사이버안보연구, 2집 1호 2025 여름, 005-043

사이버 보안 진단 전문인력 자격제도 도입에 관한 연구

0201-005043

임지훈 | 고려대학교 정보보호대학원

* 이 논문은 2024년 11월 2일 한국사이버안보학회 연례학술대회에 발표한 내용을 토대로 한 것임

논문접수일 2025년 6월 5일 | 논문심사일 2025년 6월 27일 | 게재확정일 2025년 6월 29일

논문 요약

디지털 전환이 가속화되면서 사이버 위협은 양적으로 늘어날 뿐 아니라 질적으로도 고도화되고 있다. 최근 발생한 SKT 해킹사건과 같이 국가 안보에 중대한 영향을 미치는 기간산업에 대한 공격 등 공공부문을 대상으로 한 지능형 지속 위협(APT)과 공급망 공격이 급증함에 따라, 방어 중심의 기존 보안 전략만으로는 한계가 분명해졌다. 이에 따라 공격자 관점에서 수행되는 선제적 보안 진단의 중요성이 부각되고 있으며, 이를 전문적으로 수행할 진단 인력의 수요가 급증하고 있다. 그러나 현행 국내 정보보호 자격제도는 일반적인 보안 지식과 관리 역량 평가에 치우쳐 있어, 고난도 실전 해킹 역량을 제대로 검증하지 못한다는 한계가 지적된다.

본 연구는 이러한 문제점을 해결하기 위해 진단 전문인력 자격제도의 도입 타당성을 이론적·실천적으로 검토하였다. 주요국의 진단 업무 체계와 자격제도를 심층 비교·분석해 국내 적용 시 고려해야 할 시사점을 도출하고, 국내 교육 현황과 산업계 요구를 반영한 실무 중심 자격제도 설계안을 제시하였다.

이러한 자격제도 도입은 국내 사이버 보안 역량 제고는 물론 진단 전문인력의 위상 및 전문성 강화, 보안 산업 활성화, 그리고 궁극적으로 국민 신뢰 향상에 크게 기여할 것으로 기대된다.

주제어 보안 진단 전문인력, 화이트해커, 모의침투, 취약점 분석, 자격제도

Ⅰ. 서론

1. 연구의 배경 및 필요성

1) 사이버 위협 고도화와 침해 사례 증가

사이버 위협은 디지털 전환의 가속화와 함께 그 양적, 질적 측면에서 빠르게 진화하고 있다. 과거의 단순한 해킹 시도를 넘어, 오늘날의 사이버 공격은 국가 안보와 사회·경제 전반에 심각한 파급 효과를 미칠 수 있는 수준에 이르렀다. 이러한 변화는 기존의 방어 중심 보안 전략만으로는 충분한 대응이 어렵다는 인식을 확산시켰으며, 공격자 관점에서의 선제적 진단 및 예방 전략의 중요성을 부각시키고 있다.

2017년 전 세계를 강타한 워너크라이(WannaCry) 랜섬웨어 공격은 150개국 30만 대 이상의 컴퓨터를 감염시키며 랜섬웨어의 파괴력을 각인시켰다(문정후 2022). 이 공격은 알려진 운영체제 취약점을 활용했음에도 불구하고 막대한 피해를 야기했으며, 최근에는 랜섬웨어가 단순히 금전적 이득을 넘어 데이터 유출, 서비스 중단, 심지어 국가 간 갈등을 초래하는 수단으로 확장되고 있다(Tidy 2021). 특히, 더욱 정교해진 위협인 지능형 지속 위협(APT 공격)은 특정 대상을 목표로 다양한 해킹 기술을 결합하여 은밀하고 지속적으로 공격하는 특징을 보인다. 2025년 4월 전 국민을 혼란으로 빠트린 SKT 해킹 사건 역시 BPF도어 계열 악성코드를 통한 은밀한 공격이 장기간에 걸쳐 발생하였다는 점에서 APT 공격에 대한 위협이 더욱 높아지고 있다(양준규 2025). 공급망 공격 또한 심각한 위협으로 부상했다. 2020년 발생한 솔라윈즈(SolarWinds) 사건은 공급망 공격의 대표적인 사례로, 솔라윈

즈의 소프트웨어 업데이트에 악성코드를 주입하여 미 재무부, 국방부 등 주요 정부 기관과 마이크로소프트, 시스코 등 대형 기업에 광범위한 피해를 입혔다. 이러한 공급망 공격은 특정 조직을 직접 공격하는 대신, 그 조직이 의존하는 공급망을 대상으로 하여 간접적으로 피해를 입히는 방식으로, IT 환경과 인프라의 복잡성이 증가할수록 성공 가능성이 높아지고 방어는 더욱 어려워질 것으로 전망된다(문가용 2022).

무엇보다 이러한 고도화된 사이버 위협이 공공부문에 대한 심각한 피해를 안기고 있다는 점에 주목할 필요가 있다. 2023년에는 북한 정찰총국 소속 해커 조직 '라자루스'에 의해 대한민국 법원 전산망이 해킹당하여 1,014GB에 달하는 법원 자료와 개인정보가 유출된 사실이 드러났다(김영명 2024a). 법원 전산망은 거의 모든 개인정보의 총합이라 할 수 있어, 북한 해킹 조직이 2차 범죄에 활용할 수 있는 신뢰성 있는 공공기관을 노리고 있음을 시사한다. 같은 해 한국고용정보원의 워크넷에서 23만 명의 개인정보가 유출되었고(김영명 2023), 중앙선거관리위원회 직원 PC의 악성코드 감염으로 선거 정보와 내부 기관 정보가 다크웹에 유출되기도 했다(김민진 2024). 국가정보원의 발표에 따르면, 2023년 국내 공공기관을 대상으로 한 사이버 공격은 하루 평균 162만 건으로 전년 대비 약 43만 건 증가한 것으로 나타났다(김영명 2024b).

이러한 사이버 위협의 양적 증가와 질적 고도화는 단순한 데이터 유출을 넘어 사회 시스템 마비, 국가 안보 위협, 경제적 손실 등 예측 불가능한 복합적 파급 효과를 야기한다는 점에서 대응에 총력을 기울일 필요가 있다.

2) 진단 전문인력의 중요성 및 역할 부각

이를 위해 최근에는 사건이 발생한 뒤에 사후 대응을 하는 것이 아닌 사전 예방 중심의 보안 전략으로의 전환이 강력히 요구되고 있으며, 이를 위한 보안위협을 진단할 수 있는 전문인력의 중요성이 부각되고 있다. 과학기술정보통신부와 한국인터넷진흥원(KISA)이 발표한 바에 따르면, 디지털 전환 흐름에 맞춰 사이버 방어체계 고도화 노력에도 불구하고 공격자들의 새로운 취약점을 통한 공격 진화로 예측하기 어려운 침해사고가 발생할 것이라고 내다보았다(과학기술정보통신부 2024). 따라서 기관 및 기업은 단순히 보안 시스템을 도입하는 것을 넘어, 만일의 상황에 대비하여 면밀한 공격 탐지 및 차단, 보안 취약점 점검, 그리고 발전하는 공격 유형에 맞춰 실전형 모의침투를 통한 고도화된 진단이 필요하다.

민간 분야에서는 이미 사이버 위기 대응을 위한 모의침투나 취약점 탐지의 필요성을 적극적으로 주장하고 있다. 특히 보안 취약점 관리 및 대응이 기업의 존폐를 위협하는 상황에 이르렀다는 점에서 많은 기업이 보안 취약점 관리의 중요성을 인식하고 취약점 관리 TF를 구성하거나, 모의 해킹 및 전문 취약점 식별 도구 도입 등 진단 역량 강화에 적극적으로 나서기 시작했다(박일 2024). 이처럼 사회적 요구가 방어에서 선제적 진단으로 전환되고 있으며, 이는 기존의 일반 정보보호 전문가가 아닌 '공격자 관점'의 전문성을 가진 '진단 전문인력'이라는 새로운 직무 영역의 부상을 시사한다. 즉, 단순히 취약점을 '찾는' 것을 넘어, 실제 공격 시나리오를 '재현'하고 '예방'하는 핵심적인 가치를 제공할 수 있는 것이 앞으로의 보안 전문가가 갖추어야 할 자질이라고 할 수 있다.

진단 전문인력의 중요성은 정부의 「사이버안보 업무규정」에서도

찾아볼 수 있다. 「사이버안보 업무규정」 제12조는 중앙행정기관등의 장이 해당 기관에 대한 사이버 공격 및 위협 예방과 대응에 필요한 자체 진단·점검을 연 1회 이상 실시하도록 규정하고 있다. 이는 「정보통신기반 보호법」이나 「전자금융거래법」에 따른 취약점 진단 의무를 모든 중앙행정기관으로 확대하는 조항으로, 공공 분야 사이버 보안 수준을 높이는 것을 목표로 한다. 더욱이 2024년 3월 5일 개정된 「사이버안보 업무규정」 제9조 제5항에 따르면, 국가정보원장은 중앙행정기관등의 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템의 취약 요소를 발굴·개선하기 위해 보안관리 수준을 측정할 수 있도록 규정하고 있는데, 이를 통해 모의침투나 취약점 진단이 가능할 것으로 보인다. 기존에는 협의 하에 보안관리 컨설팅이 가능했으나, 개정으로 사전 통보를 통해 점검할 수 있게 되어 진단 업무가 더욱 증가할 것으로 예상된다. 이러한 규정 변화는 공공분야에서 공격자 관점의 모의해킹 등 적극적인 진단 업무의 수요를 확대를 불러오고 이를 수행할 전문 인력의 필요성을 증대시킬 것으로 보인다.

3) 현행 제도의 한계와 문제점

다만, 고도화되는 사이버 위협에 대응하기 위한 진단 전문인력의 필요성이 증대되고 있음에도 불구하고, 현행 국내 정보보호 자격제도는 여러 한계와 문제점을 안고 있다.

국내의 대표적인 보안 분야 공인 자격증으로는 과학기술정보통신부 주관의 정보보안산업기사와 정보보안기사가 있다. 이 자격증들은 시스템 보안, 네트워크 보안, 애플리케이션 보안, 정보보안 일반, 정보보안관리 및 법규 등 다양한 역량을 평가하지만, 실기시험에서 시스템 해킹, 웹 해킹 등 기초적인 이론을 일부 다룰 뿐, 실제 해킹을 통해

취약점을 찾는 실질적인 공격자 관점의 역량 평가는 미흡하다.

이에 따라 현재 정보보호 기업 등에서 모의침투 전문 인력을 채용하거나 평가할 때는 정보보안기사 자격증 취득 여부가 아닌 주로 해킹 대회 입상 실적, 민간 및 공공의 버그바운티(Bug Bounty) 이력, 동종업계 경력 이력 등 포트폴리오에 의존하고 있다. 그러나 해킹 대회나 버그바운티의 경우 팀을 이루어 진행되는 경우가 많아 개인의 실질적인 기여도를 판단하기 어렵고, 객관적인 평가 기준이 부족하여 평가자의 역량에 따라 결과가 상이할 수 있다는 문제가 있다.

관련 법·제도의 공백 또한 문제점으로 지적된다. 사이버안보 업무규정 제12조에 따른 중앙행정기관의 자체 진단·점검 의무는 모의침투와 같은 높은 수준의 취약점 진단을 의무사항으로 포함하지 않아, 대부분의 기관에서 단순한 체크리스트 기반의 보안 진단에 머무를 수 있다. 국가정보원의 보안관리 수준 측정(제9조 제5항)에 모의침투가 포함될 수 있겠지만, 이를 수행할 전문 인력에 대한 객관적인 평가 기준은 여전히 부재한 실정이다. 이러한 규제적 모호성은 피상적인 컴플라이언스 준수를 유도할 수 있으며, 실제 보안 강화에 어려움을 초래할 수 있다.

결론적으로, 기존 제도의 한계는 단순히 자격증 종류의 부족을 넘어, '공격자 관점의 실질적 진단'이라는 핵심 역량에 대한 사회적 정의와 평가 메커니즘의 부재에서 기인한다. 이는 공공기관의 위탁 업무 수행 시 객관적 인력 평가의 어려움으로 이어져, 결국 국가 사이버 보안 수준 향상에 걸림돌이 될 수 있다. 현재의 법적 및 제도적 환경은 사이버 위협의 심각성을 인지하고 있으나, 이를 실질적으로 대응할 수 있는 전문 인력의 양성과 검증 체계를 충분히 뒷받침하지 못하고 있는 것이다.

2. 연구 목적 및 방법

따라서 본 연구는 고도화되는 사이버 위협에 효과적으로 대응하기 위한 진단 전문인력 자격제도 도입 방안을 연구하고자 한다.

먼저 진단 전문인력이 구체적으로 어떤 자질과 역량을 갖추어야 하는지 기준을 정립한다. 또한, 이러한 인력을 양성하고 평가하기 위한 국내 제도의 한계점을 분석하고, 미국, 영국, 독일 등 주요국의 진단 업무 수행체계, 자격제도, 교육 동향을 심층 분석하여 국내 도입 시 고려해야 할 핵심 시사점을 파악하고자 한다. 이어서 실효적인 제도 설계 및 운영 방안을 제시하기 위해 국가공인 대 민간공인 모델, 자격 등급화 및 세부 분류, 응시 자격, 시험 구성, 교육과정 연계, 자격 갱신 및 지속 교육 체계, 운영 주체 및 관리체계 등 진단 전문인력 자격제도를 운영하기 위한 구체적인 설계 방안을 제안한다. 마지막으로, 해당 제도의 도입을 통한 기대 효과를 분석하고, 제도 도입과 연계되어 수행되어야 할 정책 과제를 도출하고자 한다.

본 연구는 기본적으로 주요국의 사례나 제도를 비교 분석하는 문헌연구와 정책 비교분석을 중점적으로 연구를 수행하지만 국내 현실에 보다 적합한 자격제도를 설계하기 위하여 국내 업계 전문가들을 대상으로 인터뷰를 진행하여 현실적으로 운영 가능한 진단 인력 자격제도 도입 방안을 제안하고자 한다.

Ⅱ. 진단 전문인력의 개념 및 직무 분석

1. 진단 전문인력의 정의

진단 전문인력은 그 범위와 역할에 따라 광의적 정의와 협의적 정의로 구분될 수 있다. 광의적으로는 정보보호 전반의 취약점을 식별하고 개선하는 모든 전문가를 포괄한다. 이는 시스템 감사, 보안 컨설팅, 취약점 스캐닝 등 다양한 정보보호 활동을 수행하는 인력을 포함하는 개념으로 볼 수 있다. 한편 진단 전문인력은 협의적인 의미에서 '공격자 관점'으로 시스템, 네트워크, 애플리케이션 등의 취약점을 모의 해킹 기법을 활용하여 능동적으로 탐지하고, 이에 대한 실질적인 개선 방안을 제시하는 데 특화된 전문가를 의미한다. 이들은 단순히 알려진 취약점을 점검하는 것을 넘어, 실제 해커가 사용하는 기술과 전략을 모방하여 시스템의 숨겨진 약점을 찾아내고, 이를 통해 발생 가능한 위협 시나리오를 구체화하는 역할을 수행한다.

따라서 본 연구에서는 제도 설계를 위한 실질적인 정의로서 진단 전문인력을 '사이버 공격자의 시각에서 정보시스템 및 네트워크의 잠재적 취약점을 선제적으로 발굴하고, 모의 침투(Penetration Testing) 및 취약점 분석(Vulnerability Analysis)을 통해 실제 공격 가능성을 검증하며, 이에 대한 효과적인 예방 및 대응 방안을 제시하는 고도의 전문성을 갖춘 인력'으로 정의하고자 한다. 이 정의는 이른바 '화이트해커' 내지는 '윤리적 해커'의 역할을 강조하며, 이들이 단순한 방어자가 아닌 능동적인 위협 분석가이자 해결사로서 기능함을 명확히 한다.

2. 진단 전문인력의 직무와 활동

진단 전문인력은 사이버 보안 환경에서 다양한 직무와 활동을 수행한다. 특히 취약점 분석은 진단 전문인력의 핵심 직무 중 하나로 볼 수 있는데, 이들은 일반적인 정보보호 전문 인력과 다르게 시스템, 네트워크, 애플리케이션 등 정보 자산 전반에 걸쳐 알려진(known) 취약점뿐만 아니라, 알려지지 않은(unknown) 잠재적 보안 취약점을 식별하고 평가하는 활동을 수행하게 된다. 이를 위해 자동화된 취약점 스캐닝 도구와 함께 수동 분석 기법을 병행하여 시스템의 숨겨진 약점을 파악하는데, 이 과정은 단순히 기술적인 결함을 찾는 것을 넘어, 해당 결함이 실제 위협으로 이어질 수 있는 가능성을 평가하는 데 중점을 둔다.

여기에 더해 모의해킹(Penetration Testing)은 진단 전문인력의 가장 특징적인 활동으로 볼 수 있다. 이는 합법적인 범위 내에서 실제 사이버 공격과 동일한 기법과 절차를 사용하여 대상 시스템에 침투를 시도하고, 식별된 취약점이 실제 공격으로 이어질 수 있는지 검증하는 실전적 활동이다. 모의해킹은 단순한 취약점 스캔을 넘어선 검증 과정을 포함한다. 침투 테스트 표준인 PTES에 따르면(PTES 2014), 다음과 같은 주요 단계로 업무가 진행된다.

〈그림 1〉 모의침투 진단 업무 프로세스

정보 수집(Intelligence Gathering)단계에서는 공격 대상에 대한 공개

된 정보를 최대한 수집하여 공격 계획 수립에 필요한 기반을 마련한다. 이후 위협 모델링(Threat Modeling) 과정에서 수집된 정보를 바탕으로 조직의 내·외부적인 위협을 모델링하고, 취약점 분석을 통해 공격에 활용될 수 있는 취약점을 구체화하게 된다. 다음으로 식별된 취약점을 이용하여 시스템에 침투를 시도하고, 보안 제한을 우회하여 시스템 또는 리소스에 대한 접근 권한을 확보하는 과정을 거치게 된다. 이 과정에서 회피 기술(IDS/IPS 우회, 웹 애플리케이션 방화벽 우회 등)이 사용될 수 있으며, 대상에 특화된 맞춤형 시나리오와 익스플로잇 개발이 이루어지기도 한다. 무엇보다 시스템 침투에 성공한 후, 추가적인 정보를 수집하고 다른 시스템을 공격하기 위한 기반을 마련하는 후속 공격 활동인 포스트 익스플로잇(Post-Exploitation) 작업을 수행하는데, 이때 지속적인 시스템 접근 유지를 위해 백도어를 심거나 패스워드를 크래킹하는 등의 작업이 포함될 수 있다.

진단 전문인력은 이러한 일련의 해킹 과정에 대해 테스트 결과를 정리하고 보안 컨설팅 및 개선안을 제시하여 진단 결과의 실질적인 가치를 창출할 수 있어야 한다. 즉, 진단 전문인력은 모의해킹 및 취약점 분석을 통해 발견된 취약점의 심각도를 평가하고, 이에 대한 구체적이고 실현 가능한 기술적, 관리적, 물리적 개선 방안을 제시해야 한다. 또한, 조직의 전반적인 보안 정책 및 프로세스 개선을 위한 전략적 자문을 제공하여, 장기적인 보안 강화 로드맵을 수립하는 데 기여한다.

3. 진단 전문인력의 자질과 역량

앞서 살펴본 것처럼 진단 전문인력은 고도화되는 사이버 위협에 효과적으로 대응하기 위해 다양한 기술적, 비기술적 역량을 종합적으로 갖추어야 한다. 이들의 역량은 단순히 해킹 기술에만 국한되지 않고, 법적, 윤리적, 그리고 커뮤니케이션 능력까지 포괄한다.

1) 기술 실무 역량

진단 전문인력에게 요구되는 가장 기본적인 역량은 바로 공격자 관점에서의 진단 수행 능력이다. 소프트웨어에서 발생하는 오류나 에러는 무작위로 발생할 수 있지만, 해킹은 공격자가 "의도성"을 가지고 시스템의 가장 취약한 부분에 집중하여 발생시킨다는 점에서 큰 차이가 있다. 따라서 진단 전문인력은 이러한 공격을 사전에 예방하기 위해 침투 테스트와 취약점 진단을 수행할 때 이러한 공격자의 의도성에 대한 이해를 바탕으로 시스템에 발생 가능한 위협과 취약점을 식별하고, 이를 바탕으로 공격 시나리오를 도출하여 실제로 익스플로잇하는 과정을 수행할 수 있는 기술 역량이 요구된다.

특히 침투 테스트는 일반적인 체크리스트 기반의 보안 점검과 달리 명확한 점검 기준이 제시되지 않으므로, 주어진 시스템에 발생할 수 있는 위협과 취약점을 모두 도출해낼 수 있는 기술 능력이 중요하다는 점에서 실제로 많은 오펜시브 시큐리티 전문 업체에서는 진단 전문인력을 채용할 때 CTF 대회 입상, 버그바운티 제보 이력 등을 통해 지원자가 실제로 공격자 관점에서 시스템에 침투해 본 경험이 있는지를 확인하고 있다.

이외에도 Metasploit, Kali Linux, Nessus, Nmap 등 침투 테스트

및 취약점 진단에 사용되는 다양한 도구에 대한 숙련된 사용 능력이 요구되며, 기본적인 웹 해킹, 시스템 해킹, 네트워크 해킹, 암호학, 디지털 포렌식, 리버스 엔지니어링 등 다양한 보안 분야의 깊이 있는 이해가 필수적이다. 이는 대상 시스템의 보호 메커니즘을 이해하고, 이를 우회하거나 무력화하는 방법을 찾아내는 데 기반이 되기 때문이다. 추가로 컴퓨터 구조, 자료 구조, 네트워크 구조, 운영체제(Windows, Linux), 프로그래밍 언어(Python 등)에 대한 깊은 이해가 필수적이다. 클라우드 컴퓨팅과 같은 새로운 기술 및 인프라 환경에 대한 즉각적인 반응 능력 또한 요구된다. 프로그래밍 지식은 자동화된 공격 스크립트나 맞춤형 익스플로잇 작성에 활용될 수 있으며, 네트워크 지식은 중간자 공격(MITM) 시뮬레이션 등에 사용될 수 있다.

2) 윤리 역량과 법제도 이해

다음으로 법제·정책 이해도는 진단 업무 수행의 합법성과 윤리성을 보장하는 중요한 역량으로 작용한다. 진단 전문인력은 정보통신망법, 개인정보 보호법, 사이버안보 업무규정 등 국내외 유관 법령 및 규제를 정확히 이해하고 준수해야 한다. 침투 테스트 과정에서 허가받지 않은 시스템에 접근하거나, 승인 범위를 넘어 데이터를 조작하는 행위는 법적 문제로 이어질 수 있으므로, 법적 허용 범위 내에서 업무를 수행하는 능력이 필수적이다.

이와 더불어 윤리적 책임의식은 진단 전문인력에게 가장 강조되어야 할 자질이다. 이들이 보유한 고도의 기술 역량은 악용될 경우 심각한 범죄로 이어질 수 있기 때문이다. 실제 2021년 전국 아파트 월패드 해킹 사건의 범인이 보안 전문가로 밝혀진 사례는 기술적 능력만으로는 사회적 신뢰를 얻을 수 없으며, 오히려 심각한 사회적 피해를

야기할 수 있음을 보여준다(김영명 2022). 따라서 진단 전문인력은 자신의 기술을 오직 합법적이고 윤리적인 목적, 예컨대 보안 강화를 위해 활용하려는 확고한 직업 윤리 의식을 갖추어야 하며, 기밀 유지, 독립성, 중립성, 공정성을 유지하는 것이 필수적이다. 이러한 역량은 기술적 우수성만큼이나 중요하며, 자격제도는 기술 평가와 함께 윤리 교육 및 평가를 의무화하여 '신뢰할 수 있는 전문가'를 양성하는 데 주력해야 한다.

3) 커뮤니케이션 역량

기술 역량과 윤리 역량 이외에도 커뮤니케이션 및 보고 능력은 진단 결과를 효과적으로 전달하고 보안 강화를 위한 실행을 이끌어내기 위해 매우 중요한 요소이다. 진단 전문인력은 기술적 내용을 경영진이나 일반 사용자 등 비기술적 이해관계자에게 명확하고 효과적으로 설명할 수 있어야 하며(Ullah 2025), 진단 결과를 체계적인 보고서로 작성하여 전달하고, 이를 바탕으로 개선 방안을 설득력 있게 제시하는 능력을 갖추어야 한다(Hammond 2024).

Ⅲ. 국내외 진단 전문인력 제도 및 정책 현황

1. 국내 현황 분석

취약점 진단 업무 수행에 대한 적정성을 보장하기 위한 제도로 국내에서는 정보보호 전문서비스 기업 지정 제도를 운영하고 있으며, 이는 「정보보호산업의 진흥에 관한 법률」 및 「정보통신기반보호법」에 근거한다. 이 제도는 주요 정보통신기반시설에 대한 취약점 분석 및 평가, 보호대책 수립 업무 지원을 위해 전문 능력과 신뢰성을 갖춘 민간 기업을 지정하여 양질의 정보보호 컨설팅 서비스를 제공하는 것을 목표로 하는 제도이다(과학기술정보통신부 2024). 다만 해당 제도만으로는 다음과 같은 한계가 존재한다.

1) 기존 자격제도의 구조 및 한계

정보보호 전문서비스 기업이 수행하는 컨설팅 업무는 주로 시스템, 네트워크, 애플리케이션 등 일반적인 보안 취약점 점검과 조직의 보안 정책 수립, 보안 절차 및 프로세스 평가, 규제 준수 점검에 중점을 둔다. 이들은 자동화된 도구와 체계적인 점검 방법론, 체크리스트를 활용하여 보안 점검을 수행하는 경우가 많은데, 이러한 방식은 법령 등에서 정한 보호 조치를 적절히 구축하고 있는지 확인하는 데 유용하지만, 실제 공격에 얼마나 취약한지 등 실질적인 위협을 파악하는 데는 한계가 있다.

또한, 정보보호 전문서비스 기업 지정 등에 관한 고시의 [별표1]에 따르면 정보보호 전문서비스 기업 지정 시 기술 인력의 역량 평가는

학력, 자격증, 경력, 실적 등으로 이루어지며, 모의침투나 해킹 등 실질적인 공격자 관점의 역량 평가는 별도로 이루어지지 않는다. 이는 국내 정보보호 전문서비스 기업의 진단 업무가 주로 '컴플라이언스 준수'와 '일반적 취약점 점검'에 초점을 맞추고 있음을 의미하며, '실제 공격 시뮬레이션'을 통한 심층적 위협 파악과는 거리가 있음을 의미한다.

이처럼 현재의 지정 제도는 기업의 '기술 인력 보유 현황'을 평가하지만, 그 인력의 '실질적인 모의침투 역량'을 검증하는 메커니즘이 부재하여, 고도화되는 사이버 위협에 대한 실효적 대응에 한계를 보이고 있다고 할 수 있다. 이러한 상황은 보안 전문가의 역량 평가가 평가자의 주관적인 판단에 의존하게 만들며, 객관적인 기준의 부족으로 인해 인력 채용 및 활용에 어려움을 야기한다.

2) 산업계 수요 및 인력 수급 문제

앞서 언급한 바와 같이 국내 산업계는 '컴플라이언스'를 넘어선 '실질적 위협 검증'의 필요성을 인지하고 있으며, 이를 위해 고도화된 모의침투 솔루션 및 맞춤형 서비스를 도입하기 위한 움직임이 있다. 일반적인 보안 컨설팅의 취약점 진단이 형식적인 틀에서 벗어나 실제 위협 여부를 테스트하는 모의침투를 보완적인 업무로 인식하는 경향이 나타나고 있는 것이다. 현재 국내에는 모의침투를 전문으로 하는 기업이 많지는 않지만, 일부 정보보호 전문서비스 기업이 보안 취약점 진단 및 모의해킹 솔루션(Cobalt Strike, CORE IMPACT, Rapid7 Metasploit 등)을 제공하거나, PTES(Penetration Testing Execution Standard)를 참고하여 정보수집-취약점분석-침투-포스트 익스플로잇-보고 단계의 맞춤형 모의침투 서비스를 제공하고 있다(조재학 2025).

이러한 동향은 진단 전문인력에 대한 시장의 잠재적 수요가 크다는 것을 보여주지만, 이러한 고수준의 진단 업무를 수행할 수 있는 인력의 '정량적/객관적' 검증 기준이 부재로 실질적인 산업계의 수요에 대응할 수 있는 인력 수급 및 활용이 어려울 수 있다는 문제가 있다. 전문적인 모의침투는 고도의 기술과 많은 시간, 비용을 필요로 하며, 이를 수행할 수 있는 인력은 일반적인 정보보호 전문가와는 다른 역량을 요구한다는 점에서 별도의 자격 검증 제도가 필요하다.

3) 관련 법령 및 정책 분석

정부의 사이버보안 관련 법규는 취약점 진단 및 점검의 중요성을 인지하고 그 범위를 확대하고 있으나, '모의침투'와 같은 공격자 관점의 심층 진단을 명시적으로 의무화하거나, 이를 수행할 전문인력에 대한 구체적인 자격 기준을 제시하고 있지 않다. 사이버안보 업무규정 제12조는 중앙행정기관의 자체 사이버보안 진단·점검을 연 1회 이상 실시하도록 의무화하고 있으나, 이는 모의침투와 같은 높은 수준의 취약점 진단을 필수로 포함하지 않아 단순 체크리스트 기반 진단에 머무를 수 있다. 또한, 국가정보원의 보안관리 수준 측정(제9조 제5항)에 모의침투가 포함될 수 있게 되었지만, 이를 수행할 전문 인력의 객관적 평가 기준은 여전히 부재하다는 점은 변함이 없다.

이러한 규제적 모호성은 정책적 의지는 있으나, 이를 뒷받침할 구체적인 '실행력'과 '전문성 검증' 체계가 미흡함을 보여준다. 법적 프레임워크가 진단 업무의 필요성을 강조함에도 불구하고, 실제 현장에서 요구되는 고도의 공격자 관점 진단을 촉진하고 그 수행 인력의 전문성을 보장하는 명확한 기준이 부재한 것이다. 이는 결국 피상적인 컴플라이언스 준수를 유도하고, 실질적인 사이버 보안 강화에는

한계로 작용하여 국가 사이버 보안 회복력을 저해하는 요인으로 작용한다.

2. 해외 주요국 사례

사이버 보안 진단 전문인력의 중요성이 전 세계적으로 부각됨에 따라, 주요국들은 다양한 방식으로 관련 제도와 정책을 운영하고 있다. 각국의 접근 방식은 자격제도 설계에 중요한 시사점을 제공한다.

1) 미국: CISA RVA 및 주요 민간 자격

미국은 연방 정부의 보안을 보장하기 위해 「연방 정보 보안 현대화법(FISMA, Federal Information Security Modernization Act of 2014)」을 통해 연방 기관의 정보 보안 프로그램 및 관행에 대한 '연간 독립 평가(Annual Independent Evaluation)'를 의무화하고 있다. 이 평가에서는 침투 테스트가 명시적으로 의무화되어 있지는 않지만, '2024 IG FISMA 지표 평가 가이드'에 따르면, 침투 테스트 및 취약점 스캐닝 결과를 연간 독립 평가에 반영할 것을 권장하고 있다(CISA 2024a).

진단 업무 수행체계는 각 기관의 내부 감사관(IG) 또는 독립된 외부 감사인에 의해 FISMA 연간 독립 평가가 수행되며, 그 결과는 예산관리국(OMB)과 의회에 보고된다. 특히 국토안보부(DHS) 산하의 사이버 보안 및 인프라 보안국(CISA)은 연방 기관과 중요 인프라 시설에 '위험 및 취약점 평가(RVA, Risk and Vulnerability Assessments) 프로그램'을 무료로 제공하고 있다. 이 프로그램은 MITRE ATT&CK 프레임워크에 따라 취약점 스캐닝, 네트워크 스니핑, 침투 테스트, 시스템 및 네트워크 장비의 보안 구성 검토, 피싱 평가 등의 활동을 통한 실질적인

보안 평가의 과정이 포함된다. 특히, 침투 테스트의 경우 최신 기법 및 절차를 사용하여 대상 환경에 침투하고, 실제 발생 가능한 공격에 대한 취약점을 파악하는 진단 방식이 적용되고 있다(CISA 2022).

진단 인력에 대한 자격 제도로 CISA에서 '진단 평가 및 기준(AES, Assessment Evaluation and Standardization) 프로그램'을 운영하여 CISA RVA 팀 소속 진단 전문인력을 양성하고 선발한다(CISA 2024b). AES 프로그램은 기본 지식, 경험, 그리고 CISSP, OSCP와 같은 유관 자격증 취득을 권고하여 침투 테스트에 대한 전문성이 요구된다. 특히 RVA 운영자 자격 취득 과정은 침투 테스트 기본 지식, Kali Linux, Metasploit, Nessus, Nmap 등 도구 지식, 그리고 최소 3년 이상의 공인 침투 테스트 수행 경력을 필수적으로 요구하고 있다. 이 과정에는 24시간 동안 진행되는 실습 및 퀴즈 형태의 기술 테스트가 포함되어 실무 역량을 엄격하게 검증한다(CISA 2023).

이처럼 미국은 정부 주도의 진단 프로그램(CISA RVA)을 운영하면서 그 수행 인력에 대해서는 엄격한 실무 중심의 기술 및 경력 요건(AES 프로그램)을 요구한다. 이는 '정책적 필요성'과 '실질적 역량 확보'를 동시에 추구하는 모델로, 자격증 자체를 법제화하기보다는 정부 프로그램의 '운영 기준'으로 전문성을 확보하는 유연한 접근 방식을 보여준다. 이러한 접근 방식은 정부가 자체적인 테스트 및 인증 인프라를 구축하지 않고도 고품질의 침투 테스트를 보장하며, 변화하는 위협에 대한 대응력을 높일 수 있도록 한다는 특징이 있다.

2) 영국: CHECK 프로그램 및 관련 자격

영국은 중요한 네트워크와 정보 시스템의 보안 강화를 위해 EU의 NIS Directive를 기반으로 도입된 「The Network and Information

Systems Regulations 2018 (NIS 2018)」을 통해 필수 서비스 운영자(OES)에게 적절한 기술 및 조직적 보안 조치를 의무화하고 있다(GOV.UK 2023). 또한, 정부 부서의 자산 및 데이터 보호를 위한 「Government functional standard GovS 007: Security」는 정기적인 위험 및 취약성 평가 수행 정책 및 프로세스 마련을 명시하고 있다(UK Government Security 2024).

진단 업무 수행체계는 국가 사이버 보안 센터(NCSC, National Cyber Security Centre)가 운영하는 CHECK 제도를 통해 공공부문 및 국가 중요 인프라(CNI)에 대한 침투 테스트를 수행할 사이버 보안 서비스 제공업체를 승인하고 있다. 승인된 업체는 NCSC가 지정한 프레임워크를 사용하여 침투 테스트를 수행하고 그 결과를 보고해야 한다. 침투 테스트는 화이트박스와 블랙박스 테스트로 구성되며, 취약성 식별, 시나리오 기반 테스트, 탐지 및 대응 역량 점검 등 세 가지 유형으로 분류된다(NCSC 2022). 특히 'OFFICIAL' 등급 데이터를 처리하는 시스템은 CHECK에 따른 침투 테스트가 필수적으로 적용되어야 한다.

진단인력 전문 자격 제도는 CHECK 프로그램에 따라 침투 테스트 작업을 수행하는 팀 내 최소 1명 이상이 팀 리더 자격을 갖추도록 요구한다(NCSC 2024). 팀 리더는 NCSC에서 지정한 민간 보안 인증 시험 업체인 CREST와 The Cyber Scheme에서 대행하는 인증 자격 시험을 통과해야 한다. CREST 팀 리더 시험은 기본적인 필기 시험과 실습 평가 2가지 과제(시나리오 기반 실습, 침투 테스트 실습)로 구성되며, 팀원 시험은 객관식 및 가상머신 내 실기 평가로 이루어진다(CREST 2022). The Cyber Scheme 팀 리더(CSTL) 시험은 실제 침투 테스트를 시뮬레이션하는 3단계의 실습 시험(범위 지정, 실제 침투 테스트, 인터뷰)

으로 구성되며, 팀원(CSTM) 시험은 4단계 시험 절차(객관식, 주관식, 네트워크 공격 실습, 시험 브리핑)로 구성된다(The Cyber Scheme 2022).

이처럼 영국은 정부(NCSC)가 '민간 업체'를 '공인'하여 공공부문 진단 업무에 대한 자격을 평가하는 '민간 주도형 국가 공인 모델'을 채택하고 있다. CREST와 The Cyber Scheme과 같은 민간 기관이 실제 시험을 대행하며, 이 시험들은 매우 실기 중심적이고 난이도가 높다는 특징을 가진다. 이는 정부의 규제적 요구(CHECK)와 민간의 전문성(실기 평가)을 결합하여 고품질 진단을 보장하는 효과적인 접근 방식을 보여준다. 이러한 모델은 정부가 광범위한 침투 테스트 및 인증 인프라를 구축할 필요 없이, 시장의 경쟁과 민간의 전문성을 활용하여 사이버 보안 역량을 강화할 수 있도록 한다는 특징이 있다.

3) 독일: BSI 진단 업무 및 인증 제도

독일은 「연방정보기술보안청법(BSIG)」을 통해 연방정보기술보안청(BSI)의 사이버보안 진단 업무를 법제화하고 있다. BSI는 연방기관에 정보보안 컨설팅 및 지원 서비스를 제공할 의무가 있으며, 연방시설, 핵심기반시설(KRITIS), 디지털서비스 등의 정보 시스템이 취약하다고 판단될 경우 포트 스캔 등 진단을 수행할 수 있다.

진단 업무 수행체계는 BSI 내부 담당자가 수행하거나 민간 업체가 대행할 수 있으며, BSI는 민간 업체 이용 시 'IT 보안 서비스 제공 업체 인증 제도'를 통해 인증된 업체를 권장한다. BSI의 보안 진단 업무는 IS 침투 테스트 및 웹 검사, IS 감사, IT 포렌식 등으로 분류되며, 침투 테스트 및 웹 진단은 주로 연방 기관을 대상으로 3년에 한 번 이상 받을 것을 권고하고 있다(BSI 2022).

진단인력 전문 자격 제도는 독일 법률상 법제화되어 있지는 않으

나 BSI는 IT 보안 서비스 제공업체의 역량을 인증하는 'IT 보안 서비스 제공 업체 인증 제도'와 IT 보안 서비스 제공업체 직원의 전문적 역량을 입증하는 '개인 평가 및 역량 인증 제도'를 운영한다. '실용 가이드: IT 보안 침투 테스트 가이드라인'에서는 진단 인력 및 업체 선정 시 참고할 요구사항을 제시하는데(BSI 2016), 기술적 요구사항(시스템 관리, 네트워크 프로토콜, 프로그래밍 언어, IT 보안 제품, 애플리케이션, 네트워크 구성 요소 지식), 자격 및 경력사항(BSI 개인 평가, CEH 등 국제 자격증, 수석 진단자/관리자/인력별 경력 요건), 기타(신뢰성, 독립성, 중립성, 2인 이상 팀 구성) 등이 포함된다. IS 침투 테스터 프로그램의 역량 평가 항목에는 기술적 역량 외에 의사소통, 팀워크, 독립성, 윤리 의식 등 비기술적 역량도 포함된다.

이처럼 독일은 BSI가 직접 진단 서비스를 제공하거나 민간을 활용하는 방식을 취하면서 국가가 민간 업체 및 개인의 역량을 평가하는 '인증 제도'를 운영하여 신뢰성을 확보하고 있다. 다만 이때 정부가 직접 자격증을 발행하기보다, 민간의 전문성을 인정하되 정부가 설정한 '기준'에 따라 '인증'하는 방식으로 품질을 관리하는 접근법을 보여준다. 이 모델은 정부의 감독 하에 민간 시장의 전문성을 활용하여 사이버 보안 서비스의 품질을 높이는 데 기여할 수 있다는 특징을 지닌다.

3. 해외 사례 비교 및 시사점

해외 주요국들의 진단 전문인력 제도 및 정책 현황을 비교 분석한 결과, 각국은 사이버 위협에 대응하기 위해 다양한 접근 방식을 취하고 있음을 확인할 수 있다. 이러한 비교를 통해 국내 진단 전문인력

자격제도 설계에 중요한 시사점을 도출할 수 있다.

1) 국가 주도 vs 민간 주도 모델 비교

해외 사례는 '국가 주도'와 '민간 주도'의 스펙트럼 내에서 다양한 모델을 보여주지만, 공통적으로 '정부의 관여(규제, 인증, 권장)'와 '민간의 전문성 활용'의 균형점을 찾고 있다.

국가 주도 모델인 미국 CISA와 독일 BSI는 정부 기관이 직접 진단 서비스를 제공하거나, 민간의 참여를 유도하되 정부가 설정한 엄격한 기준과 인증을 통해 품질을 관리한다. 이들은 인력 양성 프로그램을 직접 운영하기도 한다. 한편 민간 주도 모델로 영국 CHECK 프로그램은 정부가 민간 기관을 공인하여 진단 업무를 위탁하고, 민간 기관이 자체적으로 또는 협력하여 자격 인증 시험을 운영하는 방식이다. 이 모델은 시장의 유연성과 민간의 전문성을 적극적으로 활용한다.

이러한 모델 비교를 통해, 사이버 보안 분야의 특성상 정부가 모든 것을 직접 수행하기보다는 민간의 깊이 있는 기술 전문성과 시장의 유연성을 활용하는 것이 효과적이라는 점을 알 수 있다.

2) 실기 중심 평가 및 역량 기반 모델의 중요성

사이버 위협의 본질이 '실전적 공격'이라는 점을 고려할 때, 진단 전문인력의 역량 평가는 단순한 이론 지식 확인을 넘어 '실제 공격을 모의하고 방어 체계를 우회하며 문제를 해결하는 능력'을 검증해야 한다. 이는 자격제도의 '신뢰성'과 '현장 적용 가능성'을 결정하는 핵심 요소이며, 국내 정보보안기사 자격의 한계를 극복하는 방안이 될 수 있다.

해외 주요 자격들은 모두 실무 역량 평가에 중점을 둔다. 미국 CISA AES 프로그램은 24시간 실습 기술 테스트를 포함하고, 영국 CREST 및 Cyber Scheme은 시나리오 기반 실습 시험을 통해 실무 역량을 평가한다. 특히 미국이나 독일에서 취득을 권장하고 있는 대표적인 글로벌 민간 자격제도인 OSCP의 경우에도 48시간의 실기 시험과 보고서 작성을 통해 실제 침투 능력을 검증하고 있는데, 이러한 실기 중심 평가는 단순히 이론적 지식을 아는 것을 넘어, 실제 위협 상황에서 문제를 해결할 수 있는 능력을 가진 전문가를 선별하는 데 필수적이다(Mancao 2022). 국내 정보보안기사 자격이 실기 시험에서 시스템 해킹 등 기초 이론을 일부 평가하고 있지만 실제 해킹을 통한 취약점을 탐색하는 역량에 대해서는 평가하고 있지 않다는 점을 고려할 때, 국내 진단 전문인력 자격제도는 실기 평가의 비중을 대폭 확대하고 실전적 시나리오 기반의 평가를 도입할 필요가 있다.

3) 지속적 교육 및 갱신 체계의 필요

사이버 위협 환경은 매우 빠르게 변화하므로, 자격 취득 후 지속적인 역량 개발 없이는 전문성이 빠르게 퇴색될 수 있다. '평생 유효'한 자격은 시대에 뒤떨어질 위험이 크며, 자격의 '사회적 신뢰성'을 유지하기 위해서는 정기적인 재교육 및 갱신 의무를 통해 최신 기술 및 트렌드에 대한 숙련도를 지속적으로 검증해야 한다.

이와 관련해서 CEH, CompTIA PenTest+, OSCP 등 대부분의 국제 해킹 및 정보보안 자격증은 2~3년마다 갱신이 필요하며, 교육 수강, 학점 취득, 재시험 응시 등을 요구한다. 이러한 사례들을 참고하여 국내 진단 전문인력 자격제도 역시 3년 정도의 유효 기간을 설정하고, 해당 기간 내에 관련 교육 이수나 재시험을 통해 자격을 갱신하

도록 의무화하는 방안을 고려해야 할 수 있을 것이다. 이는 자격 취득자의 역량을 최신 상태로 유지하고, 자격제도의 공신력을 장기적으로 확보하는 데 기여할 수 있다.

Ⅳ. 진단 전문인력 자격제도 설계 방안

1. 제도 설계의 기본 방향

진단 전문인력 자격제도를 설계함에 있어 가장 근본적인 질문은 해당 자격이 국가공인 자격으로 운영될 것인가, 아니면 민간공인 자격으로 운영될 것인가이다. 각 모델은 명확한 장단점을 가지고 있으며, 국내 사이버 보안 환경과 기존 자격제도의 특성을 고려하여 최적의 방향을 설정해야 한다.

1) 국가공인 vs 민간공인 모델

국가전문자격으로 운영하는 경우 법령에 직접 근거하여 신설되며, 특정 업무에 대한 배타적 지위(면허와 유사)를 부여할 수 있다는 장점이 있다. 이를 위해 사이버보안 기본법 제정 또는 정보통신기반보호법 개정을 통해 진단 전문인력의 역할을 법률에 명시하고 자격을 부여하는 방안을 고려할 수 있다. 그러나 법 개정에는 상당한 시간과 노력이 소요되며, 급변하는 사이버 위협 환경에 대한 유연한 대응이 어렵다는 단점이 존재한다.

한편 국가기술자격으로 운영하는 경우에는 「국가기술자격법」에

근거하여 주어지는 자격으로, 진단 전문인력의 업무가 전문적인 해킹 기술을 활용한 진단 서비스 제공이라는 점에서 기술자격으로 포섭할 수 있을 것이다. 특히 해당 기술이 국민의 생명·안전, 공익에 직결되는 분야라는 점에서 자격기본법 제8조의2에 따른 국가기술자격 신설 기준에도 부합한다. 그러나 국가기술자격 신설에도 상당한 시간이 소요되며, 현행 국가기술자격 제도가 지식 확인 위주의 평가 방식이다 보니 실제 직무 수행 중심의 평가가 미흡하다는 지적이 있다(관계부처합동 2024, 2). 이는 실무 역량이 핵심인 진단 전문인력에게는 적합하지 않을 수 있다는 우려를 낳는다.

이런 점에서 민간자격(공인민간자격)으로 운영하는 방안도 고려해볼 필요가 있다. 사회 변화와 산업계 수요에 유연하게 대응할 수 있으며, 민간 전문가의 참여가 용이하다는 장점이 있다. 특히 5차 국가기술자격 기본계획에서도 민간 주도의 자격제도로의 전환을 강조하고 있어, 민간 자격의 역할이 더욱 중요해질 것으로 예상된다. 다만, 민간자격은 공신력 확보를 위해 '국가 공인' 여부가 매우 중요하다. 공인민간자격으로 지정될 경우, 특정 업무에 대한 배타성을 부여하거나 정부 지원을 받을 수 있어 실효성을 확보할 수 있다.

각 모델의 장단점을 고려할 때, 특히 '신속성'과 '현장성'을 확보하는 것이 중요한 진단 전문인력 자격제도의 경우, 초기에는 '공인민간자격'으로 시작하여 시장 수요와 제도 정착 상황에 따라 '국가기술자격'으로 전환하는 방안이 가장 현실적이고 유연한 접근이 될 수 있다. 이는 정보보안기사 자격이 2001년 한국인터넷진흥원이 주관하여 신설한 민간 자격인 정보보호전문가(SIS)로 시작하여 2013년 국가기술자격으로 전환된 선례 참고할 수 있을 것이다. 이러한 단계별 접근은 급변하는 사이버 보안 환경에 신속하게 대응하면서도 장기적인 공신

력을 확보할 수 있는 균형 잡힌 전략이 될 수 있다.

2) 자격 등급화 및 세부 분야별 분류

앞서 살펴본 바와 같이 진단 전문인력의 역량은 다양하며, 이를 반영하여 자격제도 역시 등급을 나눌 필요가 있다. 일반적으로 해커들의 역량은 초급(Script Kiddie)부터 엘리트 해커(Elite Hacker)까지 다양하게 구분되는데(Rawal 2022, 21-46), 자격제도 운영의 효율성을 고려하여 너무 많은 등급으로 구분하는 것은 지양해야 한다. 미국이나 주요국의 자격제도에서도 크게 2가지 등급(관리/책임급과 일반 인력)을 나누어 관리하는 것을 참고할 수 있다. 따라서 진단 전문인력 자격제도는 어느 정도의 해킹 지식을 보유하고 실제 공격이 가능한 '중급 해커(Intermediate Hacker)' 수준에서 자격을 부여하고, 이보다 높은 수준의 '고급 해커(Advanced Hacker)'에 대해 상위 자격을 부여하는 등급화 전략을 취하는 것이 필요하다.

또한, 해킹 분야는 웹 해킹, 모바일 해킹, 시스템 해킹 등 매우 다양하며, 특정 유형에 특화된 전문가가 존재한다. 이러한 다양성을 반영하여 세부 분야별로 자격을 세분화하는 '모듈형 자격'을 고려할 수 있다. 이는 전문가에게 자신의 전문 분야에 대한 합당한 인정을 제공하고, 수요자에게는 보다 적합한 인재를 찾는 데 도움이 될 수 있다(관계부처합동 2024, 8). 그러나 초기 운영의 현실적인 어려움을 고려하여, 우선 단일 자격으로 실시하고 추후 산업계의 요구와 기술 발전 추이를 반영하여 세분화하는 방안이 운영 효율적 측면에서 더욱 타당할 것으로 판단된다.

3) 공공/민간 활용 범위와 의무화 여부

자격제도의 실효성 확보를 위해서는 공공 및 민간 부문에서의 활용 범위를 명확히 하고 의무화 여부를 검토해야 한다. 초기에는 자발적인 참여를 유도하되, 공공기관의 사이버안보 업무규정상 진단 업무(특히 중요 정보통신기반시설 취약점 분석·평가)에 '모의침투'를 명시적으로 포함하고, 해당 업무 수행 시 본 자격 취득자 참여를 '권고' 또는 '의무화'하는 방안을 검토할 수 있다.

미국의 경우 정부 부처의 취약점 진단에 대해 모의해킹을 적극적으로 권장하고 있으며, 영국과 독일의 경우에도 정부에서 모의침투를 실시하는 사항에 대해 세부적인 자격 지침 등을 보유하고 있다. 이러한 해외 사례를 참고하여 국내에서도 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드」(과학기술정보통신부·한국인터넷진흥원 2021) 등에서 모의침투를 적극 권장하거나, 법령에서 모의해킹을 의무화하는 방안을 고려할 수 있다.

2. 자격 요건 및 역량 평가 방안

진단 전문인력 자격제도의 성공적인 운영을 위해서는 합리적인 응시 자격 요건 설정과 실무 역량을 정확히 평가할 수 있는 시험 구성이 필요하다.

1) 응시 자격 요건 설정

자격 응시 최소 요건은 제도의 진입 장벽과 신뢰도에 직접적인 영향을 미친다는 점에서 매우 신중하게 설계할 필요가 있다.

앞서 자격제도 설계 시 등급을 구분할 필요가 있다는 점에서 응시

자격 요건 역시 구분하여 검토할 필요가 있다. 기본 등급에 대해서는 가급적 많은 인원이 유입될 수 있도록 별도의 경력 요건을 두지 않는 것이 바람직하다. 이는 해킹 분야에 대한 관심과 잠재력을 가진 인재들이 쉽게 접근할 수 있도록 하여 인력 풀을 확대하는 데 기여할 수 있다. 한편 상위 등급에 응시하는 경우에는 충분한 역량을 검증하기 위해 최소경력에 대한 요건을 설정할 필요가 있다. 실제로 미국의 RVA 운영자 자격에는 3년 이상의 침투테스트 수행 경력을 필요로 하고, 독일의 경우에도 IS 침투 테스터 프로그램에 참여하기 위해서는 최소 2년 이상의 보안 기술적 진단 분야에서의 경력 혹은 최근 2년 이내의 기간에서 최소 100일의 프로젝트 및 5일 이상의 침투 테스트 참여를 요건으로 하고 있다는 점에서 3년 이상의 유관 경력 또는 하위 자격 취득 후 1년 이상의 실무 경력을 요구하는 것이 바람직하다.

또한, 프로젝트 경력이 없더라도 뛰어난 기술력을 갖춘 모의침투 전문가가 다수 존재하므로, 경력 요건 외에 검증 가능한 주요 해킹 대회 수상 실적, 버그바운티 실적, 신규 취약점 연구/발표 실적 등의 비전통적 경력도 인정해줄 필요가 있다. 이는 OSCP와 같은 국제 자격증이 공식적인 사전 응시 요건을 요구하지 않으면서도 높은 수준의 자격을 유지하는 사례를 참고할 수 있다.

2) 시험 구성

진단 전문인력의 핵심 역량이 실무 수행 능력에 있으므로, 시험 방식은 실기 평가를 중점으로 이루어져야 한다. 해외 자격제도들은 필기와 실기를 병행하되, 높은 등급의 자격을 부여할수록 실기 평가에 상당한 시간을 부여하고 결과에 대한 보고서 작성 및 면접을 실시하는 특징을 보인다.

따라서 국내 진단 전문인력 자격제도의 시험은 필기 시험과 실기 시험으로 구성하되, 실기 평가의 비중을 높게 설정하는 것이 적합할 것으로 판단된다.

〈표 1〉 진단 전문인력 자격제도 필기 평가 항목(안)

분류	평가 항목
1. 정보 수집 및 네트워크 스캐닝	• 네트워크 환경에서의 정보 수집 및 스캐닝 기법 이해 • 포트 스캐닝, 서비스 버전 파악, 운영체제 감지 및 네트워크 분석 도구 활용 능력 • 다양한 네트워크 구조와 DNS, Whois, 소셜 엔지니어링 기법에 대한 이론적 이해
2. 웹 애플리케이션 해킹	• OWASP Top 10 웹 취약점 및 공격 기법에 대한 이해 (SQL 인젝션, XSS, CSRF 등) • 웹 애플리케이션 아키텍처, API 보안, 세션 관리 취약점 이론 • RESTful API와 GraphQL API의 취약점 및 공격 기법
3. 모바일 애플리케이션 해킹	• iOS 및 Android 애플리케이션의 구조와 보안 모델 이해 • 모바일 애플리케이션에서의 인증, 암호화 및 데이터 저장소 취약점 • 모바일 앱 리버스 엔지니어링과 API 통신 분석 방법
4. 시스템 해킹	• Windows, Linux 등 주요 운영체제의 내부 구조와 권한 모델 이해 • 버퍼 오버플로우, 파일 권한, SUID 등 시스템 레벨 취약점과 권한 상승 기법 • 로컬 및 원격 익스플로잇 기법에 대한 이론
5. 네트워크 보안 및 프로토콜 분석	• 주요 네트워크 프로토콜 (TCP/IP, HTTP, HTTPS, DNS 등)의 구조와 보안 취약점 • 네트워크 패킷 분석 기법 (Wireshark 등 네트워크 분석 도구) • 보안 프로토콜(TLS, IPsec) 및 VPN 구조에 대한 이해
6. 포스트 익스플로잇 및 후속 처리	• 침투 후 유지 접근(Persistence) 및 데이터 수집 기법 • 로그 분석 및 은폐 기술에 대한 이론 Ÿ 추가 공격 확장 및 시스템 복구 방지 방법론
7. 윤리적 해킹과 법적 준수 사항	• 윤리적 해킹의 원칙과 침투 테스트 윤리 • 법적 규제(정보통신망법, 개인정보보호법 등)와 침투 테스트의 법적 책임 및 규정 • 고객과의 계약서 작성 및 범위 설정 방법론

〈표 2〉 진단 전문인력 자격제도 실기 평가 항목(안)

분류	평가 항목
1. 네트워크 스캐닝 및 정보 수집 능력 평가	• Nmap, Netcat 등을 사용하여 네트워크, 포트, 운영체제, 서비스 정보를 수집하는 실습 • 소셜 엔지니어링을 통한 정보 수집, DNS 레코드 분석 등
2. 웹 애플리케이션 침투 테스트	• SQL 인젝션, XSS, CSRF 등의 웹 애플리케이션 공격 수행 • Burp Suite 또는 Zap Proxy를 활용한 웹 애플리케이션 취약점 스캐닝 및 수동 공격 • 파일 업로드, 인증 우회, API 공격 및 세션 탈취 등 심화된 웹 취약점 공격 수행
3. 모바일 애플리케이션 침투 테스트	• 모바일 앱 분석을 위한 리버스 엔지니어링 수행 (Android APK, iOS IPA 파일 분석) • 모바일 API 통신 분석 및 공격 수행 • 데이터 저장소 분석(모바일 데이터베이스 접근 및 탈취), 코드 주입 및 인증 우회 등
4. 시스템 해킹 실습	• Windows 및 Linux 환경에서의 권한 상승 실습 (SUID, 패스워드 해싱, Lateral Movement 등) • 메타스플로잇, 버퍼 오버플로우 익스플로잇 및 권한 상승 수행 • 로컬 취약점을 활용한 시스템 접근 및 제어 권한 확보
5. 네트워크 및 프로토콜 공격	• 네트워크 패킷 분석(Wireshark 등 사용), 패킷 캡처 및 분석을 통해 취약점 식별 • Man-in-the-Middle (MITM) 공격, ARP 스푸핑, DNS 포이즈닝 실습 • TLS 및 VPN 해제(SSL/TLS 스니핑) 및 관련 보안 조치 회피
6. 포스트 익스플로잇 및 흔적 은폐	• 시스템 내 흔적 제거(로그 파일 조작 및 삭제) • 공격 후 유지 접근(Persistence)을 위한 스크립트 설치 및 레지스트리 설정 • 시스템 설정, 백도어 설치 등 후속 공격을 위한 시스템 유지 접근
7. 보고서 작성 및 프레젠테이션 평가	• 수행한 침투 테스트 과정과 결과를 명확하게 보고서에 작성 • 보고서에는 각 공격의 상세 설명, 취약점, 권고 사항, 개선 방안 등을 포함하여야 하며, 고객이나 상위 관리자에게 설명할 수 있는 능력 평가 • 시험 후 프레젠테이션을 통해 보고서의 주요 내용을 요약 및 설명하는 발표 능력 평가

제안된 시험 구성은 OSCP 등 국제 최고 수준의 실기 중심 평가 모델을 반영하였다. 특히 '보고서 작성 및 프레젠테이션'을 실기 평가에 포함하는 것은 단순한 기술적 침투 능력을 넘어, 진단 결과를 이해관계자에게 명확히 전달하고 설득하는 '컨설팅 역량'까지 평가하겠다는 의지를 보여준다. 이는 진단 전문인력이 단순히 기술자에서 벗어나 '보안 전략가'로서의 역할을 수행하는 데 필요한 역량이기 때문이다. 이처럼 기술적 역량과 더불어 커뮤니케이션 능력을 평가함으로써, 발견된 취약점이 실제 조직의 보안 개선으로 이어질 수 있도록 하는 실질적인 가치를 창출할 수 있다.

3. 자격 갱신 및 교육 체계 연계 방안

자격제도의 활성화를 위해서는 교육 이수 의무화를 포함하는 방안을 검토해야 한다. 특히 윤리 교육과 법률 지식은 진단 전문인력에게 필수적인 소양이므로, 자격시험 응시 요건으로 이수 의무를 지정하는 것 역시 가능할 것이다.

교육 커리큘럼은 실무 중심의 접근 방식을 채택해야 하며, 이론 교육과 실습 교육의 적절한 분배를 통해 수강생이 직접 모의침투를 실습할 수 있는 환경을 제공해야 한다. 이때, 기존 교육 제도의 활용도 가능 할 것이다. 한국인터넷진흥원(KISA)의 K-Shield 프로그램이나 한국정보기술연구원(KITRI)의 Best of the Best(BoB), 화이트햇 스쿨 등 국가 교육 프로그램의 노하우와 인프라를 적극적으로 활용할 수 있다. 또한 라온시큐어, SK쉴더스, NSHC 등 민간 기업에서 제공하는 실습형 교육 프로그램과의 연계를 통해 교육의 질과 현장 적합성을 높일 수 있다. 특정 교육기관의 교육 이수를 의무화하기보다는, 민간

업계에서 다양한 보안 교육 산업이 발전할 수 있도록 자율적으로 다양한 교육을 이수할 수 있도록 하는 것이 장기적인 관점에서 긍정적인 효과를 가져올 것으로 예상된다.

이러한 교육 체계는 자격제도의 갱신과도 연계될 수 있다. 앞서 확인한 바와 같이 사이버 위협 환경은 매우 빠르게 변화하므로, 자격 취득 후 지속적인 역량 개발 없이는 전문성이 빠르게 퇴색될 수 있다. 따라서 자격제도의 공신력을 유지하고 사회적 신뢰를 확보하기 위해서는 정기적인 재교육 및 갱신 체계가 필수적이다.

대부분의 국제 해킹 및 정보보안 자격증이 2~3년마다 갱신이 필요하며, 교육 수강, 학점 취득, 재시험 응시 등을 요구하고 있는 것처럼 국내 진단 전문인력 자격제도에도 3년의 유효 기간을 설정하고, 해당 기간 내에 관련 교육 이수나 재시험을 통해 자격을 갱신하도록 의무화할 필요가 있다. 재교육에는 반드시 최신 사이버 공격 기술 트렌드, 변화하는 법률 및 정책, 윤리적 이슈 등을 포함하여, 자격 취득자가 항상 최신 지식과 기술을 유지할 수 있도록 해야 한다. 이는 자격제도가 장기적으로 시장에서 인정받고 활용될 수 있는 기반을 마련할 것이다.

V. 결론

디지털 전환이 가속화되는 오늘날, 사이버 위협의 양상은 갈수록 지능화되고 있으며, 이에 효과적으로 대응하기 위한 고도의 전문 인력의 필요성이 절실히 대두되고 있다. 특히 모의해킹을 포함한 취약점 진단은 사이버 방어 체계의 선봉에 위치한 기술로, 이 분야에 특화된 전문 인력을 체계적으로 양성하고 인증하는 제도의 도입은 국가와 산업 전반의 보안 역량을 획기적으로 제고할 수 있는 핵심 수단이 될 것이다. 본 연구는 그러한 필요성을 반영하여, 공격자의 시각에서 보안 취약점을 분석하고 이를 실제로 해결할 수 있는 실무 능력을 평가하는 자격제도의 필요성과 방향성을 제시하였다.

이미 미국, 영국 등 주요 선진국에서는 모의해킹을 기반으로 한 진단 자격제도를 운영하고 있으며, 이를 통해 사이버보안 인력의 전문성을 제고하고 있다. 미국 CISA의 RVA 프로그램, 영국의 CHECK 프로그램, 그리고 OSCP, CEH 등과 같은 국제적 자격은 실무 중심의 평가 체계를 통해 현장에 바로 투입 가능한 인재를 선별하고 있다. 이는 한국형 자격제도 설계 시 실기 중심의 평가 비중 강화, 윤리 교육과 법적 소양 평가의 포함, 그리고 자격 유효기간 설정을 통한 지속적 전문성 유지 등 구체적인 설계 방향에 있어 중요한 시사점을 제공한다.

자격제도의 운영 방식에 있어서는 국가자격과 민간자격의 장단점을 비교 분석한 결과, 공공성과 신뢰성을 확보하기 위해서는 국가 공인을 전제로 하되, 민간의 실무 전문성과 유연성을 반영한 혼합형 모델이 적절할 것으로 판단된다. 한국인터넷진흥원(KISA)이나 한국정보

기술연구원(KITRI)과 같은 전문 기관이 주관이 되어 자격제도를 운영하되, 민간 보안기업과 교육기관이 협력하여 실기시험과 교육 커리큘럼을 공동 개발하고 운영하는 방식이 바람직할 것이다. 이를 통해 변화하는 기술 환경에 탄력적으로 대응하면서도, 자격제도의 실효성과 공신력을 동시에 확보할 수 있을 것이다.

또한, 자격 취득을 위한 교육은 특정 기관에 한정하거나 학위 요건을 부여하는 방식보다는, 다양한 민간 교육 프로그램의 자율적 선택을 허용함으로써 보안 교육 산업 전반의 생태계를 활성화하는 방향이 요구된다. 자격 유지를 위해 일정 주기의 재교육이나 재인증 제도를 도입하는 것도 실무 적합성과 윤리의식을 지속적으로 유지하는 데 효과적이다. 이는 주요 국제 자격에서도 보편적으로 채택되는 방식이며, 고급 기술을 보유한 인력이 사회적 책임을 다할 수 있도록 유도하는 장치로서 기능한다.

결론적으로, 본 연구는 모의해킹 기반 진단 전문인력 자격제도의 필요성과 설계방향, 운영방식에 대한 구체적인 제언을 통해, 사이버 보안 인재 양성의 새로운 제도적 전기를 마련하고자 하였다. 자격제도는 단순한 인증 수단을 넘어 국가의 사이버 방어 역량을 강화하고, 정보보호 산업 전반의 수준을 높이는 핵심 인프라로 작동할 수 있다. 향후에는 본 연구를 바탕으로 민관 협의체를 구성하여 실질적인 자격제도 도입에 필요한 정책적·기술적 설계 작업이 구체화되어야 할 것이다.

〈참고문헌〉

과학기술정보통신부·한국인터넷진흥원. 2021.『주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드』

과학기술정보통신부·한국인터넷진흥원. 2024.『2024년 사이버 보안 위협 분석과 전망』

과학기술정보통신부·한국인터넷진흥원. 2024.『정보보호 전문서비스 기업 지정 제도 해설서』

관계부처합동. 2024.『국가기술자격 혁신방안 – 제5차 국가기술자격 기본계획』

김민진. 2024. “법원 전산망 해킹으로 살펴본 공공기관 정보 보안 현주소.”『테크월드뉴스』(6월 5일) https://www.epnc.co.kr/news/articleView.html?idxno=301562 (검색일: 2025.6.5.)

김영명. 2022. “아파트 ‘월패드 해킹’ 피의자 검거... 범인은 보안 전문가였다!”『보안뉴스』(12월 20일) https://www.boannews.com/media/view.asp?idx=112743 (검색일: 2025.6.5.)

김영명. 2023. “워크넷, 해외 IP에서 사용자 계정으로 로그인 시도 포착...개인정보 유출.”『보안뉴스』(7월 7일) https://www.boannews.com/media/view.asp?idx=119929 (검색일: 2025.6.5.)

김영명. 2024a. “지난해 법원 전산망 해킹...2년여간 1,014GB 분량 및 5,171개 문서 탈취.”『보안뉴스』(5월 12일) https://m.boannews.com/html/detail.html?idx=129709 (검색일: 2025.6.5.)

김영명. 2024b. “2023년 국내 공공기관, 일 평균 162만건 사이버 공격 받았다.”『보안뉴스』(1월 24일) https://m.boannews.com/html/detail.html?idx=126047 (검색일: 2025.6.5.)

문가용. 2022. “너무나 위협적인 해킹 ‘공급망 공격’, 2022년에도 가장 두려운 이름.”『시큐리티월드』(1월 16일) https://www.boannews.com/media/view.asp?idx=104140&kind= (검색일: 2025.6.5.)

문정후. 2022. “[주말판] 워너크라이 랜섬웨어 사태 5주년을 기념하며.”『보안뉴스』(5

월 14일) https://www.boannews.com/media/view.asp?idx=106772 (검색일: 2025.6.5.)

박일. 2024. "보안기업의 공급망 보안 강화 위한 '취약점 관리 방법'." 『보안뉴스』 (6월 28일) https://m.boannews.com/html/detail.html?idx=130920 (검색일: 2025.6.5.)

양준규. 2025. "SKT 공격은 APT 공격… 미궁 속 악성코드 침투 3년." 『SKYDaily』(5월 20일) https://www.skyedaily.com/news/news_view.html?ID=273558, (검색일: 2025.6.5.)

조재학. 2025. ""해킹 공격은 실전"…IT취약점 찾아주는 착한 해커기업 뜬다." 『전자신문』(5월 26일) https://lrl.kr/cXpYR (검색일: 2025.6.5.)

Bundesamt fur Sicherheit in der Informationstechnik(BSI). 2016. Praxis-Leitfaden: IT-Sicherheits-Penetrationstest.

Bundesamt fur Sicherheit in der Informationstechnik(BSI). 2022. IS-Webcheck – Sicherheits-Check fur Webauftritte durch das BSI

CISA. 2022. "Cyber Assessment Fact Sheet – Risk and Vulnerability Assessment." https://www.cisa.gov/sites/default/files/publications/VM_Assessments_Fact_Sheet_RVA_508C.pdf (검색일: 2025.6.5.)

CISA. 2023. Assessment Evaluation and Standardization (AES) Program Overview, 8-11.

CISA. 2024a. FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide, 1.

CISA. 2024b. "Assessment Evaluation and Standardization Program." https://www.cisa.gov/resources-tools/programs/assessment-evaluation-and-standardization-program (검색일: 2025.6.5.)

CREST. 2022. CREST Registered Tester Certification Examination Notes for Candidates

GOV.UK. 2023. "The Network and Information Systems Regulations 2018", (January 20) https://www.gov.uk/government/collections/nis-

directive-and-nis-regulations-2018 (검색일: 2025.6.5.)

Hammond, Anna. 2024. "How to optimize your vulnerability management process."(July 31) https://www.intigriti.com/blog/business-insights/how-to-optimize-your-vulnerability-management-process (검색일: 2025.6.5.)

Mancao, Michael. 2022. Offensive Security OSCP Exam with AD Preparation

NCSC. 2022. Penentration testing

NCSC. 2024. Assured CHECK Scheme Standard V1.1

PTES. 2014. "High Level Organization of the Standard." (August 16) http://www.pentest-standard.org/index.php/Main_Page (검색일: 2025.6.5.)

Rawal, Bharat S., Gunasekaran Manogaran, and Alexender Peter. 2022. "The basics of hacking and penetration testing." *Cybersecurity and Identity Access Management*. Singapore: Springer Nature Singapore, 21-46.

The Cyber Scheme. 2022. SYLLABUS.

Tidy, Joe. 2021. "Colonial hack: How did cyber-attackers shut off pipeline?." 『BBC』 (May 11) https://www.bbc.com/news/technology-57063636 (검색일: 2025.6.5.)

UK Government Security. 2024. Principle: A2 Risk Management

Ullah, Faheem, et al. 2025. "What Skills Do Cyber Security Professionals Need?." arXiv preprint arXiv:2502.13658.

A Study on the Classification of Cyber Intrusions Based on National Situations and the Establishment of Governing Bodies

Lim Ji-Hun | School of Cybersecurity, Korea University

As digital transformation accelerates, cyber threats are not only increasing in quantity but also becoming more sophisticated in quality. The recent surge in Advanced Persistent Threats (APTs) and supply chain attacks targeting the public sector, including attacks on critical national infrastructure that significantly impact national security (such as the recent SKT hacking incident), clearly demonstrates the limitations of existing defense-centric security strategies. Consequently, the importance of proactive security diagnostics performed from an attacker's perspective is being highlighted, leading to a rapidly increasing demand for personnel specialized in this field. However, current domestic cybersecurity certification systems are criticized for focusing predominantly on general security knowledge and management capabilities, failing to adequately verify advanced practical hacking skills.

To address these issues, this study theoretically and practically examined the feasibility of introducing a certification system for diagnostic specialists. It conducted an in-depth comparative analysis of diagnostic work frameworks and certification systems in major countries, drawing implications for their application in South Korea. Furthermore, it proposed a practical-oriented certification system design that reflects the current state of domestic education and the demands of the industry.

The introduction of such a certification system is expected to significantly contribute to enhancing South Korea's cybersecurity capabilities, elevating the status and professionalism of diagnostic specialists, revitalizing the security industry, and ultimately, improving public trust.

Keyword Cybersecurity Diagnosis Professional, White Hat Hacker, Penetration Testing, Vulnerability Analysis, Certification System