특집 05

보안 엔지니어링 국가직무능력 표준화 동향

조수빈·한민수·고승철 (수원대학교)

목 차 »

1. 서 론

국내 정보보호 산업계는 2013년도 발생된 대형 금융기관과 대기업의 고객 정보유출 등 보안사고와 개인정보보호법 시행에 따른 사업 확대로 말미암아 보안 인력에 대한 수요가 급격히 확대되는 추세이다. 특히 금융감독원이 총 IT 인력의 5% 이상, 예산의 7% 이상을 보안에 투자하도록 금융기관에 권고한 결과, 기존 보안 인력들이 금융권으로의 이직이 심각하게 진행되었으며, 보안 산업계의 인력 부족 현상은 매우 심각한 현실이다[1].

2012년 현재, 국내 4년제 대학교에 27개, 전문대학에 4개의 정보보호 관련 학과들에서 496명의 졸업생들을 배출하였으며, 있으며, 대학원 과정 25개의 학과에서 260명의 고급 인력들을 배출 하였으나, 보안 산업계에서 필요한 인력 규모와는 큰 차이를 보이고 있다[2].

보안 산업계는 즉각적인 업무 투입이 가능한 경력직원들을 선호하고 있으나, 필요한 경력 직원 수가 절대적으로 부족한 결과, 부득이 신입직원들을

〈표 1〉 2014년도 정보보호 산업계 인력채용 동향

연구개발		관리		영업		관련직		합계	
신입	경력	신입	경력	신입	경력	신입	경력	신입	경력
224	272	48	60	67	123	68	85	407	540
496(52.4%)		108(11.4%)		190(20.1%)		153(16.2%)		947(100.0%)	

자료 : 2013 정보보호산업실태조사, 지식보안산업협회

채용하고 있으며, 대학 등 교육기관에서 실시한 정보보호 교육 내용과 산업계 현장에서 필요한 직무 역량의 심각한 괴리 때문에, 신입직원 재교육 등 직원 실무역량 강화에 기업의 에너지를 소모하고 있는 실정이다.

따라서 교육기관들을 통해, 보안 산업계 현장에서 즉시 투입 가능한 우수한 정보보호 전문 인력 양성을 위한 특단의 대책이 필요하다. 정부는 보안 산업계의 이러한 문제점들을 해소할 목적으로, 정보보안 산업 중심의 전문 인력 양성을 위해, 국가직무표준 개발 사업의 일환으로, 보안 엔지니어링 직무표준을 정보기술 직무 표준의 세 분류 과제로 채택하고, 2014년도부터 표준 및 활용 패키지 개발을 추진하고 있다.

본고에서는 개발될 보안 엔지니어링 직무표준이 산업계와 교육기관에서 널리 활용되어, 국내 정보보호 산업의 발전과 현장 중심의 인력 양성을 목적으로, 2014년 6월부터 시작된 보안 엔지니어링 직무표준과 활용 패키지 개발 동향을 소개한다.

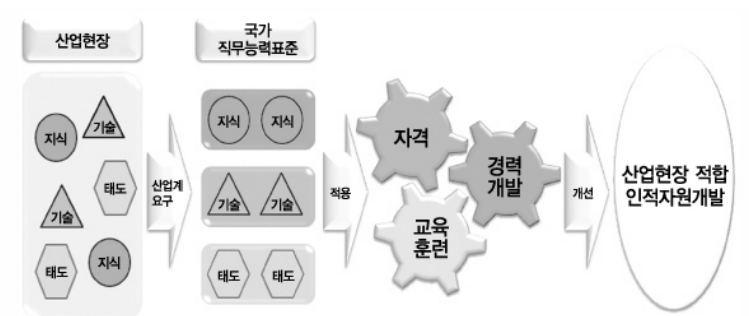
2. 국가직무능력표준 소개

국가자격기본법 제2조에 따르면, 국가직무능력표준(NCS: National Competency Standards)은 산업현장에서 직무를 수행하기 위하여 요구되는 지식·기술·소양 등의 내용을 국가가 산업부문별·수준별로 체계화한 것으로, 산업현장의 직무를 성공적으로 수행하기 위해 필요한 능력을 국가적 차원에서 표준화한 것을 의미한다[3].

정부는 2012년도부터 국내 대학과 직업교육 및 각종 자격제도의 주요 내용들이 산업현장과 괴리가 존재하여, 산업계는 교육과정 이수 및 자격증을 취득한 학생들을 대상으로 현장 교육을 실시해야만 업무에 투입할 수 있는 낭비가 초래되는 문제점들을 해소하고, 학벌이 아닌 능력 중심의 사회 구현을 목적으로, 현장과 실무 중심의 직무 능력표준 개발을 추진하고 있다.

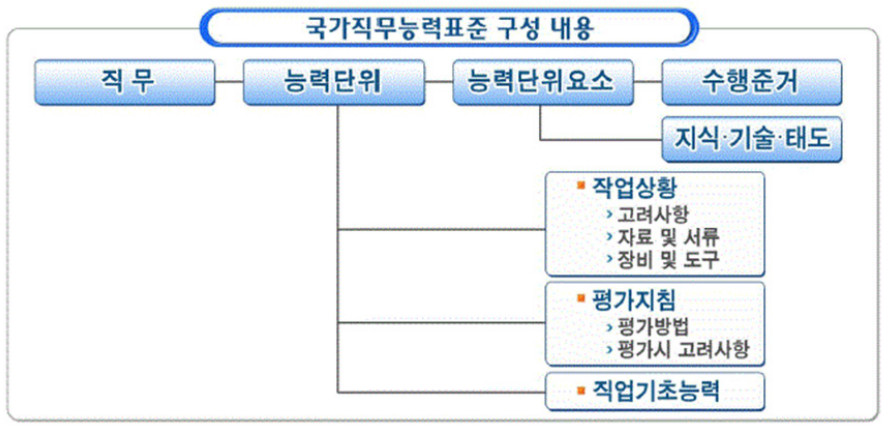
직무능력표준은 한 사람의 근로자가 해당 직업 내에서 소관 업무를 성공적으로 수행하기 위하여 요구되는 실제적인 수행능력을 의미하며, 직무 정의와 능력단위 및 능력단위 요소, 그리고 능력단위 요소별로 필요한 수행준거와 지식, 기술, 태도로 구성된다.

국가직무능력표준은 산업현장의 직무수요를 체계적으로 분석하여 제시함으로써 '일-교육·훈련-자격'을 연결하는 고리, 즉 인적자원개발의 핵심 토대로 기능하며, 교육훈련기관의 교육훈련과정, 직업능력개발 훈련기준 및 교재 개발 등에 활용되어



자료 : 국가직무능력표준개발 매뉴얼 2014. 고용노동부

(그림 1) 국가직무능력표준 개념도



자료 : 국가직무능력표준개발 매뉴얼 2014. 고용노동부

(그림 2) 국가직무능력표준 구성내용

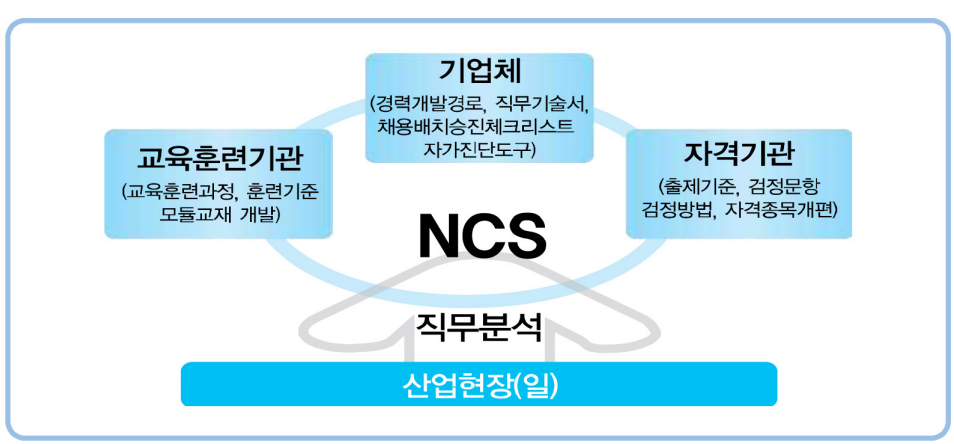
산업 수요 맞춤형 인력양성에 기여하는 동시에, 근로자를 대상으로 경력개발경로 개발, 직무기술서, 채용·배치·승진 체크리스트, 자가진단도구로 활용 가능하다.

한국산업인력공단에서는 국가직무능력표준을 활용하여, 교육훈련과정, 훈련기준, 자격종목 설계, 출제기준 등 제·개정시 활용하며, 한국직업능력개발원에서는 국가직무능력표준을 활용하여 전문대학 및 마이스터고·특성화고 교과과정을 개편을 추진 중이다.

3. 보안 엔지니어링 직무표준 개발 과정

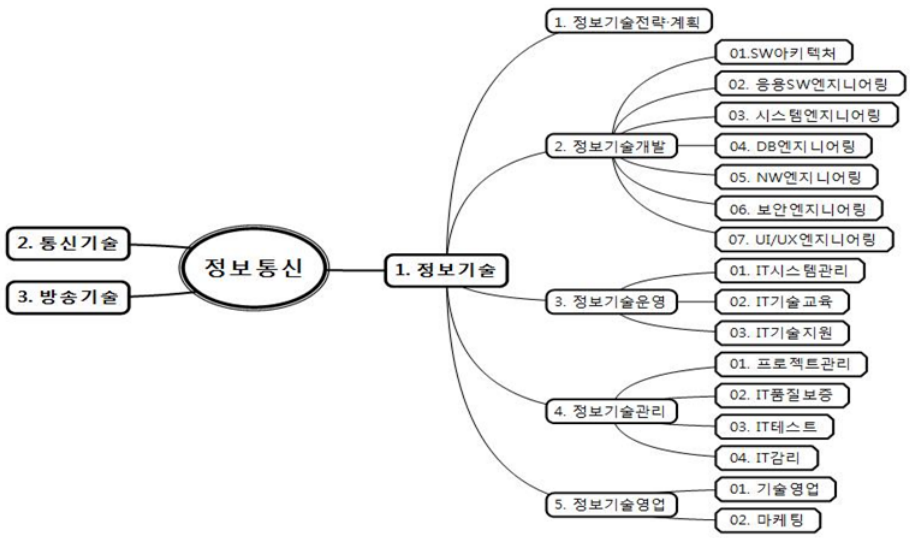
국가직무능력표준에서는 일반적으로 직무를 대분류-중분류-소분류-세분류로 분류한다. 보안 엔지니어링 직무는 대분류인 정보통신 직무에 소속된 1개 세분류로 직무로 개발된다.

표준 개발은 진행 책임자 1명과 산업현장 전문가



자료 : 국가직무능력표준개발 매뉴얼 2014. 고용노동부

(그림 3) 국가직무능력표준 기능



자료 : 소프트웨어 산업협회 발표 자료

(그림 4) 보안 엔지니어링 직무의 위치

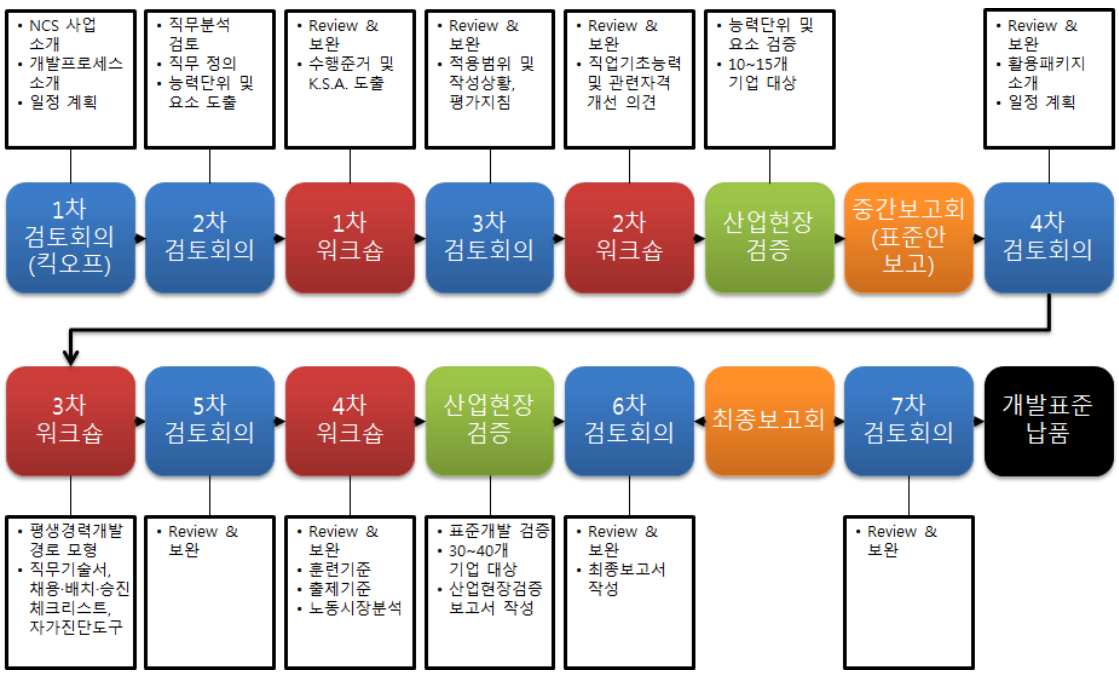
7명 그리고 교육훈련 전문가 3명 및 자격 전문가 1명으로 구성된 개발팀에 의해, 7회의 검토회의와 4회의 워크샵을 거쳐 개발되며, 그 결과는 산업 현장 전문가들과 중간보고회 및 최종보고회를 거쳐 국가직무표준(안)으로 확정된다.

4. 보안 엔지니어링 직무표준 개요

보안 엔지니어링 직무는 보안이론과 실무능력을 갖추고 정보자산을 보호하기 위하여, 계획을 수립하고 위험을 평가하며 요구사항에 따라 보안체계를 구축 및 운영하는 일로 정의된다. 보안 엔지니어링 직무는 보안계획 수립 등 10개의 능력단위로 구성되며, 각각의 능력단위는 3 - 5개 정도의 능력단위 요소로 구성된다.

능력 단위 보안계획 수립은 조직의 최고 수준의 보안정책 수립을 목적으로, 보안 환경을 분석하고, 보안 범위를 설정하며, 보안 목표를 수립하는 능력이다. 보안계획 수립은 보안환경 분석과 보안범위 설정, 보안목표 수립 과정을 통해 진행되며, 필요 지식 및 기술에는, 보안사고 원인과 사고과정 분석 지침에 관한 지식, 보안사고 대응절차에 관한 지식, 국내 정보보호 관련 법과 규정에서 정의된 조직의 보안 역량에 관한 규격에 대한 이해, 컴퓨터와 네트워크의 취약점 분석 기술, 국내외 정보보호 유관기관들이 발표한 보안지침 해석 능력, 국내 정보보호 법률과 규정 분석 해석 능력 등이 필요하다.

능력 단위 보안위험평가는 보호하여야 할 자산을 식별, 분석하고 내재된 취약성을 도출하여 자산에 대한 위협의 종류와 영향을 분석, 평가함으로써 위험의 정도를 산정하는 능력이다. 보안위험을 평가하기 위해서는, 정보자산 조사 능력, 정보자산관리 도구 사용 기술, 사용자 계정관리 기술, 정보보호 아키텍처 분석 능력, 정보보호 IT기술 등이 필요하며, 평가자는 정보보안에 대한 논리적이고 객관적인 사고와 식별 대상 자산의 누락을 방지하기 위한 적극적인 노력 그리고 조직의 보안시스템 구성과 현황을 지속적으로 숙지하려는 노력 및 관련 이해 당사자와의 협업을 위한 개방적 태도가 요구된다.



자료 : 소프트웨어 산업협회 발표 자료

(그림 5) 보안 엔지니어링 직무표준 개발절차

능력 단위 보안요구사항 정의란 사용자의 관리적, 물리적, 기술적 보안요구사항을 도출, 분석, 명세화하고 요구사항의 오류를 검증하는 능력이다. 보안요구사항을 정의하기 위해서는 사용자의 요구내용에 대한 적극적인 수용의지와 원활한 의사소통을 위해 대화법을 준수하려는 태도 및 사용자의 의견을 경청하여 분석하려는 노력이 필요하며, 이를 이행하기 위해서는 정보보호 전략과 IT전략, 보안공학(Security Engineering) 기본 개념, 소프트웨어 공학과 요구공학, SWEBOK(Software Engineering Body of Knowledge) 및 소프트웨어 개발방법론과 같은 지식이 필요하다.

능력 단위 관리적 보안 구축이란 정보보호 정책을 수립하고, 이를 시행 및 유지관리 할 수 있는 정보보호조직을 구성하여, 조직의 인적보안을 관리하는 능력이다. 관리적으로 보안을 구축하기 위해서 필요한 지식 및 태도에는, 정보보호 및 개인정보보호 관련 법률에 대한 이해, 문서 작성 능력, 문서에 대한 형상관리 기술을 지니고 있어야 하며 요구사항을 모든 판단과 활동의 기준으로 하는 태도, 법적 준거성을 준수하려는 노력, 주어진 현상의 근본 원인을 파악하려는 노력이 필요하다.

능력 단위 물리적 보안 구축이란 물리적 보호구역을 지정하고, 시스템을 보호하며, 사무실 보안을 구축하는 능력이다. 물리적 보안 구축을 하기 위해 요구되는 지식 및 기술에는, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적된 정보통신시설의 보호), 방송통신설비의 기술기준에 관한 규정, 정보보호관리체계 국제표준(ISO/IEC 27001), 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS), 네트워크 이론 등의 지식이 필요하며 시스템 및 네트워크 구축 능력과 문서작성 능력의 기술이 요구된다.

능력 단위 기술적 보안 구축이란 정의된 보안 요

구사항에 적합하게 어플리케이션 보안, 서버 보안, 네트워크 보안, DB 보안을 설계, 구현, 테스트하는 능력이다. 운영체제별 보안을 설치하는 기술, 서버별 인증 접근통제 구현 관리 능력, 서버 보안 소프트웨어 설치 및 운영 기술, 서버 및 운영체제 취약점 분석 능력 및 로그 분석 도구 기술을 지니고 있어야 하며, 모든 활동에 보안 요구사항 준수하고 설계된 서버 보안을 준수하여 구현하려는 노력을 하며 객관적인 테스트와 적극적인 문제해결 태도가 요구된다.

능력 단위 보안체계 운영관리능력이란 보안엔지니어링을 위하여 운영보안체계를 수립하고 이에 따라 직원의 정보보호 교육을 수행하며 침해사고대응 및 IT재해사항 발생 시 복구를 진행하는 능력이다. 갖추어야 할 태도 및 지식에는, 업무의 객관적 수행의 자세, 근본원인 파악을 위하여 접근하는 태도와 분석적 사고방식 그리고 조직과 사용자중심의 사고, 법률 준수 태도 및 식별 대상 자산의 누락을 방지하기 위해 적극적으로 노력을 하며 주어진 절차를 준수하려는 의지를 가지고 있어야 한다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 정보보호 대상의 분류를 위한 개인정보보호법에 대한 지식, 보안관련 규정 지침 및 프로세스, 정보보호관리체계(ISMS) 및 개인정보보호관리체계(PIMS) 등의 지식이 필요하다. 능력 단위 보안관제 수행이란 보안위협으로부터 정보자산을 보호하기 위해 구축된 보안 시스템을 통하여 보안위협을 탐지, 분석, 대응하고 사후 처리하는 능력이다. 네트워크 개념, 시스템 이론, 네트워크와 시스템 취약점에 관한 지식, 네트워크와 시스템 보안 설정 지식, 보안위협 원리 등의 지식을 바탕으로 보안관제시스템 사용 기술과 보안시스템 로그분석 도구 사용 기술 그리고 네트워크와 시스템 취약점 분석 능력 및 보안위협 행위 분석 능력, 취약점 점검 체크리스트 관리 능력이 요구된다.

능력 단위 보안감사 수행이란 보안과 관련된 통제절차의 기록과 행동을 독립적으로 조사하고 관련 증거를 수집하여 분석함으로써 주요 정보자산의 기밀성, 무결성, 가용성을 점검하는 능력이다. 보안감사를 수행하는 것은 보안감사를 계획하고 수행하며 시정조치를 확인하는 과정으로 진행된다. 감사 자동화 도구(CAAT) 사용 기술과 디지털 포렌식 기술, 인터뷰 능력 및 감사증적 수집 및 분석 기술을 바탕으로 수행하며 피감사인에 대한 사후 인터뷰시 강압적이거나 권위적이지 않은 태도로 대해야 하며 시정조치 결과에 대한 현장점검시 합리적인 자세로 임해야하고 보안감사 수행 평가 및 학습 교훈(Lessons Learned) 작성시 적극적인 노력을 해야하는 것과 같은 태도가 필요하다.

능력 단위 보안인증 관리란 조직이 정보보호 관리체계를 구축・운영하고 있을 때, 보안인증기준에 적합한지를 인증기관으로 하여금 객관적이고 독립적인 평가를 통해 적합성 여부를 검 증받는 능력이다. 보안인증 관리는 보안인증을 준비, 신청하여 심사를 받으며 부적합사항이 있으면 조치를 취하고, 보안인증을 사후 관리하는 순서로 진행되며 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법과 보안관련 정책·지침·절차, 정보보호관리체계에 관한 국제 표준 규격(ISO27001), 정보보호관리체계(ISMS) 등과 같은 지식이 바탕이 되어야 하며 문서작성 능력, 감사 자동화 도구(CAAT) 사용 기술, 감사자료 수집 및 분석 등과 같은 기술, 보안감사 기획 능력을 갖추어야 한다.

4. 결 론

본고에서는 실무중심의 전문 인력 양성을 목적으로 개발된 국가직무능력 표준을 소개하였으며, 정보통신 분야의 세 분류 과제로 개발되고 있는 보안 엔지니어링 직무표준 개발과정과 주요 내용들을 소개하였다.

최근 급속하게 성장을 지속하고 있는 정보보호 산업계는 보안 직무능력을 보유한 우수한 인력 확보에 큰 애로를 겪고 있다. 대학 등 각급 교육기관의 교육과정과 산업계에서 필요한 직무 역량과의 불일치로 말미암아, 기업들은 경력직들을 선호하며, 부득이 신입직원을 채용한 경우, 재교육을 실시 등 다양한 형태의 실무 인력 확보에 큰 어려움을 호소하는 실정이다.

교육기관은 보안 엔지니어링 직무표준을 사용하여, 보안 산업 실무에 즉각 투입이 가능한 현장중심 보안 엔지니어들을 배출하여, 국내 정보보호 산업 발전에 기여하기를 기대한다.

참 고 문 헌

[1] 지식보안산업협회, 2013 정보보호산업실태조사, 2013년 12월.
[2] 국가정보원, 미래창조과학부, 방송통신위원회, 안전행정부, 2013 국가정보보호백서, 2014년 4월.
[3] 고용노동부, 한국산업인력공단, 국가직무능력표준개발 매뉴얼, 2014년 4월.

저 자 약 력

조 수 빈
이메일 : jsb9040@naver.com

• 2012년~현재 수원대학교 정보보호학과 / 학생

한 민 수
이메일 : item9009@naver.com

• 2010년~현재 수원대학교 정보보호학과 /학생

고 승 철
이메일 : goh5703@hanmail.net

• 1981년 연세대학교 수학과 (학사)
• 1983년 연세대학교 수학과 (석사)
• 1992년 포항공대 수학과 (박사)
• 1984년~1996년 한국전자통신연구원 / 책임연구원
• 1996년~2004년 한국인터넷진흥원 / 기반사업본부장
• 2004년~2008년 지식보안산업협회 / 상근부회장
• 2011년~현재 수원대학교 정보보호학과 /교수
• 관심분야 : 융합보안, 네트워크 보안, 암호응용 기술