인력 구성은 보안관제 대상기관의 규모 및 보안 관제센터의 여건에 따라 전담 조직을 구성할 수 있다.

보안관제센터를 운영하는 기관의 장은 사이버공격에 대하여 24시간 탐지·분석·대응할 수 있도록 상시 근무 체계를 구축·운영하여야 하며 총괄부서, 운영부서, 운영 인력 등으로 구분하여 구성한다. 보안관제센터의 운영조직 구성은 해당 보안관제센터 운영에 맞게 일정 수 이상의 전담 직원을 반드시 배정해야 하며, 외부 인력(보안관제 전문기업 등)을 활용하여 구성하는 경우 「국가정보보안기본지침」 제132조제2항에 따라 과학기술정보통신부장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」에 따른 보안관제 전문기업의 업무수행능력 평가기준 등을 준수해야 하고 보안관제 업무의 책임 있는 수행 및 보안관리 등을 위하여 적정한 수의 공무원 또는 정규직원을 상시 배치해야 한다.

국가·공공기관의 보안관제 운영 유형은 「국가사이버안전관리규정」과 「사이버안보업무규정」에 근거하여 단위보안관제(각급기관), 부문보안관제(중앙행정기관), 국가보안관제(국가사이버안전센터)로 구성된 3단계 사이버공격 탐지·차단체계를 구축하여 운영 및 연계하는 체계이다.

구분	내용	설치 근거
단위보안 관제센터	▪ 시·도, 시·도 교육청, 시·군·자치구, 교육지원청, 공공기관, 국·공립학교 및 군(軍)기관의 장이 해당 기관의 정보통신망을 대상으로 운영하는 보안관제센터	「국가사이버안전관리규정」 제10조의2제1항
부문보안 관제센터	▪ 중앙행정기관의 장이 해당 기관 및 관할 하급기관의 정보통신망을 대상으로 운영하는 보안관제센터 ▪ 「책임운영기관의 설치·운영에 관한 법률」 제4조제1항에 따라 설치된 국가정보자원관리원(이하 "정보자원관리원"이라 한다)의 장이 국가기관·지방자치단체의 공동 활용을 위하여 운영하는 정보통신망(이하 "국가정보통신망"이라 한다) 및 정보자원관리원에 입주한 기관의 정보시스템을 대상으로 운영하는 보안관제센터 ▪ 행정안전부장관이 지방자치단체의 정보통신망을 대상으로 운영하는 보안관제센터 ▪ 교육부장관이 시·도 교육청의 정보통신망을 대상으로 운영하는 보안관제센터 ▪ 한국인터넷진흥원이 운영하는 침해사고대응센터	「국가사이버안전관리규정」 제10조의2제1항 「사이버안보업무규정」 제14조제2항
국가사이버 안보센터	▪ 「국가정보원법」 및 「사이버안보업무규정」 제14조제1항 및 제3항에 따라 사이버공격·위협의 탐지 및 대응을 위한 설립된 보안관제센터	「사이버안보업무규정」 제14조제1항

[표 1] 공공 보안관제센터 유형



[그림 1] 공공 보안관제센터 체계

2. 공공분야 보안관제 위탁운영

보안관제센터가 구축된 해당 기관은 운영 주체에 따라 각급 기관이 직접 운영하는 방식과 「보안관제 전문기업 지정 등에 관한 공고」에 따라 지정된 보안관제 전문기업을 통한 위탁운영 방식으로 구분된다.

공공분야의 보안관제센터는 대부분 보안관제센터 유형 중 중앙행정기관급의 기관이 운영하는 "부문보안관제센터" 및 일부 공공, 소속기관이 운영하는 "단위보안관제센터"로 구축 및 운영되고 있으며, 대부분 「국가정보보안기본지침」 제132조제2항에 따라 과학기술정보통신부장관이 고시하는 보안관제 전문기업에 의해 위탁 운영되고 있다.

국내 보안관제 전문기업은 23개 기업이 지정받은 상태이며 44개 부문보안관제센터 및 약 50여개의 단위기관 보안관제센터에 보안관제 운영 인력을 파견하여 운영되고 있다. 관제센터의 규모, 관제범위, 소요예산별로 수십명에서 수명이 대부분 현장에서 파견 관제 형태로 운영 중이며, 일부 기관은 파견과 원격관제를 혼합한 형태로 운영 중이다.

번호	지정기업	지역	번호	지정기업	지역	번호	지정기업	지역
1	에스케이쉴더스(주)	경기	9	(주)케이티디에스	서울	17	씨엠티정보통신(주)	서울
2	한전케이디엔(주)	전남	10	삼성에스디에스(주)	서울	18	(주)씨큐넥스트	서울
3	(주)싸이버원	서울	11	(주)파이오링크	서울	19	(주)신한디에스	서울
4	(주)이글루코퍼레이션	서울	12	(주)가비아	서울	20	엔아이티서비스(주)	경기
5	한국통신인터넷기술(주)	서울	13	(주)에이쓰리시큐리티	서울	21	(주)메타넷티플랫폼	서울
6	(주)안랩	경기	14	롯데이노베이트(주)	서울	22	엔에이치엔클라우드(주)	경기
7	(주)윈스	서울	15	(주)엘지씨엔에스	서울	23	(주)두산	서울
8	(주)시큐어원	서울	16	(주)시큐아이	서울			

[표 2] 보안관제 전문기업 지정 현황

3. 보안관제센터 위탁운영 범위

일반적으로 각급 기관에서 보안관제센터를 구축하여 운영하기 위해 자체 보안관제센터 운영규정을 수립하고 보안관제센터 목적, 적용 범위, 조직 및 기능, 사이버 안전시스템 구축 운영, 공격정보 탐지 및 수집, 초동 조치 등 보안관제센터 운영에 관한 사항을 구체적으로 규정하고 있다. 이에 따라, 보안관제 업무를 위탁하는 경우 아래의 주요 과업 내용을 고려하여 위탁운영을 실시하고 있다.

보안관제 전문기업 위탁 시 주요 과업내용

- 보안관제센터 24×365 실시간 보안관제 실시
- 사이버 침해사고 분석 및 대응
- 사이버공격에 대한 보안위협 분석 및 기술 지원
- 사이버 침해시도 탐지 및 차단규칙 개발
- 보안관제센터 정보시스템 운영 및 유지보수
- 보안취약점 점검 및 예방, 개선활동 수행
- 보안관제 지침/매뉴얼/절차 현행화
- 최신 정보보호 동향 수집 및 분석
- 정보보호 교육 및 사이버위기 대응훈련 실시
- 정기 및 비정기 운영현황 보고서 작성
- 서비스 수준 협약

II.

공공분야 보안관제 용역 사업 분석

II 공공분야 보안관제 용역 사업 분석

1. 공공분야 보안관제 용역사업 계약 현황

보안관제 전문기업은 보안관제센터와 긴밀한 관계가 있으며 보안관제센터 운영은 보안관제 수행에 충분한 역량을 지닌 보안관제 전문기업과의 협업이 얼마나 효과적으로 이루어지는지 여부에 따라 많은 영향을 받을 수밖에 없다. 근본적으로는 보안관제센터의 운영에 있어서 적절한 역량을 보유한 보안관제 전문기업을 확보하는 것이 우선적으로 요구된다.

대부분의 공공분야 보안관제 위탁운영 용역사업은 해당년도의 보안관제 용역과 2년 혹은 3년의 다년도 보안관제 용역, 보안관제와 유지보수 통합 용역 등의 형태로 다양하게 발주된다. 또한, 제안요청서상 보안관제 용역사업의 필요 요청 인력 구성은 각 보안관제센터의 유형(단위, 부문)과 기관 보안관제 대상 범위의 규모 및 상주와 상주/원격 혼합된 형태에 따라 상이하지만 대부분 소규모 센터에서는 3~5명, 대규모 센터에서는 10명~15명 안팎으로 투입인력을 요청하고 요청 기준으로 편성되어 운영된다.

공공분야의 국가조직 관련 법과 규정상 보안관제를 수행하여야 하는 공공분야 수요기관은 2024년 기준 600여개 기관 이상이다. 보안관제센터 미구축기관 대부분이 예산, 고유업무 분야, 상위기관 위탁을 이유로 보안관제센터의 구축 및 운영이 진행되지는 않지만, 향후 사이버보안의 중요성으로 인해 공공분야의 보안관제 시장이 더욱 확대되고 신규 구축되는 보안관제센터 위탁운영이 대폭 증가될 것으로 예상된다.

2. 공공분야 보안관제 용역사업 개선 필요 사항

공공분야 보안관제 용역사업에서 요청하는 투입 인력은 다양한 기술자 등급으로 요청하고 있으나, 대부분 교대근무를 수행하는 초급 보안관제요원의 편성이 절반 이상이다. 초급 보안관제 전문인력은 각 대학, 전문대학, 일부 특성화고, 전문학원에서 지속적으로 양성하고 있지만 24시간 365일 운영되는 보안관제 업무 특성상 기관별 최소 8여명 이상의 인력 구성이 필요하다. 또한, 대부분의 관제센터는 고급, 중급, 초급 인력을 골고루 요구하고 있으나, 모든 기술 등급별 인력 수급이 어려운 상태이다. 보안관제 분야 외 보안 컨설팅, 보안시스템 구축 등 타 직무에도 보안 인력 수급 부족 현상은 나타나고 있지만 24시간 365일 주야간 교대근무의 특수성을 요하는 보안관제 업계의 인력 수급이 가장 어려운 문제로 확인된다. 특히, 이러한 인력 수급의 어려움은 초급기술자 확보부터 시작된다.

III.

보안관제 용역 사업 인력 수급 개선

III 보안관제 용역 사업 인력 수급 개선

공공분야 보안관제 용역의 대부분은 '보안관제 전문기업 지정 등의 관한 공고'에 별첨인 '기술인력의 자격기준'에 의거하여 분류되는 초급, 중급, 고급, 특급 기술자를 필요 인원에 따라 편성하여 요청하고 있으며, 일부 기관이 기존에 소프트웨어자격기준 등급으로 요청하고 있다. 보안관제센터 위탁운영 용역사업 인력 편성에 활용되는 기술 인력의 자격 기준은 다음과 같다.

<table>
<tr><th>구분</th><th>관련 자격 또는 관련 학력을 보유한 사람</th><th>관련 자격 또는 관련 학력을 보유하지 않은 사람</th></tr>
<tr><td>초급
기술자</td><td>▪ 학사 이상의 학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 사람
▪ 전문대학 졸업 또는 산업기사 자격을 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람
▪ 기능사 자격을 취득한 자로서 4년 이상의 자격을 취득한 자</td><td>▪ 학사 이상의 학위를 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람
▪ 전문대학을 졸업한 후 4년 이상의 정보통신 관련 경력이 있는 사람
▪ 정보통신 관련 경력 6년 이상 있는 사람</td></tr>
<tr><td rowspan="2">중급
기술자</td><td>▪ 1년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
▪ 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 3년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학 졸업 또는 산업기사 자격을 취득한 후 5년 이상의 정보보호 관련 경력이 있는 사람</td><td>▪ 학사 이상의 학위를 취득한 후 5년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학을 졸업한 후 7년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">▪ 초급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
<tr><td rowspan="2">고급
기술자</td><td>▪ 박사학위 또는 기술사 자격을 취득한 사람
▪ 4년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
▪ 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 6년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학 졸업 또는 산업기사 자격을 취득한 후 8년 이상의 정보보호 관련 경력이 있는 사람</td><td>▪ 학사 이상의 학위를 취득한 후 8년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학을 졸업한 후 10년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">▪ 중급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
<tr><td rowspan="2">특급
기술자</td><td>▪ 3년 이상의 정보보호 관련 경력이 있고 박사학위 또는 기술사 자격을 취득한 사람
▪ 7년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
▪ 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 9년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학 졸업 또는 산업기사 자격을 취득한 후 11년 이상의 정보보호 관련 경력이 있는 사람</td><td>▪ 학사 이상의 학위를 취득한 후 11년 이상의 정보보호 관련 경력이 있는 사람
▪ 전문대학을 졸업한 후 13년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">▪ 고급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
</table>

[표 3] 기술인력의 자격기준

대부분의 공공분야 보안관제센터는 PM의 자격을 특급기술자, 고급기술자로 요청하고 있으며, PL 및 침해사고 분석, 취약점 분석 등의 업무수행 인력은 고급기술자, 중급기술자로 편성을 한다. 실시간 보안관제 모니터링과 초동대응을 수행하며 주/야 교대근무하는 보안관제요원은 일부 중급기술자를 요청하는 기관을 제외하고 대부분 초급기술자를 요청하고 있다. 보안관제 업무를 수행하는 초급기술자의 업무 경력이 증가되면 중급과 고급기술자로 직무 업무가 변경되는 형태로 보안관제 직무가 운영되고 있다.

따라서, 보안관제센터의 인력 수급의 주요 공급은 초급기술자를 기반으로 운영되며 경력이 상승되고 한 단계 수준 높은 업무를 수행하게 되면서, 새로운 신규 초급인력이 수급되는 과정의 선순환 체계가 마련되어야 한다.

보안관제센터 용역사업에서 보안관제 모니터링을 담당하는 초급인력이 참여되는 자격기준은 대부분 관련 자격 또는 관련 학력을 보유한 사람으로, 초급기술자인 경우 관련 자격 란에 "학사 이상의 학위, 기사 또한 정보보호 관련 학위를 보유한 자" 이거나 "전문대학 졸업 또는 산업기사 자격을 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람"으로 명시되어 있다. 여기에서 관련 학위의 전공분야는 전기, 정보통신, 정보처리기술 등의 관련 전공이 모두 포함되며, 관련 자격은 "전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용" 종목으로 기술자격이 모두 포함된다. 따라서, 관제센터 초급기술자의 역할인 주야 교대근무 형태의 보안관제 모니터링 및 초동대응 직무는 대부분 처음 보안관제 분야에 입사해서 상위 기술직급인 중급, 고급기술자에게 기술을 전수받아 역량을 키울 수 있도록 관련 학위와 자격을 폭넓게 배치해놓은 것으로 보안관제 신규 인력 유입이 원활하도록 기준이 마련되어 있다고 볼 수 있다.

그러나, 공공분야 보안관제센터 용역사업의 제안요청 내용을 분석해보면 이러한 신규 인력이 참여할 수 없는 사업의 비율이 매우 높다. 최근 6개월간 공공기관에서 발주한 보안관제 용역사업 40여건을 분석한 결과 약 30%에 해당되는 12건의 사업에서 초급인력의 자격요건으로 학력, 자격기준 이외 "보안관제 경력 1년 이상" 혹은 "정보보안 경력 2년 이상" 등의 특수 요건이 포함되어 있음을 확인할 수 있다. 이러한 요건은 인력 수급이 어려운 보안관제 분야의 초급기술자가 보안관제 전문기업에 채용되어 공공분야 보안관제 업무에 투입되기 어려운 기준이다. 특히, 학사학위자임에도 경력이 요구되는 바 관련 전공의 전문대학, 특성화고 출신의 신규 직원을 채용하여 사업을 수행하기 어려운 조건이다. 공공분야의 보안관제 발주사업을 다년사업으로 확대 분석해보면 공공분야에 상당히 많은 사업들이 초급기술자의 자격요건 이외에 추가 특수 자격 사항으로 요청하는 사례가 더 많을 것으로 예상된다.

발주기관의 보안기술능력 제고 등의 필요사항이 있을 경우 중급, 고급기술자에 공공보안관제센터 근무경력, 악성코드 분석 경력, 취약점 분석 경력 등의 특약 요건이 특정 업무를 위해 필요할 수 있으나, 초급기술자는 관련된 학위와 자격요건으로 상주인력에 투입되어 실시간 모니터링과 초동 조치 대응 업무 기술을 숙련된 상위 기술자에게 전수받아 보안관제 업무를 수행하는 것이 공공분야 보안관제센터의 원활한 인력 수급과 더 나아가 보안관제 전문기업의 사업 참여가 활발해질 수 있는 방안이다.

IV.

결론

Ⅳ 결론

공공분야 보안관제센터는 기본적으로 실시간 모니터링 및 초동대응을 위해 초급기술자 위주의 인력 구성을 요구하고 있으나, 일부 발주사업에서 초급기술자에게 경력 요건을 추가하는 경우가 증가하고 있다. 이는 보안관제 전문 기업들이 초급 인력을 채용하여 신입 인력을 투입하는데 어려움을 초래하고 있으며, 추가 특수 경력 요건을 부가적으로 요구하는 경우가 많아 신규 인력의 진입 장벽이 높아지고 있는 상황이다. 이러한 경력 요건 강화는 보안관제 분야 인력난을 가중시켜 인력 수급에 어려움을 초래하며, 더 나아가 향후 사이버보안관제 수요가 대폭 증가할 상황에서 공공분야 보안관제센터의 인력 운용에 불균형적인 영향을 미칠 수 있다.

따라서, 보안관제 초급기술자의 경력 요건을 최소화하고 관련 학위와 자격을 보유한 인력이 원활하게 투입될 수 있도록 기준을 완화할 필요가 있다. 이를 통해 보안관제 전문기업들이 신규 초급기술자를 보다 쉽게 채용하고 교육할 수 있어야 한다. 보안관제 전문기업은 초급기술자를 대상으로 체계적인 경력 향상 프로그램을 운영하여 상위 기술자에게 업무를 습득하고 중급, 고급기술자로 성장할 수 있도록 지원하여 경력 경로를 명확히 설정하도록 돕고, 발주기관은 프로젝트 요구 사항에 따라 초급기술자 및 상위 기술자 배치를 조정할 수 있도록 유연한 조건을 마련해야 한다. 특정 보안관제 업무에 중급, 고급기술자의 참여가 필요한 경우 해당 업무에만 경력 요건을 명시하고, 초급기술자는 실시간 모니터링 및 초동 대응 업무를 통해 경력을 쌓도록 하는 방식이 적절할 것이다.

사이버보안 분야와 같은 기술 산업은 빠르게 성장하면서 인력 수요가 급증하고 있으며 기존 중급 및 고급 인력만으로는 이 수요를 충족하기 매우 어려우므로, 초급 인력을 확보하여 점진적으로 역량을 키우는 것이 필요하다. 또한, 초급 인력을 채용해 산업 내 인력을 확장하면, 향후 고급 인력으로 성장할 수 있는 기반을 마련할 수 있다.

정부의 사이버보안인력 양성계획과 부족문제 등을 개선하기 위해 공공분야 보안관제 발주기관과 보안관제 전문기업 등 정부와 민간이 협력이 필요하며, 초급 인력의 양성은 국가 전체의 사이버보안관제 기술 역량을 높이는 데 중요한 역할을 할 것이다.

이는 단순히 보안관제 인력 수급을 넘어서 사이버보안 산업의 장기적인 성장을 위한 필수적인 인력이 양성 전략에 기여할 것이다.

정보보호 인적자원개발위원회
Information Security Industrial Skills Council

ISSUE REPORT

(05717) 서울특별시 송파구 중대로 135, IT벤처타워 서관 14층
정보보호 인적자원개발위원회