https://doi.org/10.21186/IPR.2024.9.4.227

산업보안 시장에서의 탐정 직무역할에 관한 연구

손종욱*, 정은선**, 염건령***
㈜바핀파트너스 대표*, ㈜바핀파트너스 연구센터장**, 가톨릭대학교 행정학과 탐정학 교수***

A Study on the Role of the Private Investigator in the Industrial Security Market

Jong-Wook Sohn*, Eun-Sun Jeong, Yeom Keon-Ryeong*****
President, Vad Fint Partners Co.*, Director, Vad Fint Partners Co.,**
Professor, Major on Private Investigation, Catholic University of Korea***

요 약 본 연구는 산업보안 시장에서의 탐정 직무역할을 도출하는 것을 목적으로 한다. 이를 위하여 융합보안 프레임워크를 분석하여 x축을 예방-모니터링-사후관리로 설정하고, y축은 관리적 보안, 물리적 보안, 기술적 보안으로 설정하였다. 세부 직무 분류를 위해 ASIS 산업보안 자격증별 직무를 분석하여 프로세스에 따른 직무역할을 도출하였다. 연구결과 융합보안 관점에서 산업보안 탐정의 직무는 8개 영역에서 25개의 직무역할이 도출되었다. 직무영역은 예방-관리, 예방-물리, 예방-기술, 모니터링-관리, 모니터링-물리, 모니터링-기술, 사후관리-관리, 사후관리-물리보안, 기술보안으로 나타났다. 이를 통해 산업보안 산업에서 탐정의 직무와 역할과제를 도출할 수 있었고, 향후 산업보안 탐정의 직역 구체화 및 역할 활성화를 가능하게 할 것이다. 또한 본 연구 결과는 산업보안 시장에서 탐정의 직무역할을 제시하는 초기적 시도로 향후 탐정산업의 활성화 방안 연구의 기초로 활용될 수 있다.

주제어 : 산업보안, 탐정, 탐정직무, 산업보안탐정, 융합보안

Abstract This objective of this study is to identify the roles of private investigation in the industrial security market. In order to achieve this, the converged security framework was subjected to analysis, with the x-axis d efined as prevention, monitoring, and follow-up, and the y-axis defined as administrative security, physical secur ity, and technical security. To gain a more detailed understanding of job classification, the job duties were anal yzed using the ASIS industrial security certification framework, and job roles were derived according to the pro cess. As a result of the study, 25 job role derived from 8 areas for industrial security investigation from the p erspective of converged security. The job areas are as follows: prevention-management, prevention-physical, prev ention-technical, monitoring-management, monitoring-physical, monitoring-technical, post-management-management, post-management-physical security, and technical security. This study has enabled the duties and role tasks of p rivate investigation in the industrial security industry to be identified, and it has also facilitated the specification of the role of industrial security investigation and their revitalisation. Furthermore, the finding of this study repr esent an initial effort to delineate the role of the private investigarion in the industrial security market. It may serve as a foundation for future research into strategies for revitalising the private investigation industry.

Key Words : Industrial Security Market, Private Investigation, Private Investigation Job, Private Investigator of Industrial Security, Security Convergence

Received 01 Oct 2024, Revised 23 Oct 2024
Accepted 24 Oct 2024
Corresponding Author: Yeom Keon-Ryeong
(Catholic University of Korea)
Email: kicl2001@naver.com
ISSN: 2466-1139(Print)
ISSN: 2714-013X(Online)

© Industrial Promotion Institue. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 서론

최근 우리 사회는 AI, 데이터 등 디지털 전환 기술의 일상화로 인해 예측과 통제가 어려운 첨단화된 신종범죄에 대한 우려와 걱정이 증폭되고 있다[1]. 모방학습과 기술의 진보로 인해 발생하는 현대사회의 신종범죄는 공권력의 통제를 벗어나 심각한 양상으로 전개되고 있으며, 국가의 치안권에 의해 예방·감시·추적·징벌하지 못하는 다수의 신흥범죄 유형은 점차 증가하는 추세이다.

디지털 기술의 진보와 맞불려 신흥범죄가 발생하는 대표적인 시장 중 하나는 산업보안으로, 중소기업벤처부산하 대·중소기업·농어업협력재단에서 시행하는 '중소기업 기술보호 수준 실태조사'에 의하면 중소기업의 기술보호 역량점수는 56.8점으로 대기업 87.2점의 65.1% 수준에 불과했다[2].

2003년 국가정보원에서는 산업기밀보호센터를 설립하고 국가핵심기술 지정 및 해당 기술 중심 산업기밀 보호활동을 전개해 왔다[3]. 산업보안 가이드라인을 발표하고 산업체의 정보보호활동을 촉진해 왔으며, 이러한 노력으로 반도체, 디스플레이, 조선 등의 국가핵심기술의 유출[4]로 인한 기업이익의 침해 발생을 효과적으로 막았다는 평가를 받고 있다. 그러나 국가핵심기술을 보유한 연구소나 대기업이 아닌 중소·중견기업들의 형편은 크게 다르다.

중소중견기업들은 여전히 다양한 산업보안 침해사고의 위험에 노출되어 있고, 자구책으로 산업보안을 강화하기에는 다양한 제약요인이 존재하고 있다. 향후 중소·중견기업들의 산업보안 역량 강화를 위한 대책들이 필요하며, 기업의 유형·무형자산의 침해를 방지하고 손실 방지를 위한 적극적인 지원 프로그램의 도입이 필요한 시점이다.

2020년 8월 탐정이라는 명칭의 사용을 금지한 '신용정보의 이용 및 보호에 관한 법률(신용정보법)'에 대한 헌법재판소의 위헌 결정 이후 탐정업의 영업자유화가 시행되고 자유서비스업 형태로 승인되었다. 이에 탐정업은 탐정 및 조사서비스업(분류코드:75330)이라는 업종[5]으로 사업자 등록이 가능한 하나의 직업이 되었다. 민간조사업인 탐정업의 직무 역할은 사실조사(Investigation)를 바탕으로 범죄, 비위행위, 각종 사고 및 재난, 산업기밀유출 등 다양한 영역에서 원인을 조사하고 후속 처리 등을 지원하는 것이다.

최근에는 앞서 논의한 산업보안 영역에서 기업정보유출, 평판조사, 디지털포렌식 등의 사실조사 및 보안 컨설팅을 수행하는 탐정회사가 증가하는 추세이다. 대표적인 글로벌 탐정회사인 핑커톤社(Pinkerton), 콘스텔리스社(Constellis), 가드월드社(Gardworld), 크롤社(Kroll) 등은 모두 주요 서비스로 사이버 위험 진단 및 예방, 산업정보 유출사건 사실조사 및 공적 조사의 기초조사 서비스를 제공하고 있다. 또한, 공권력이 할 수 없는 피해 예방을 위한 선제적 조치 영역에서 산업·기업의 정보보호를 위해 필요한 산업보안 체계 전반에 걸친 컨설팅 서비스를 제공하고 있다. 이러한 해외사례와 마찬가지로 한국에서도 공권력 지원의 한계가 존재하는 산업보안 시장에서 한국 탐정기업의 민간조사 역량 활용을 위한 방안을 논의할 필요가 있다.

이상과 같은 배경 아래 본 논의에서는 산업보안 역량 강화를 위한 외주화 가능 영역을 중심으로 직무 역할과 직무 역량을 논의한다. 이와 더불어 국가 공권력이 효과적으로 대응하지 못하는 산업기밀 및 정보 유출에 대한 보완재인 산업보안 탐정의 역할강화 방안을 논의한다. 이를 통해 산업체의 수요와 산업보안 탐정의 역할과 역량을 효과적으로 매칭하고, 산업보안 시장에서 '탐정 서비스 주류화'가 이뤄질 수 있는 직무역할에 관한 기초 논의를 진행한다.

2. 산업보안의 개념 및 특징

2.1 산업보안의 개념

산업보안은 협의의 개념으로 '산업기술이나 기밀의 유출 방지'에 국한하고 있으며, 나아가 산업보안 활동은 '기업 비밀을 누설 또는 침해당하지 않도록 관리하는 활동'으로 정의된다[6]. 국가정보대학원이 편찬한 「산업보안실무」에서는 산업보안을 "산업 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 대응방안이나 활동"[7]으로 정의하고 있다.

또한 국가정보원이 편찬한 「산업보안업무편람」에서는 산업보안을 산업체・연구소등에서 보유하고 있는 기술・경영상정보 및 이와 관련된 인원・문서・시설・

통신 등을 경쟁국가 또는 업체의 산업스파이나 전·현직 임직원, 외국인 유치과학자 등 각종 위해 요소로부터 침해되지 않도록 보호하는 활동"으로 정의했다[8]. 이상의 산업보안에 대한 정의는 보호에 초점을 맞추고 있다.

나아가 Cunningham과 Taylor(1985)는 산업보안을 "범죄로부터 모든 경제활동을 보호하는 일체의 노력으로 정의할 수 있으며, 산업 및 기업의 자산보호(Asset Protection)와 손실방지(Loss Prevention) 활동"으로 정의하며 보다 확대된 개념을 제시한다[9]. 이 경우 산업보안은 단순히 보안 침해사고 예방이라는 협의적 의미에서 벗어나 자산을 보호하고 손실을 방지하는 예방과 감시/관제, 추적/징벌에 이르는 전주기(全週期) 활동을 의미하게 된다.

광의의 전주기 산업보안 활동은 협의의 정의나 정보보호산업과 차이가 존재한다. 협의의 정의나 정보보호 차원에서는 예방, 감시/관제를 중요한 목표로 보고 있다면, 광의의 산업보안은 자산보호와 손실방지를 넘어선 안정과 질서를 지키는 제반 활동을 포함하여 예방은 물론 추적/징벌 등을 위한 사실조사, 법적대응, 자력 구제 조치 등의 중요성이 강조되고 있다.

2.2 산업보안 시장의 특징

산업보안시장은 비대면 환경이 펼쳐져 다양한 정보보호 수요가 존재했던 팬데믹이 종식된 이후인 2022년에도 전년 대비 9% 급성장하였고 세계적인 저성장 기조가 예상되는 2024년에만 3.8%의 성장이 예상되는 시장이다. 정부는 정보보호 산업을 "정보보호를 위한 기술 및 정보기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련된 서비스를 제공하는 산업(정보보호산업법 제2조)"으로 정의하고 있다[10].

산업의 주요 목표를 첫째, 네트워크상의 정보 유출 및 훼손 방지, 둘째, 물리보안을 통한 안전안심생활, 셋째, 융합보안을 통한 안전성 강화로 하고 있으며, 특히 전통산업과 디지털 융합에 따른 디지털 융합시장으로 보안의 범위가 확대됨에 따라 융합보안 시장이 빠르게 성장하고 있다.

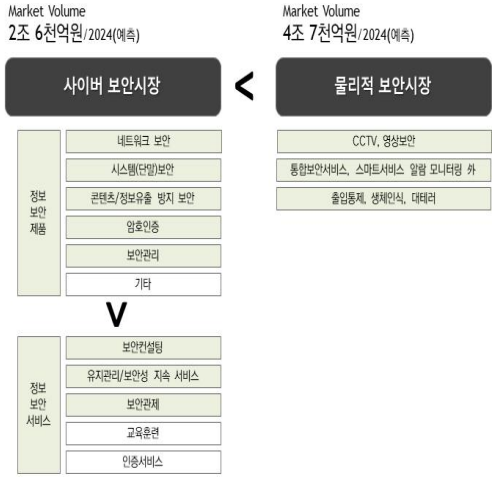
더욱이 최근의 스마트공장, 자율주행차 등의 디지털 융합산업의 정보보안 필요성에 대한 정관계의 인식이 강화되고 있다. 실제로 Market & Market의 리서치에 따르면 디지털 전환 시장에서 정보보호가 차지하는 비율은 약 13.8~15%로 매우 높은 비중을 차지할 것으로 전망하고 있다.

이러한 정보보호 시장은 크게 관리적 보안, 물리적 보안, 기술적 보안 등의 유형으로 구성된다. 관리적 보안은 인적 자산에 대한 보안, 절차/규정 등에 의한 보안, 조직 내부 정보보호체계 정립, 정보시스템 이용 및 관리절차 수립 등의 거버넌스 관련 보완활동으로 구성된다.

반면 물리적 보안은 설비/시설 자산에 대한 보안, 물리적 위협을 보호하기 위한 다양한 활동을 이야기하며 경비업의 활동 영역이다. 기술적 보안은 정보자산에 대한 보안으로 주로 예방기술을 활용한 IT 보안 영역을 지칭한다.

IT기술이 주도하는 2024년(예측) 국내 정보보호 시장 규모를 보면, 사이버 보안시장은 2조 6천억원, 물리적 보안시장은 4조 7천억원으로 물리적 보안의 시장규모가 더 크다. 사이버 보안시장만 놓고 보면 정보보안제품(IT기술과 소프트웨어) 시장이 정보보안 서비스(컨설팅, 보안/관제) 시장의 매출 규모보다 더 크다[11].

정보보호 시장 자체는 첨단 관제장비와 소프트웨어가 주도하는 시장이지만, 컨설팅, 관제 등의 물리적 보안 등의 정보보안 서비스 시장에서는 전문성을 가진 인력의 참여가 중요하다. 반면에 정보보호 시장에서는 전문인력의 참여가 차지하는 비중은 작은 편이다.

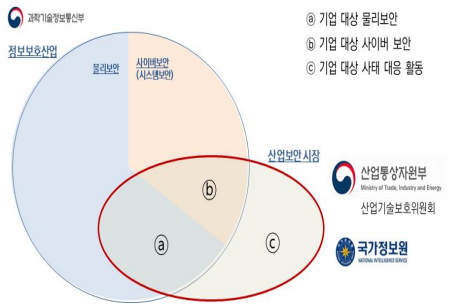


[그림 1] 2024 정보보호 시장의 규모

정보보호 시장이 IT기술 중심으로 구성된다면, 산업보안 시장은 상대적으로 인력에 대한 의존도가 크다. 산업기밀보호, 기업보안, 보안관리, 민간관리, 민영보안 등의 용어가 혼용되고 있는 산업보안 시장은 명확하게 그 역할과 기능이 있음에도 불구하고 정보보호, 비위행위감시, 통제장비, 인력경비 등 다양한 산업이 혼재된 융합보안 시장이므로 독자 산업으로 구분하지는 않고 있다.

이러한 산업보안은 정보보호 산업의 하위에 존재하고 있으며, 별도의 산업이라기보다는 하나의 시장으로 볼 수 있다. 산업보안이라는 용어는 2003년 10월 국가정보원 산업기밀보호센터가 설립되고 2006년 '관련법인 산업기술의 유출방지 및 보호에 관한 법률'이 제정되면서 제 18조, 제 20조 등에 산업보안기술과 보안산업 등을 법률용어로 구체화하면서[12] 일상적으로 사용되기 시작했다.

산업보안 시장의 위치를 명확히 하기 위해 정보보호 산업의 유형 내에 산업보안 활동을 맵핑할 때 정보보호의 하위 개념으로 산업보안 시장을 위치하도록 했다. 산업보안 시장은 하위시장인 동시에 예방적 개념의 정보보호 산업과 달리 예방-모니터링-추적/사후관리를 포함하는 시장이다.



[그림 2] 정보보호산업과 산업보안 시장의 관계

3. 산업보안 활동의 유형화 및 직무역할

3.1 융합보안 프레임워크 기반 직무

전통적인 산업보안 프레임워크는 물리적 보안, 관리적 보안, 기술적 보안 3개 영역으로 구성되어 있으며, 국가기관 및 공공기관의 보안감시도 이와 유사한 프레임워크를 중심으로 진행하고 있다. 전통적인 산업보안 프레임워크에서는 물리보안을 책임지는 경비원과 관제장비, 기술보안을 담당하는 정보통신 기술자, 소프트웨어가 주요 행위자로 인식되어 왔다[13].

산업보안의 복잡성에 따라 3개의 영역으로 구분된 산업보안 관리 행태의 한계가 제기되면서 보다 강력한 통합적인 융합보안(convergence security)활동의 필요성이 강조된다. 산업보안의 수행자도 물리적 보안 관리자에서 수행영역을 확장하여 분야별 전문탐정으로도 확장되고 있다.

즉, 전통적인 산업보안은 물리적, 관리적, 기술적 보안의 상호 연계된 분야에서 보안을 강화하는 것으로 정보보안 거버넌스를 강조하고 있는 반면, 융합보안활동은 각 산업별 특징을 반영한 보안활동이 필요하다는 인식 아래 특정 산업의 전문가(Filed Expert)가 참여하는 산업맞춤형 보안체계의 필요성을 강조한다. 융합보안으로의 패러다임이 전환되면서 Brooks(2010)[14]가 제안한 융합보안 모델, Gartner(2004)[15]의 융합보안모델 및 AESRM(Alliance for Enterprise Security Risk Management) 모델이 대표적으로 제시되고 있다.

Brooks의 융합보안 모델은 산업보안 전략 거버넌스를 최상위에 두고 경영관리, 오퍼레이션을 하위에 배치하여 융합보안을 위한 경영진의 방향성 제시, 조직의 전략과 운영방식이 잘 정렬되어 있어야 함을 주장했다. 산업보안 요소들을 2개의 Level로 구분하였는데, 산업보안 요소 중 위험관리, IT 및 컴퓨팅, 물리보안, 기술, 조사 등을 핵심기술인 Level 1로 제시하였다. 또한 비즈니스 연속성 관리(BCM), 관련법, 범죄학, 시설관리 등을 핵심기술은 아니지만 반드시 필요한 Level 2로 제시하는 통합 프레임워크를 제시했다.

이처럼 정보보호산업이 IT 중심의 예방활동을 중요하게 인식하고 있는 반면, Brooks의 융합보안 모델에서는 사고대응 즉 탐정의 전통적인 직무영역인 사실조사 역시 중요한 핵심기술로 보고 있다.

Gartner의 융합보안 모델은 물리적 보안과 사이버 보안이 통합되어 한층 더 높은 수준의 보안관리와 대응을 위한 프레임워크로 제안되었다. 융합보안 모델은 y축과 x축으로 나누어 격자형으로 구성되어 있으며, y축은 경영활동으로 경영관리, 기능, 프로세스, 기술을 포함하고 있다. x축은 대응방안으로 근절, 연계, 유사, 공통을 포함해 각 영역의 기능, 프로세스, 기술이 상호 연계된 정도

에 따라 세 가지의 수준으로 유합되어 하나의 영역에서 관리되도록 한다.

융합보안 논의를 주도하고 있는 AESRM(The Alliance for Enterprise Security Risk Management)에서 제시한 융합보안 모델인 AESRM은 미국의 ASIS(미국산업보안협회), ISSA(국제정보시스템감사통제협회, Information System Security Association), ISACA(정보시스템 감사 및 통제협회, Information System Audit and Control Association) 등 3개 협회가 연합하여 구축했다. AESRM 모델은 전통적인 프레임워크를 y축, 보안 프로세스를 x축에 두고 융합보안 요인들을 제시하고 있다[16].

산업보안 프레임워크의 패러다임은 기존의 개별화된 보안체계로는 첨단화, 지능화, 이해관계 중첩화, 산업의 융합화 및 전문화 속에서 증가하고 있는 기업의 보안 유출 사고를 효과적으로 예방할 수 없는 한계로 인해 예방 및 보안관리의 범위로 확장하며 전환되었다. 산업보안 영역의 확장으로 인해 탐정의 직무 범위가 넓어질 수 있으므로, 융합보안 프레임워크를 중심으로 탐정의 전문성과 기업의 수요가 매칭되는 직무에 대한 논의가 필요하다.

3.2 확장된 융합보안 프레임워크와 탐정의 직무

본 연구에서는 산업보안 탐정의 직무 분석을 위해 선행연구에서 제시된 AESRM 모델에 근거하여 x축을 프로세스(예방-모니터링-사후관리(사고대응))으로 설정하고, y축을 관리, 물리, 기술보안 3개 프레임워크를 적용한 매트릭스 형태의 융합보안 프레임워크를 재구성한다. 이러한 재구성을 통해 산업보안의 각 단계별 프로세스 중 탐정의 직무를 탐색하기 위한 프레임워크로 활용하고자 한다. 프레임워크의 재구성은 기존의 IT 기술 중심에서 벗어나 산업보안 활동의 확장 관점에서 탐정의 직무 역량을 활용하여 융합보안 수요를 탐색하기에 유용하다.

또한 ASIS 자격체계에 따른 직무역할(Job Domain)과 산업보안 탐정의 직역을 매칭하였다. 전통적인 정보보호, 산업보안 프레임워크인 관리, 물리, 기술보안 등 기존의 유형화된 활동을 적용한 y축과 달리 x축은 AESMR의 프로세스인 예방(Prevent) → 추적관리(Detact) → 사고대응(Respond)을 변형하여 예방(Prevent) → 모니터링(Monitoring) → 사후관리(Respond, Investigation) 등 3단계 프로세스를 적용하였다. 이러한 프로세스 변형은 美 ASIS의 자격체계[17]를 기준으로 진행했다.

미국 ASIS에서는 4개의 자격체계를 운영 중이며, 이러한 자격체계는 제시한 프로세스에 맞게 구분하여 운영중에 있다. 4개의 자격증은 CPP(Certified Protection Professional), PCI(Professional Certified Investigator), PSP(Physical Security Professional), APP(Associate Protectional Professional)이며, 이중 분야 입직 성격인 APP 자격을 제외한 CPP는 각각 기획/총괄(예방전략 수립, 전체 프로세스 운영), PCI(사고대응, 사건/사실조사), PSP(물리적 보안, 관리 및 모니터링)는 3단계 프로세스의 직무역할과 직무역량을 제시하고 있다.

CPP(Certified Protection Professional)는 최고 보안관리자를 위한 자격증으로 전체 프로세스를 기획하고 관장할 수 있는 역량을 보유했음을 증명한다. 해당 자격을 취득하기 위해서는 석사 학위 후 5년, 학사학위 후 6년, 학위가 없는 경우 7년의 현업 종사 경력이 있어야 하며, APP 자격증을 취득할 경우 위의 기간에서 1년을 감해준다[18].

PCI(Professional Certified Investigator)는 케이스 조사, 증거 수집, 구체적인 진술 조사 내용을 보고하는 사고발생 대응 활동 수행 역량을 보유했음을 증명한다. 해당 자격을 취득하기 위해서는 석사 학위 후 3년, 학사 학위 후 4년, 학위가 없는 경우 5년의 현업 종사 경력이 있어야 하며, APP 자격증을 취득할 경우 학사, 학위가 없는 경우에 한 해 1년의 경력을 인정해 준다[19].

PSP(Physical Security Professional)는 물리적 보안, 관제, 모니터링을 담당하는 자격으로 위협조사, 통합보안 시스템 설계, 시스템 운영 및 유지 보수 등의 수행역량을 보유했음을 증명하는 자격증으로 PCI와 동일하게 석사, 학사, 학위가 없는 경우 각각 3년, 4년, 5년의 현업 경력이 필요하며, APP 자격증 취득 시 학사는 3년, 학위가 없는 경우 4년이면 자격취득 자격이 부여된다[20].

이러한 각 자격시험 가이드에는 해당 자격증 취득자들이 수행해야 하는 직무역할과 범위에 대해 구체적으로 제시하고 있는데, 이는 <표 1>과 같다. CPP(Expert Level)와 APP(Beginer Level)는 수준의 차이는 있으나 공통 직무를 보면 보안 프로그램 기획, 평가와 지속적 개선, 사태 대응 계획 수립, 자원의 효율적 관리 등의 전반적인 직무영역을 가지고 있다.

산업보안 탐정의 직역에서 보면 ① 보안 프로그램의 진단 및 지속적 개선, ② 임직원 보안인식 강화 프로그램 개발, ③ 법적 조치에 필요한 증거의 획득, ④ 인사 결정에 필요한 평판체크, ⑤ 직원 일탈행위 방지를 위한 감시, ⑥ 임직원 보호계획 수립(경비), ⑦ 물리보안 프로그램의 개발, ⑧ 보안 위협요인 평가 및 우선순위화, ⑨ 비즈니스 연속성 관리, ⑩ 보안침해사고 예방계획 수립, ⑪ 사고 리뷰 및 분석, ⑫ 증거수집 및 사고 리뷰, ⑬ 사고대응 활동 평가, 감사 및 모니터링, 분석 등의 수행이 가능하다.

PCI의 직무는 현재 보편적인 탐정의 직무와 동일한 사실조사의 영역으로 ① 이해충돌 사례 분석, ② 사건조사 목표 및 전략, 리스크 진단, ③ 사실조사 자원의 관리 및 결정, ④ 사실조사 실행 프로세스 식별, 평가, 실행, ⑤ 물리적, 행위적, 전자적 수단을 활용한 감시/관제 실행, ⑥ 인터뷰 등 사실조사, ⑦ 증거의 수집 및 조사실행, ⑧ 타 기관/조직의 정보 획득, ⑨ 사실조사 기술의 활용, ⑩ 사실조사 결과의 보고 등이 주요 직역이며, 해당 직역은 현재 산업현장에서 활동하고 있는 탐정의 직무와 동일하다.

물리보안 직무전문가 자격인 PSP의 직역에는 물리보안 계획 수립 등 기획 업무 수행도 가능하지만, ① 리스크 분석, ② 물리보안 수단의 결정, ③ 물리보안 프로그램 모니터링 및 평가 등이 산업보안 탐정의 전문영역인 동시에 수행이 가능한 영역이다.

<표 1> ASIS 산업보안 자격증 별 직무(Job Task)

자격체계	주요 직무 도메인
CPP (Certified Protection Professional) + APP (Associate Protectional Professional)	☞ CPP: 산업보안 총괄 관리자 및 최고 전문가(Professional) 수준 ☞ APP: 산업보안 입문자(Associate) 수준 공통 직무영역(Job Domain & Task) ☐ 조직 보안 프로그램의 실행 및 조율 역할 ☑ 진단, 감사 등을 통한 보안 프로그램의 지속적 개선 ☐ 법, 제도 등 외부 기관과의 관계 강화 및 협조(대관업무) ☑ 임직원의 보안인식 강화 프로그램 개발 및 실행 ☐ 사실조사 프로그램의 실행 및 조율 ☑ 소송/고발을 위한 문서, 진술 등의 증거 확보 및 지원 ☑ 채용, 승진 등의 인사에 대한 평판체크 (Background Investigation) ☑ 직원 일탈행위 방지를 위한 프로그램 개발, 실행, 조율, 평가 ☑ 임직원 보호 프로그램 실행 ☑ 자산 보호를 위한 물리보안 프로그램 개발 및 운영 ☑ 물리보안 계획 수립 및 조율을 통한 보안 위협 감소 ☐ 조직성과목표 달성을 위한 보안 프로그램 통합 및 평가
	☐ 정보보안을 위한 보안정책의 실행 및 조율 ☐ 보안 예산 수립 및 예산 통제 ☐ 보안절차 및 기술의 개발 및 관련부서의 생산성 향상 ☐ 보안실무 인력의 역량개발 ☐ 윤리경영 문화 모니터링 및 육성 ☐ 보안 외주사와의 계약협상, 보안 KPI 개발 ☑ 보안 위험요인 평가 ☑ 잠재적 사고 위협 평가 및 우선순위화 ☐ 위협의 식별, 유형화, 정의 등을 조직 구성원에게 커뮤니케이션 ☐ 새로운 위협 대응 전략 수립 ☑ 비즈니스 연속성 관리 (COOP, Continuity or Continuity of Operations Plan) ☑ 사전 사고예방 계획 수립 ☑ 우수사례 기반 사고 대응 및 관리 ☑ 사고 수습 및 회복을 위한 코디네이팅 ☑ 사고 리뷰 및 분석 ☑ 비상(사태) 계획의 실행 ☑ 취약성 식별 및 사고 후 성능이 저하된 자산에 대한 대책 마련 ☑ 사고 영향력 최소화 ☑ 증거수집 및 사고 리뷰 ☑ 사고대응 간 신고 및 긴급대응 태세 유지 ☑ 사고대응 효율성 리뷰 ☑ 현 상황에 대한 조직 구성원, 핵심 이해관계자 대상 소통 ☑ 사고에 대한 조직 대응상황 감사 및 모니터링
PCI (Professioanl Certified Investigator)	사고대응, 사건조사 실무 전문가 수준 ☑ 윤리(이해충돌) 사례 분석 ☑ 케이스 분석 및 전략, 리스크 진단 ☑ 사실(사건)조사 목표 및 전략 개발 ☑ 사실조사 자원의 관리 및 결정 ☑ 사실조사 실행 프로세스 식별, 평가, 실행 ☑ 물리적, 행위적, 전자적 수단을 활용한 감시관제 실행 ☑ 개인 인터뷰 실행 ☑ 증거의 수집 및 보존 ☑ 물리적, 디지털, 전자적 수단을 활용한 조사 실행 ☑ 정부기관, 타 조직으로부터의 정보 획득을 위한 협업 ☑ 사실조사 기술의 활용 ☑ 사실조사 결과의 보고 ☑ 사실 증언의 준비
PSP (Physical Security Professional)	물리보안 실무 전문가 수준 ☐ 물리보안 진단계획 개발 ☐ 자산의 가치와 손실 피해 규모 파악을 위한 자산의 사전 식별 ☐ 위협의 본질과 위험 진단 ☐ 영향력 진단 실행 ☑ 리스크 분석 실행 ☐ 보안 프로그램의 성과요구 수준 결정 ☑ 적절한 물리보안 수단의 결정 ☐ 물리보안 시스템과 프로젝트 구상/계획 ☐ 물리보안 장비의 입찰 준비 ☐ 조달 계획 수립 ☐ 장비 및 서비스의 실행/운영 관리 ☐ 보안 부서 구성원의 프로그램 지원 요구사항 정리 ☑ 프로그램 모니터링 및 평가

4. 산업보안 탐정의 직무역할 도출

선행연구 분석을 통해 산업보안 시장에서 탐정의 활동이 진행되고 있거나 확장될 수 있는 영역을 재구성한 융합보안 프레임워크에 매칭하여 분석한 결과 총 8개 영역에서 25개의 직무역할(job role, job domain)이 도출되었으며 다음과 같다.

① 예방-관리 : 해당 영역은 임직원의 (1) 보안인식 강화나 (2) 일탈행위 방지, (3)보안 위협요인 평가 등에서의 역할이 가능하며, 한 단계 높은 전문성을 축적할 경우 (4) 보안사고로 인한 침해를 최소화하는 비즈니스 연속성 관리에서 활동이 가능하다. 해당 부분에서 활동하는 탐정은 산업보안 컨설턴트의 역할을 수행하며, 경영자문 등의 방식으로 전체 보안업무를 조직화하고 거버넌스를 확립하는 전문가적 조언을 제시할 수 있다.

② 예방-물리 : (5) 사전 사고예방 계획을 수립하거나, (6) CCTV, 출입통제 장비 등의 설치 및 운용을 기획하는 물리보안 계획을 수립하는 역할을 할 수 있다. 이미 산업보안 탐정기업들은 적절한 관제장비를 통해 핵심 자산을 지키는 활동을 기획하거나 컨설팅을 제공 중이지만, 이러한 활동이 탐정들의 직역이라고 사회적으로 인정을 받지 못하고 있다. 오히려 이런 직역을 경비회사나 민간 군사기업의 영역이라고 인식하고 있다.

③ 예방-기술 : 美 ASIS에서도 ISSA(국제정보시스템감사통제협회, Information System Security Association), ISACA(Information System Audit and Control Association)와의 전문영역을 상호 인정해 주는 관점에서 적극적인 IT 중심 기술보안 역량강화 교육이나 자격체계를 운영하지 않고 있다. 이런 분야에서 일하고자 하는 탐정들은 오히려 IT 기술 중심 자격체계 취득을 권장하고 있다. 하지만 CPP 등의 포괄적인 산업보안 기획 및 전문가 직역 내에 관리적 보안 관점에서 기술보안을 다룰 수 있도록 허용하고 있는데, 대표적인 것인 IT 보안을 담당하는 장비의 구입과 인력의 관리이다. 산업보안 고위 전문가인 탐정들에게 (7) 기술보안을 담당하는 인력에 대한 평판체크 및 감시 등을 의뢰하고 있다.

④ 모니터링-관리 : 탐정들은 일상적인 산업보안 감시 활동에서 특정 직무를 부여받고 있는데, 대표적인 것은 (8) 산업보안 침해 및 위기관리 활동에 대한 상시 자문을 제공하는 것과 (9) 조직 내에서 근무 중인 보안인력의 역량개발을 지원하는 것이다. 글로벌 탐정회사들은 관리보안의 실행 과정에서 전문가적인 자문, 자체 인력의 역량개발이나 역량보조 등의 서비스를 제공하고 있다.

⑤ 모니터링-물리 : 관제장비의 노후화 혹은 신기술, 새로운 장비들의 등장으로 산업보안 침해 위협으로부터 더욱 안정적으로 회사의 자산을 지키고 손실을 방지하려는 기업들이 늘고 있다. 새로운 장비를 도입하거나 새로운 통제수단을 구매, 설치하여 산업보안 역량을 강화하고자 하는데, 이 과정에서 물리보안 전문가로서 탐정의 역할은 중요하다. (10) 적절한 물리보안 수단을 제안하거나, (11) 일부 산업보안 활동들을 외주화해서 받고, (12) 주기적인 프로그램을 평가하고 개선사항을 도출하는 진단 프로그램을 운영할 수 있다.

⑥ 모니터링-기술 : 상시 보안활동이 진행되는 과정에서 (13) 도입된 기술 시스템들의 효과성을 평가할 수 있다. 실제로 전사적 산업보안 프로그램 진단을 진행하는 과정에서 탐정의 전문성을 활용하여 서비스를 제공하는 탐정회사들이 존재하고 있다.

⑦ 사후관리-관리(After Event, 사고대응) : 사고 발생 이후 재발 방지 및 더 높은 산업보안 태세를 갖추고자 하는 기업들을 대상으로 (14) 취약성 분석 및 개선방안을 제시하는 사후 평가를 제공할 수 있고, (15) 진행된 혹은 진행 중인 사고대응 활동에 대한 감사 및 모니터링을 진행하거나 개선 방안을 제시하고 있다. 특히 대규모 개인정보가 유출되거나 국가핵심기술의 유출, 기업의 핵심적인 산업기밀이 침해된 시급한 상황일수록 사고의 원인을 규명하고 이를 활용하여 비즈니스 연속성을 보완·강화하기 위한 탐정의 전문가적 활동을 필요하다.

⑧ 사후관리-물리보안, 기술보안 : 한국의 중견기업들은 산업보안 침해사고가 발생하여도 수사에 걸리는 시간, 사실 및 증거 확보의 어려움 등으로 인해 경찰에 이를 의뢰하거나 변호사에게 사건을 위임하는 경우가 많지 않다. 따라서 해당 부분은 산업보안 탐정의 고유 직역으로 인식되는 동시에 현재 많은 탐정회사들이 활동하고 있다. 대표적인 활동은 (16) 사실조사 계획 수립(목표 및 전략), (17) 인터뷰 기반 사실조사, (18) 디지털포렌식 기반 사실조사, (19) 물리적, 전자적 수단을 활용한 감시/관제 실행, (20) 증거 수집 및 보존, (21) 타 기관, 조직과의 협업, (22) 사실조사 기법 활용, (23) 사실조사 결과 보고, (24) 사실에 대한 증언 준비(법정, 경찰 수사 시 진

술에 참여), (25) Lessons Learned, 즉 사고 발생에 대한 대응과정에서 습득한 지식과 사건을 통해 피해를 최소화하고 빠르게 회복할 수 있는 조치 방안을 제안하는 역할을 하고 있다.

산업보안 고도화 관점에서 IT기술(소프트웨어, IT전문가 등) 외 다양한 인적자원과 물리적 보안 수단의 활용이 필요하다. 현재 적용되는 융합보안 역시 예방 관점, IT 중심에서 예방과 사고대응을 동시에 고려하고 다양한 외부 전문가들이 참여하는 형태로 전개되고 있다. 이러한 확장된 융합보안 개념 속에서 산업보안 탐정의 직무역할도 동시에 확장된다. 기존 탐정의 직무역할은 사고대응(사실조사)과 평판조사(보안인력)에 집중되고 있었으나, 융합보안 체계에서는 기술적 보안을 포함한 전 영역에서 탐정의 역량 활용이 가능하다.

[그림 3] 융합보안 프레임워크 내 산업보안 탐정의 직무영역

5. 결론 및 제언

본 연구에서는 산업보안 탐정의 직무역할 분석을 위해 선행연구를 기반으로 탐정융합보안 프레임워크를 재구성하여 도출하였다. 제시한 융합보안 프레임워크의 산업보안 탐정의 직무역할은 탐정서비스가 고도화된 영국, 미국, 일본 등과 같은 국가에서는 보편화된 탐정서비스 중 하나이다. 미국의 노동통계국(US Bureau of labor statics)에 따르면 탐정(private detectives and investigators, 민간수사관 및 조사요원)의 고용은 2022년에서 2032년까지 6% 증가하여 다른 업종보다는 빠르게 증가할 것으로 전망되고 있다[21].

또한 디지털 기술의 일상화로 인한 다양한 보안침해 요인에 대비하기 위한 글로벌 탐정기업도 다양화되고 있다. 메이저 탐정기업일수록 자국뿐만 아니라 전 세계에서 해외 진출 기업의 산업보안 활동을 지원하고 있고, 보다 전문적인 기술 보안 서비스를 제공하기 위해 IT회사를 M&A 하는 등 서비스 수요 다양화에 대응하고 있다.

하지만 한국은 탐정업의 합법화 이후 규제의 명확성을 제공하는 탐정 법제화가 진행되지 않았고, 더욱이 산업보안과 같은 국가안보의 상위 아젠다에서는 큰 역할을 하지 못하고 있다. 향후 산업보안 분야를 반드시 탐정의 직무역량이 잘 활용되어야 하는 직무영역으로 인식하고, 탐정이 역할을 할 수 있도록 사회적 인식 개선과 함께 그 활동 범위를 확대해 나가야 할 것이다.

특정 산업이 발전하고 주류화되는 과정을 설명한 이론 중에 Vargo and Lusch(2004)[22]의 연구에서 강조한 서비스 도미넌트 로직(Service Dominant Logic)과 본 연구 결과는 맥락을 같이 한다. 여기서 강조하는 점은 제품과 서비스를 결합하는 통합적이고 융합적인 혁신이 결국 수동적 자원인 도구, 장비 등을 능동적 자원인 역량, 지식, 기술 등으로 확장시켜 사회에 영향력을 발휘하는 핵심산업으로 성장한다는 점이다.

즉, 공동가치의 생성이라는 경제적인 목표를 달성하기 위해 교환단위로서의 서비스, 경험, 활용자원으로서의 지식, 기술 같은 무형의 자원들이 상호 연계되어 서비스가 주류화된다고 보고 있다. 실제로 제품을 사용하는 과정에서 가치가 창출(Value-in-use)되고 지속 가능한 서비스 생태계를 조성하고 생태계 안의 모든 행위자들이 상호 이익이 되는 방식으로 가치를 교환한다고 주장했다.

산업보안 시장에서의 탐정 서비스는 이러한 서비스 도미넌트 로직 경로를 추구해야 한다. 즉 물리보안, 기술보안의 수동적 자원들이 탐정이 가진 역량, 지식, 기술 등과 융합하여 안전, 자산의 보호라는 공공 가치를 창출해야만 주류화된 서비스가 가능하다는 것이다. 이 점에서 서비스 제공자의 핵심역량(역량, 지식, 기술)이 고도화되는 것이 중요하며, 산업보안 탐정의 활동은 경비, 민

간군사기업, IT회사의 제품과 서비스를 상호 연계하여 활용할 수 있을 때 주류화된다는 점을 주목해야 한다.

서비스 도미넌트가 완성되기 위해서는 산업보안 탐정의 역량 제고 및 서비스 범위의 확장, 산업보안 탐정의 증가, 자원의 통합, 활발한 서비스 교환, 법적·제도적 정비, 생태계 조성 등의 프로세스 이행이 필요하다. 이를 위해 본 논의에서는 기초적인 산업보안 시장에서의 탐정의 직역을 탐색했다. 이런 논의를 토대로 보다 전문적인 연구들이 진행되어야 하므로 산업보안 탐정의 주류화를 위해 다음과 같은 후속 논의를 제안한다.

첫째, 산업보안 탐정들이 활동하는 현재의 시장에서 탐정들이 서비스를 제공하고 있는 분야, 서비스를 제공할 수 있으나 수요가 없는 분야, 서비스 수요는 있으나 탐정이 서비스를 제공할 수 없는 분야 등 시장 세그먼트 분석이 보다 정교하게 진행되어야 할 것이다. 이 과정에서 많은 기업들의 수요를 설문조사하고 고객들의 탐정서비스 이용 경험을 분석해야 할 것이다.

둘째, 현재의 산업보안 탐정의 활동영역 외에 위에서 논의한 다양한 확장 영역에서 활용할 수 있는 탐정의 역량에 대한 후속 연구가 진행되어야 할 것이다. 이러한 역량 연구는 곧 다양한 학습과 역량강화 기회의 제공으로 이어져 더 능력 있는 산업보안 탐정을 확보하고 활용할 수 있을 것이다. 이렇게 될 경우 탐정서비스의 활성화가 이루어져 산업보안 시장의 수요와 역량의 매칭이 가능할 것이다.

셋째, 핵심역량에 기반한 산업보안 탐정의 자격체계가 구축되어야 할 것이다. 물리보안, 기술보안 산업과 공동으로 산업보안 분야에서 고객이 원하는 서비스를 제공할 수 있는 최소한의 자격체계가 필요하다.

넷째, 산업보안 탐정 직무역할 수행을 통해 나타나는 다양한 성과들을 증명하고 그 성과의 동인을 찾는 연구가 필요하다. 이를 통해 사회가 요구하는 산업보안 전문가의 역량이 구체화되어 전문 탐정에 의한 서비스 주류화가 완성될 수 있을 것이다.

참고문헌

[1] Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges, Journal of Ambient Intelligence and Humanized Computing, 14(8), 10517-10553.

[2] 과학기술정보통신부·정보보호산업협회(2022). 『2022 정보보호 실태조사』, 193-194, 정보보호산업협회.

[3] 이준호·신승수 (2021). 산업안보 개념 정립에 따른 국가 핵심 기술 확대 필요성 연구, 한국산업보안연구, 11(1), 327-349.

[4] 최선영·임현묵 (2024). 국가핵심기술과 전략기술의 관계 정립과 체계적인 보호관리를 위한 개선방안, 한국산업보안연구, 14, 137-160.

[5] 통계청 (2024). 『제11차 한국표준산업분류』, http://kostat.go.kr. 통계청.

[6] 이창무 (2011). 산업보안의 개념적 정의에 관한 고찰. 한국산업보안연구, 2(1), 73-90.

[7] McCrie, R. (2021). American Society for Industrial Security(ASIS), In Encyclopedia of Security and Emergency Management. Cham:Springer International Publishing, 17-22.

[8] 국가정보원 (2002). 『산업보안업무편람』, 국가정보원, 3.

[9] Cunningham, W. C., & Taylor, T. H. (1985). Private security and police in America: The Hallcrest report. Portland, OR: Chancellor Press, 186.

[10] Talbot, J., & Jakeman, M. (2011). Security risk management body of knowledge. John Wiley & Sons, 53-269.

[11] Tyson, D. (2011). Security convergence: Managing enterprise security risk. Elsevier, 33-141.

[12] 한상암·김윤영(2024). 산업기술 유출범죄 대응역량 강화방안 고찰. 한국민간경비학회보, 23(2), 235-268.

[13] 임양규·박원형·이환수 (2023). 산업기술 유출 방지를 위한 보안 프레임워크 연구. 융합보안논문지, 23(4), 33-41.

[14] Brooks, D. J. (2010). What is security: Definition through knowledge categorization. Security Journal, 23, 225-239.

[15] Gartner. (n.d.). Definition of Operational Technology (OT). Retrieved March 14, 2022, https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

[16] Wakefield, A. (2014). Corporate security and enterprise risk management. In Corporate Security in the 21st Century: Theory and Practice in International Perspective, London: Palgrave Macmillan UK, 235-253.
[17] Westby, J. R., & Allen, J. H. (2007). Governing for enterprise security (GES) implementation guide, CMU/SEI, 1-61.
[18] Chapple, M., & Seidl, D. (2022). (ISC) 2 CCSP Certified Cloud Security Professional Official Study Guide. John Wiley & Sons, 151-245.
[19] Johnson, M. P., & Spivey, J. M. (2008). ERM and the security profession, Risk Management, 55(1), 30-35.
[20] Fischer, R., & Halibozek, E. (2008). Introduction to security. Butterworth-Heinemann, 47-86.
[21] U.S.Bureau of Labor Statistics. (2023). Occupational Employment and Wage Statistics. Private Detectives and Investigators, https://data.bls.gov/search/query/results?cx=013738036195919377644%3A6ih0hfrgl50&q=Private+Investigator.
[22] Vargo, S. L., & Lusch, R. F. (2004). Evolving to a new dominant logic for marketing, Journal of marketing, 68(1), 1-17.

손 종 욱 (Jong-Wook Sohn)

- 2009년 05월~2024년 현재: ㈜바핀파트너스파트너, 대표이사
- 1999년 08월: 중앙대학교 일반대학원 정치학 석사(국제정치 전공)
- 2023년 3월~2024년 현재: 가톨릭대학교 일반대학원 행정학과 탐정학전공 박사과정 재학
- 관심분야: 국제개발협력, 공공외교, 인사조직/인재개발, 공공정책 컨설팅, 밸류체인, SV, 산업보안, 탐정산업
- E-Mail: jwsohn@vfp.co.kr

정 은 선 (Eun-Sun Jeong)

- 2022년 9월~2024년 현재: (주)바핀파트너스 연구센터장
- 2022년 8월: 전북대학교 일반대학원 교육학 박사(교육심리·상담 전공)
- 2023년 3월~2024년 현재: 가톨릭대학교 일반대학원 행정학과 탐정학전공박사과정 재학
- 관심분야: 교육, 인재양성, 공공정책, 교육평가, 인사조직, 탐정윤리
- E-Mail: eunsunj8@gmail.com

염 건 령 (Keon-Ryeong Yeom)

- 2022년 9월~2024년 현재: 가톨릭대학교 행정대학원 탐정학전공 교수
- 2011년 8월: 국제문화대학원대학교 교육학 박사(청소년지도학 전공)
- 2015년 3월~2024년 현재: 한국범죄학연구소 소장
- 관심분야 : 탐정학, 행정학, 사회학, 통계학
- E-Mail: kicl2001@naver.com