

소프트웨어안전 법제의 제도적 실행력 확보방안 고찰

이중엽, 박태형

소프트웨어정책연구소

ilovebiz@gmail.com, parkth@spri.kr

Institutional Effectiveness of the Software Safety Legal Framework: A Strategic Approach

Lee Joong-Yeup, Park, Tae Hyung

Software Policy & Research Institute(SPRI)

요약

본 논문은 원자력, 항공, 자동차 등 필수안전 산업을 중심으로 소프트웨어 안전관리의 현황을 분석하고, 제도적 정비 방향을 고찰한다. 산업별로 기준과 지침은 점차 마련되고 있으나, 제도 간 정합성과 정책 연계 측면에서 보완이 필요한 지점이 확인된다. 단기적으로는 지침의 구체화, 적용 대상 명확화, 정보 공유 기반 마련이 중요한 과제로 제시되며, 중장기적으로는 보다 구조적인 대응 방안도 향후 검토될 수 있다. 이를 통해 소프트웨어 안전관리의 일관성과 실효성을 높일 수 있을 것으로 기대된다.

I. 서론

디지털 전환 시대에 소프트웨어(software)가 사회 전반의 핵심 인프라로 활용되면서, 소프트웨어 안전(software safety) 확보의 중요성이 크게 부각되고 있다. 실제로 항공, 철도, 자동차, 원자력, 의료, 국방 등 다양한 분야에서 소프트웨어 오류로 인한 사고가 보고되고 있으며, 이는 소프트웨어 안전 문제가 단순한 기술적 품질 문제가 아니라 국민 생명과 안전에 직결되는 사회적 문제임을 보여준다. 예컨대 자동차 급발진이나 철도 신호시스템 오류 등 소프트웨어 결함으로 인한 사례들은 인명 피해로 이어져, 소프트웨어의 안정성을 체계적으로 보장할 필요성을 드러냈다. 이러한 배경에서 각국은 제4차 산업혁명 시대에 부응하여 자율주행차나 스마트시티 등 SW 중심 혁신분야의 안전 확보를 위한 정책과 규범을 정비하기 시작했다. 우리나라에서도 소프트웨어 안전을 뒷받침할 법제도 정비가 시급한 과제로 대두되고 있다.

현재 국내의 소프트웨어 안전 관련 법제는 「소프트웨어진흥법」을 중심으로 근거를 마련하고 있으며, 구체적인 안전관리 사항은 대부분 행정 규칙인 고시 형태로 운용되고 있다. 2020년 전부개정을 통해 소프트웨어 안전의 개념 정의와 정부의 지침 제정 근거가 법에 도입되었고, 이에 따라 과학기술정보통신부 장관이 「소프트웨어안전 확보를 위한 지침」(이하 소프트웨어안전 지침)을 제정하여 공공부문에 적용하고 있다. 그러나 이러한 지침(고시) 중심의 운용에는 한계가 있다. 지침의 적용 범위는 주로 공공기관에 국한되고 법적 구속력도 강제적인 차별 조항 없이 권고적 수준에 머물러 있어, 실효성 확보가 어렵다는 지적이 나온다. 특히 민간 부문의 경우 해당 지침의 직접적 의무 대상이 아니어서 안전관리 기준의 확산이 제한적이다. 이러한 상황에서 제도적 실행력을 갖춘 법제 정비, 즉 법률 차원의 규율과 강제력 확보가 필요하다는 요구가 높아지고 있다.

본 연구의 목적은 소프트웨어 안전 관련 현행 법제도의 한계를 진단하고, 법정책적 및 법체계적 분석을 통해 실행력 있는 입법 대안을 모색하는 것이다. 구체적으로, 공공부문 고시 중심의 현 체계를 개선하여 법률적 구속력과 제도적 실효성을 강화할 방안을 검토한다. 이를 위해 우선 법정책적 검토와 법체계적 검토의 개념과 필요성을 살펴보고, 현행 소프트웨어안전

법제(소프트웨어진흥법 및 지침)의 내용을 분석한 뒤, 단계별 입법 대안을 제시하고 평가하고자 한다. 마지막으로 단기·중기·장기의 로드맵을 제안함으로써, 소프트웨어안전 법제의 단계적 발전 방향을 제시한다.

II. 법정책적 및 법체계적 검토의 개념과 필요성

입법 대안을 도출하는 과정에서, 법정책적 검토와 법체계적 검토는 서로 보완적인 분석 틀을 제공한다. 법정책적 검토(policy-oriented legal review)란 입법안이나 제도의 내용이 당초 목표한 정책 목적을 얼마나 효과적으로 달성할 수 있는지 평가하고, 사회·경제적 과급효과나 실현 가능성 등을 따져보는 분석이다. 즉, 제도가 현실의 문제를 해결하고 공익을 증진하는 데 적합한지, 대안적인 정책수단과 비교하여 효율성과 수용성이 높은지 등을 검토한다. 입법 과정에서 법정책적 분석은 해당 규제가 갖는 필요성, 타당성, 효과성을 검증하여, 실질적으로 정책 목표에 부합하는 입법이 이루어지도록 방향을 제시하는 역할을 한다.

반면 법체계적 검토(system-oriented legal review)는 제안된 법령이나 제도가 기존 법체계와 조화를 이루는지를 살펴보는 분석이다. 여기에는 새로운 규정이 상위법령이나 헌법에 부합하는지, 기존 관련 법률들과 충복·충돌은 없는지, 용어와 구조가 일관된 체계를 갖추는지 등의 검토가 포함된다. 법체계적 분석을 통해 해당 입법이 법률체계의 정합성을 유지하면서도 적절한 규범 계층(법률-시행령-고시 등)에서 제정되는지 판단할 수 있다. 입법 과정에서 법제 전문기관(예: 법제처)은 이러한 법체계적 검토를 수행하여 입법안의 형식적 완결성과 체계 정당성을 확보하도록 한다.

본 연구에서는 소프트웨어안전 법제 개선 방안을 모색함에 있어 이 두 가지 관점을 모두 활용하였다. 먼저 현행 제도의 문제점을 법정책적 측면에서 분석하여, 왜 현 제도가 실효성을 갖지 못하는지 정책적인 원인을 규명하였다. 동시에 각 대안별로 법체계적 측면에서의 적합성을 따져, 제도가 현행 법률 구조 내에 적절히 위치할 수 있는지, 다른 법률과의 관계는 적절한지를 검토하였다. 이러한 이중의 분석 과정을 거친으로써, 실질적 효과와 형식적 정합성을 고루 갖춘 제도화 방안을 도출하고자 한다. 요컨

대, 법정책적 합리성(정책 목표 달성 가능성)과 법체계적 정합성(법률 체계 내 논리성)을 모두 고려하는 것이 안전 분야 입법 전략 수립에 필수적이다.

III. 소프트웨어안전 확보를 위한 입법 대안 비교

대안1. 고시 개정 강화

현행 과학기술정보통신부 고시인 「소프트웨어안전 확보를 위한 지침」을 중심으로 하는 행정규칙 수준에서 소프트웨어 안전관리 체계를 유지해, 지침 내용을 개정·보완하여 실효성을 높이는 방안이다. 예를 들어 국민 안전과 직결되는 “안전관리 대상 소프트웨어”를 지정하여 공공기관이 해당 소프트웨어를 의무 관리하도록 하고, 위험 분석, 안전 확보를 위한 설계·구현, 시험·검증, 사고 대응 절차 등 세부 기준을 강화한다. 또한 행정규칙 차원에서 소프트웨어안전위원회 신설, 전담 지원기관 지정, 정보공유 체계 구축 등의 거버넌스 요소도 도입할 수 있다. 이는 별도의 법률 제정 없이 부처 협의를 통해 현행 고시에 일부 안전 거버넌스 체계를 반영하는 접근이다. 법 개정 절차 없이 부처 고시 변경만으로 시행할 수 있어 신속하고 유연하게 제도를 강화할 수 있다. 또한 기존 법령 체계를 건드리지 않으므로 다른 법과 충돌이나 중복 우려가 적고, 관계 부처 협의로 추진 가능하여 제도 이행이 비교적 용이하다. 다만, 행정규칙인 지침의 법적 구속력과 제재 수단이 약해 실효성 확보에 한계가 있다.

대안2. 「소프트웨어진흥법」 개정

기준에는 해당 법 제30조에 근거해 지침 고시 수준으로 안전관리 규정을 두었으나, 이제 법률 자체에 안전관리 의무와 조직 근거를 명문화함으로써 진흥법이 산업 진흥을 넘어 안전 확보까지 포괄하는 상위 법적 근거가 되도록 한다. 또한 법률 개정을 통해 “소프트웨어안전”的 정의를 명확히 하고, 국가의 소프트웨어 안전 확보 책무와 관계 기관의 역할을 법에 규정한다. 법률에 안전조항을 두면 지침에 비해 훨씬 강한 법적 구속력과 권위를 갖게 되므로, 공공뿐 아니라 민간도 법상 의무를 준수하게 되어 제도의 실효성이 높아진다. 또한 법적 근거가 생기면 관련 예산 확보나 전담 조직 설치 등이 용이해져 제도의 안정적 정착에 도움이 된다. 완전히 새로운 법을 만드는 것이 아니므로 입법 저항이 적고 신속한 통과가 가능하다는 점도 장점이다. 다만 산업 육성 목적의 법률에 안전 규제 조항을 추가하면 법 목적과 내용의 일관성이 저해되어 입법 취지가 혼재될 위험이 있다는 지적이 있다. 아울러 진흥법 개정만으로는 원칙적 수준의 규정에 그칠 가능성이 높아 세부 사항은 다시 하위법령이나 지침에 위임될 수 있다.

대안3. 「소프트웨어안전기본법」 제정

소프트웨어 안전만을 전담하는 신규 기본법을 제정하여 포괄적이고 독립적인 소프트웨어 안전 법체계를 구축하는 방안이다. 가칭 「소프트웨어 안전기본법」을 통해 소프트웨어 안전 확보를 위한 원칙, 책임, 거버넌스 구조 등을 종합적으로 규정하고, 필요시 각 분야별 개별 법률에 대한 상위 기준법 역할을 부여하도록 설계한다. 이 법은 여러 부처와 산업 분야를 아우르는 범정부 차원의 법률로, 현행 개별 법령들에 흘어진 소프트웨어 안전 규정을 하나로 묶는 역할을 할 수 있다. 또한 예방(안전성 평가·인증) - 대비(교육·훈련, 위기관리계획) - 대응(사고 보고, 긴급명령) - 복구(피해구제, 재발방지) 등 소프트웨어 안전관리 전 단계에 걸쳐 국가와 사업자의 의무를 법체계 내에 규정함으로써 전주기적 안전관리 체계를 구현할 수 있다는 장점도 가진다. 다만, 새로운 법률을 만드는 데는 관계자 의견 수렴, 부처 협의, 국회 심의 등 상당한 입법 시간과 비용이 소모될 수 있다. 또한 중복되어 규제 중첩이나 충돌이 발생할 소지도 있다. 이에 현실적으로 중장기적 로드맵을 갖춰 진행하는 것이 요구된다.

앞서 비교한 바와 같이, 대안 1에서 대안 3으로 갈수록 규율의 포괄성과 강제력은 커지지만, 동시에 준비에 필요한 시간·비용과 이해당사자 조율 난이도도 증가한다. 따라서 현실적으로 세 가지 대안을 순차적으로 단계별 추진하는 점진적 접근 전략이 합리적이다. 즉, 단기에는 대안 1을 실행하여 현행 지침을 신속히 개정·강화하고, 중기에는 대안 2를 통해 법률상의 기반을 마련하며 제도 정착을 도모하고, 장기에는 사회적 필요성과 사건의 성숙도를 보아 대안 3(기본법 제정)을 검토하는 경로가 바람직하다. 무엇보다 모든 단계에 걸쳐 “안전과 혁신의 균형” 원칙이 일관되게 관통되어야 함을 강조한다. 규제가 과도해져 산업 발전을 저해하지 않도록 주기적으로 규제 영향을 평가하고, 중소기업 등 취약 주체에 대한 지원을 병행함으로써 지속 가능한 안전관리 생태계를 구축해야 할 것이다.

IV. 결론

본 연구에서는 소프트웨어안전 확보를 위한 법제의 제도적 실행력 강화 방안으로서 세 가지 입법 대안을 검토하고 단계별 추진전략을 제안하였다. 현행 고시는 공공부문을 중심으로 한 기본 프레임워크로서, 소프트웨어 안전관리의 최소 기준과 절차를 제시하는 데 의의가 있다. 고시는 한계도 분명하여 그 개정만으로 직접 규율할 수 없고, 모든 산업 분야의 소프트웨어를 포괄하기 어렵지만, 공공부문의 선도적 역할을 통해 민간 부문의 자발적 안전관리를 견인하는 레퍼런스 모델로 기능할 수 있다. 즉, 당장은 고시의 적용 범위 밖에 있는 민간 영역이라 하더라도 공공부문의 모범 사례와 표준이 축적됨에 따라 이를 벤치마킹하고 자율적 안전체계를 갖출 필요성이 높아질 것이다. 이러한 점에서 정부의 고시 체계는 향후 민간의 안전문화 정착을 위한 선도 프레임워크로서 중요하다.

소프트웨어안전 법제 정비의 궁극적인 목표는 국민의 생명과 재산을 보호하고 디지털 사회의 신뢰 기반을 강화하는 데 있다. 단편적인 기술 기준을 넘어 제도적 실행력을 갖춘 법적 기반을 마련함으로써, 소프트웨어로 인한 사고를 예방하고 사고 발생 시 효과적으로 대응할 수 있을 것이다. 이는 곧 디지털 전환 시대의 지속가능한 발전을 위한 필수 전제조건이라 할 수 있다. 향후 입법 과정이 진행될 경우 이러한 목표를 견지하면서, 현실에 부합하는 최적의 입법 대안을 선택·조합하여 추진해야 할 것이다. 소프트웨어안전은 한 번에 완성되는 것이 아니라 단계적으로 진화하는 것이므로, 체계적이고 유연한 접근으로 실행력을 갖춘 법제를 구현해나가는 노력이 요구될 것이다.

* 본 논문은 2025년 과학기술정보통신부 SW공학경쟁력강화사업의 지원을 받아 수행된 연구의 일부 내용을 바탕으로 작성되었음.

참 고 문 헌

- [1] 과학기술정보통신부, 소프트웨어안전 확보를 위한 지침 (고시 제 2020-77호), 2020.
- [2] 박태형, 이중엽 & 손효현, (2024) 소프트웨어 안전 사고 사례로 보는 소프트웨어 안전 체계 필요성, 소프트웨어정책연구소(SPRi).
- [3] 이중엽 & 박태형, (2024) 미래 모빌리티 동향 및 SW안전 시사점, 소프트웨어정책연구소(SPRi).
- [4] 이중엽 & 박태형, (2025). 테슬라 오토파일럿 판결로 보는 SW안전 시사점, 소프트웨어정책연구소(SPRi).
- [5] 이중엽, & 박태형. (2025). SW 안전 주요산업의 관리 현황과 시사점. 한국통신학회 학술대회논문집, 1736-1737.