규제연구 제29권 제2호 2020년 12월

합리적 규제설계를 위한 위험평가 활용방안의 탐색적 연구*

심 우 현**·박 정 원***

많은 경우 정부의 규제정책은 산업발전을 위한 규제 완화와 생명보호와 안전을 위한 규제 강화라는 선택의 갈림길에 서 있다. 이처럼 상반된 목표를 앞에 두고 정부는 때때로 최선의 합리적 선택이 아닌 두 입장을 적절히 만족시키는 절충적·혼합적 방식의 의사결정을 손쉽게 하곤 한다. 특히, 신산업 분야의 경우 이러한 two-track 방식의 의사결정이 '산업발전 가능성'과 '기술·서비스의 다양한 불확실성과 위험'을 동시에 고려할 때 어느 정도 불가피한 측면이 있다. 그러나 신산업이 '기회'와 '위험'을 같이 내포했다고 해서 이러한 절충적 규제정책이 항상 정당화될 수는 없다. 산업의 활성화와 위험 최소화 사이에서 적절한 규제수준을 정하는 것이 어렵지만 포기되어서는 안 된다. 본 연구는 신산업 분야에서 합리적 규제설계를 위한 위험평가 프레임워크의 적용 방안을 탐색하였다. 구체적으로 미국국립표준기술연구소(NIST)의 위험평가 방법을 응용·적용하여 위협의 식별과 위협 시나리오의 구성 방법을 제시하고, 시나리오와 관련된 위협의 발생 가능성과 영향의 확인을 통해 위험 수준을 평가하는 작업과 시나리오와 연관된 규제와 시나리오에서 확인된 위험 수준의 차이 분석을 통해 적절한 규제수단을 도출하는 방법을 제시하였다. 결론

* 본 연구는 2018년 한국행정연구원 연구보고서(사물인터넷 환경 발전에 따른 규제 쟁점과 대응방안 연구)의 일부 분을 소논문으로 발전시킨 것임을 밝힙니다.
** 제1저자, 한국행정연구원 규제혁신연구실 연구위원, 서울 은평구 진흥로(whshim@kipa.re.kr)
*** 교신저자, 안동대학교 행정학과 조교수, 경상북도 안동시 경동로(jwpark@anu.ac.kr)
접수일: 2020/12/7, 심사일: 2020/12/18, 게재확정일: 2020/12/21

에서는 혁신성장을 견인하기 위해 정부가 시행 중인 다양한 규제개혁 전략의 한계점을 논하고, 신산업 분야에서 위험평가 및 규제개선을 위한 위험평가 프레임워크의 적용의 필요성을 논하였다.

핵심 용어: 위험평가, 규제설계, 시나리오, 규제, 신산업

I. 서론

지능정보기술의 급격한 발전은 기존에 오프라인에서 독립적으로 작동하던 사물(제품)이 다양한 센서와 통신 모듈을 통해 다른 사물, 인간, 시스템과 실시간으로 정보를 주고받으며, 정보의 폭발적인 증가와 이를 활용한 자동적·지능적 서비스를 가능하게 하고 있다. 이는 또한 정보통신기술로 대표되는 사이버 시스템과 물리적 시스템의 통합을 의미하는 사이버-물리 시스템(CPS, cyber-physical system)의 발전을 촉진하고 있다.

사이버-물리 환경의 통합이 특히 활발히 이뤄지는 신산업 분야에서는 센싱 기술(센서를 통해 신체, 위치, 환경 정보를 감지하는 기술), 네트워킹 기술(통신 칩을 통해 네트워크상에서 정보를 전달하는 기술) 및 인터페이스 기술(정보를 수집·가공·해석하여 특정 서비스에 전달하는 소프트웨어 기술)의 수요 및 활용이 급속히 증가하는 추세이다. 이러한 기술들은 생활 가전(스마트 홈, 원격 검침), 공공안전(CCTV 보안, 재난관리), 보건의료(디지털 의료기기, 원격진료), 산업(스마트공장, 스마트빌딩), 자동차(원격 차량 관리, 자율주행 자동차) 등 다양한 신산업 분야에서 활용되면서 제품과 서비스의 부가가치를 높이고 있다.

이러한 신산업 분야는 사이버-물리 환경의 통합이 제품과 서비스의 효용을 높여 만족도와 편의성을 높이는 순기능을 발생시키는 동시에, 개인정보 유출, 사생활 침해, 보안사고, 기기의 오작동 등 다양한 부작용의 발생 가능성도 증가시키고 있다. 특히, CPS 기술이 적용된 신산업 분야는 실생활과 산업현장에서 광범위하게 인터넷을 활용하기 때문에, 이러한 부작용은 단순히 소수 사용자의 피해를 뛰어넘어 사회 전체에 광범위한 위해를 발생시킬 가능성이 크다. 예를 들어 해커가 자율주행차를 해킹할 경우 차량의 구동장치 및 조향장치를 마음대로 조절하여 운전자·동승자에게 위해를 끼칠 수 있을 뿐만 아니라,

동일 모델 자동차의 사용자도 잠재적으로 위험에 노출되는 체계적 위험(systemic risk)의 발생 가능성이 있는 것이다. 한편, 통신 기능을 가진 약물 주입용 디지털 의료기기의 오작동과 같이 기기의 결함이 환자 한 명의 안전이 아니라 다수 환자의 안전을 위협하는 심각한 문제를 초래할 수도 있다. 따라서, 신산업 분야에서 제품·서비스의 이용에 따른 만족과 편의를 충분히 누리기 위해서는 이로 인해 발생할 수 있는 역기능을 적절히 통제할 수 있는 대책의 마련이 필요하다. 우리 정부는 신산업 분야에서 등장하고 있는 다양한 기술·제품·서비스의 활용으로 발생할 수 있는 순기능과 역기능을 인지하고, 법적·제도적 장애 요인을 제거하여 순기능의 강화에 노력함과 동시에 역기능을 효과적으로 통제하기 위한 다양한 안전대책의 강구를 추구하는 투 트랙(two track)전략을 시행 중이다. 따라서, 우리 정부의 신산업 분야 정책은 산업 활성화를 위한 규제 완화의 측면과 위험·피해를 최소화하려는 규제 강화의 측면이 혼합되어 있다고 할 수 있다. 이러한 쌍대(雙對)적 정책 추구는 신산업 분야의 '산업발전 가능성'과 '기술·서비스의 다양한 불확실성과 위험'을 동시에 고려할 때 불가피한 것이라 하겠다. 문제는 신산업 분야의 진흥과 규제, '산업 활성화'와 '기술·서비스의 위험 최소화' 사이에서 적절한 규제수준을 정하는 것이다. 산업 활성화만을 위해 위험을 내버려 둘 수도 없으며, 모든 발생 가능한 위험을 막기 위해 무작정 규제를 강화할 수도 없기 때문이다.

그렇다면 신산업의 활성화와 위험 최소화가 둘 다 포기할 수 없는 정책목표인 가운데 어떻게 적절한 규제수준을 정할 수 있을 것인가? 특히, 기존 산업과 다르게 신산업 분야와 같이 필연적으로 높은 예측의 불확실성이 존재하는 경우에 어떻게 이에 대응한 규제수준을 정할 것인가? 본 연구는 이러한 질문에 대한 답을 제시하고자 한다. 구체적으로, 본 연구는 높은 예측 불확실성이 존재하는 신산업 분야의 활성화를 추구하면서도 위험을 최소화할 수 있는—반대로 위험을 최대한도로 통제하면서도 신산업 분야의 활성화를 이룰 수 있는— 적절한 규제수단을 결정하는 방법을 제시하는 것을 목적으로 한다. 이를 위해 본 연구에서는 위험평가의 개념을 도입하여 신산업 분야에서 발생할 수 있는 위험 수준을 도출하고, 이를 규제수단과 연계할 수 있는 연구·분석 프레임워크를 개발하였다. 또한, 이를 통해 신산업 분야의 제품·서비스에 대한 현행 규제수준에 대응하여 위험 수준별로 적절한 규제 대응전략이 무엇인지를 제시하였다.

신산업 분야의 위험평가를 통해 본 연구는 위험 수준이 높은 경우에 대해 현재의 규제

대응 수준이 미흡한 경우 위험을 최소화하기 위한 규제 대안을 제시하고, 반대로 위험 수준이 낮음에도 불구하고 현행 규제가 과도할 경우 산업 진흥에 초점을 둔 규제 대안을 제시하고자 한다. 이처럼 위험평가에 기초한 규제 대응 체계의 마련은 신산업의 활성화와 위험의 최소화라는 두 마리 토끼를 잡기 위한 최적의 규제전략 마련에 기여할 수 있을 것으로 생각된다.

II. 위험평가의 이론적 고찰

1. 위험평가의 개요

위험(risk)[1]은 잠재적 상황·사건에 의해 위협받는 정도를 나타내는 척도를 의미한다. 일반적으로 위험은 위협 상황 또는 사건의 발생으로 인해 나타난 부정적인 영향과 발생 가능성을 결합한 함수로 정의된다. 여기서 위협(threat)[2]의 발생 가능성(likelihood of occurrence)은 바람직하지 않은 결과 또는 영향을 초래하는 의도적 혹은 비의도적 위협사건으로 인해 악영향이 발생할 가능성의 추정치를 의미한다. 한편, 위협사건의 영향도(impact)는 위협사건이 실제로 발생하면 초래될 것으로 예상되는 정보 손실·파괴나 서비스 거부·중단 등과 같은 피해의 정도를 말한다. 정보 분야를 예로 들면, 정보 관련 위험이란 정보 혹은 정보시스템의 기밀성(confidentiality), 무결성(integrity) 또는 가용성(availability)에 손실을 일으키는 사건의 발생 가능성과 이로 인한 자산·개인·조직·국가 등에의 부정적인 영향의 함수를 의미한다(NIST, 2012: 6). 위험은 제품·서비스·사업 등에 따라 다르게 측정되며, 신산업 분야에서도 분야, 시스템 등에 따라 상이하게 평가된다고 할 수 있다(Macaulay, 2016: 279).

위험평가(risk assessment)는 위험의 수준을 평가하기 위한 것으로, 일반적으로는 특정 자산, 제품, 서비스, 시스템 등에 대해 존재하는 위협을 식별하고 이의 수준을 추정하

1) '위험'이란 표현은 영어에서 'danger', 'hazard', 'risk' 등으로 다양하게 표현되며, 그 의미가 조금씩 다르다. 본 연구에서는 '위험'을 영어에서의 'risk'와 같은 의미로 사용한다.
2) 위협이란 자산에 부정적인 영향을 미칠 수 있는 행동으로 일반으로 취약성을 이용하는 행위를 의미한다.

여 위협의 경감을 위한 우선순위를 결정하는 과정으로 정의할 수 있다(NIST, 2012: 1). 구체적으로 위험평가에서는 사이버 혹은 물리적 공격, 오류, 자연재해 등과 같은 위협원(threat sources)에 의해 유발된 위협의 발생 가능성과 영향도를 평가한 후 양자를 결합해 위협사건의 위험 수준을 도출하고, 이를 바탕으로 위협 경감의 우선순위를 도출하고 경감을 위한 도구를 선정한다.

이러한 위험평가는 기술·산업발전의 불확실성과 규제 효과의 불확실성이 높은 신기술·신산업 분야에 특히 효과적으로 사용할 수 있다고 알려져 있다. 기존의 규제설계에 있어서 일반적으로 활용되는 규제영향평가기법들은 이러한 불확실성을 고려하지 못하는 한계점을 지니고 있으므로, 신기술·신산업 분야의 규제설계단계에서 규제영향평가기법에 대해 보완적으로 위험평가를 활용하면 보다 적절한 수준의 규제설계가 가능하다.

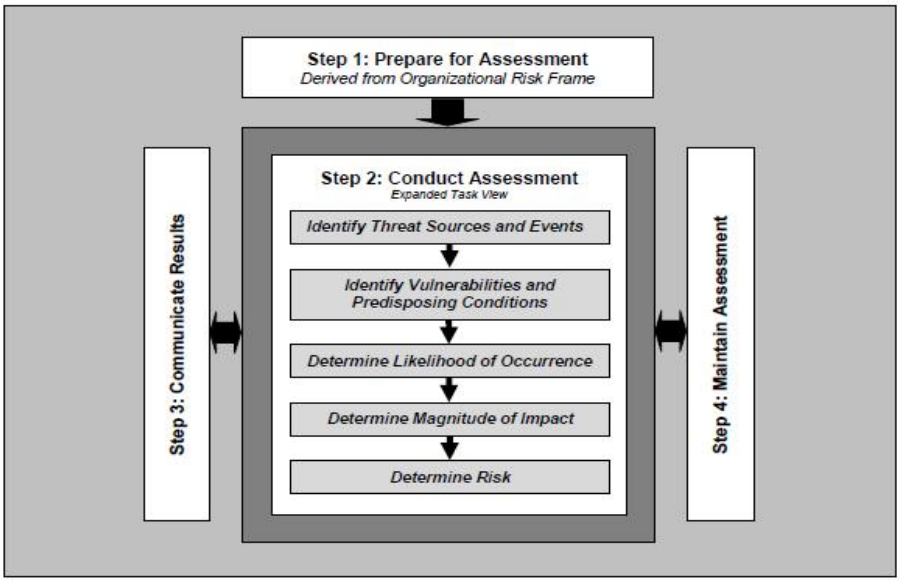
2. 위험평가 방법: NIST SP800-30 (NIST Guide)

널리 활용되는 위험평가 방법으로는 NIST SP800-30, OCTAVE(the Operationally Critical Threat, Asset, and Vulnerability Evaluation), CRAMM(The CCTA Risk Analysis and Management Method), EBIOS(The Expression of Needs and Identification of Security Objectives), MARGERIT(Risk Analysis and Management Methodology for information systems) 등이 있다. 이러한 위험평가 방법은 세부적인 절차에는 차이가 있으나, 위험 수준을 결정하는 방법은 대체로 유사하다고 할 수 있다. 따라서, 여기서는 가장 일반적으로 활용되는 NIST SP800-30을 중심으로 위험평가 방법을 설명하고자 한다.

미국국립표준기술연구소(NIST, National Institute of Standards and Technology)는 IT 시스템 내에서 효과적인 위험관리 프로그램 개발을 위한 가이드라인(SP800-30)을 제공하는데, 이러한 가이드라인은 위험의 평가 및 위험의 완화를 위한 상세한 지침을 포함한다. NIST SP800-30에서의 위험평가는 총 4단계로[3] 구분되며 각각의 단계는 다시 몇 개의 작업(task)으로 세분되어, 위험평가별 단계에 걸친 전체 작업 수

3) 1단계는 위험평가의 준비 단계, 2단계는 위험평가 수행 단계, 3단계는 위험평가 결과를 통한 의사소통 및 위험 관련 정보의 공유 단계, 4단계는 위험평가의 유지 단계이다(NIST, 2012).

〈그림 1〉 NIST 위험평가 절차



출처: NIST(2012: 23)

는 15개에 이른다. 한편 4단계 중 실제 위험평가를 수행하는 절차에 관한 단계는 두 번째 단계로 여기서는 실제 위험평가 단계에서의 6가지 작업 내용을 중심으로 평가절차를 살펴보았다.

NIST 위험평가의 첫 번째 단계는 시스템 특징(system characterization)을 분석하는 단계로 여기서는 위험평가 대상 시스템의 하드웨어, 소프트웨어, 데이터 등의 투입 요소를 확인하여 시스템의 경계, 기능 등을 산출한다. 또한, 이 단계에서는 자산을 식별하게 되는데, 자산이란 조직에서 보유한 가치 있는 모든 것을 의미하며, 크게 유형자산과 무형자산으로 구분된다. 식별된 자산에 대해서는 가치를 평가하게 된다.

둘째, 위협 식별(threat identification)로서 자산에 손해를 입히는 행위 및 환경, 즉 위협에 관해 확인한다. 이 단계에서는 주로 과거에 발생했던 사건을 검토하여 위협을 식별하며, 취약점의 의도적 활용을 노린 계획(intent)과 방식(method) 또는 비의도적으로 취약점을 활용할 수 있는 상황과 방식인 위협원(threat source)에 대해서도 파악하게 된다. 여기서 위협원은 다시 '악의적이고 의도적인 위협(attack)'과 '비의도적(비적대적)

위협'으로 구분된다. 악의적이고 의도적인 위협에 대해서는 공격자의 역량, 의도, 표적화 정도를 평가하며, 비의도적(비적대적) 위협에 대해서는 위협원의 효과 범위를 평가하게 된다. 그리고 위협원별로 발생할 수 있는 위협사건을 식별하여 기술한다. 이러한 분석을 바탕으로 최종적으로 위협 진술문(threat statement)을 작성하게 되다.

셋째, 취약성 분석(vulnerability identification)을 한다. 취약성은 자산의 잠재적 속성으로서 위협의 이용 대상이 되는 것을 의미하는데, 취약성은 자산과 위협 사이에 관계를 맺어 주는 하나의 매개체라고 할 수 있다. 예컨대, 취약성이 없다면 높은 빈도와 강도의 위협이 존재하더라도 손실로 이어지지 않는다. 3단계에서는 이러한 취약성을 식별하고 식별된 취약성의 심각 수준을 평가한다.

넷째, 발생 가능성 분석(likelihood determination)이다. 발생 가능성은 위협적 사건이 악영향을 초래할 가능성을 의미하는데, 적대적 위협사건의 개시 가능성, 비적대적 위협사건의 발생 가능성, 위협사건이 자산에 악영향을 발생시킬 가능성을 종합 평가하여 전반적인 가능성 점수(likelihood rating)를 산출한다.

다섯째, 영향도 분석(impact analysis)을 통해 영향도 점수(impact rating)를 산출한다. 여기서 영향도 분석은 위협이 취약점을 이용하는 데 성공할 경우 초래될 수 있는

〈그림 2〉 적대적 위험표 / 비적대적 위험표

(1) 적대적 위험표

1	2	3	4	5	6	7	8	9	10	11	12	13
위협 사건	위협 출처	위협 출처 특성			관련성	공격 개시 가능성	취약성 및 선행 조건	심각도 및 파급성	개시된 공격의 성공 가능성	전반적인 가능성	영향도	위험
		역량	의도	표적화								

(2) 비적대적 위험표

1	2	3	4	5	6	7	8	9	10	11
위협 사건	위협 출처	영향 범위	관련성	위협 사건 발생 가능성	취약성 및 선행 조건	심각도 및 파급성	위협 사건이 악영향을 초래할 가능성	전반적인 가능성	영향도	위험

출처: NIST(2012)에서 재구성

영향 정도 분석하는 것이다. 영향도 분석 시 영향도 평가 척도를 사용하는데 이때 질적 평가나 준-질적 평가 척도를 사용하는 것이 일반적이다.

여섯째, 위험 결정(risk determination)단계로서, 이 단계에서는 이전 단계에서의 위협적 사건의 발생 가능성과 영향도를 결합하여 위협사건의 위험 수준을 도출한다. 그리고 최종적으로 위험표를 작성하게 되는데, 이때 적대적 위험표와 비적대적 위험표(〈그림 2〉 참조)로 구분하여 작성할 수 있다.

3. 위험평가와 규제수단의 연계

규제는 정부가 가장 손쉽게 활용할 수 있는 정책수단의 하나로, 사회에 발생하는 다양한 위협을 감소시키기 위해 사용되고 있다. 구체적으로 규제는 환경보전, 국민안전, 보건·의료, 시장·산업 활성화 등 그 대상이 무엇이든지 간에 근본적으로 위협의 발생 혹은 위협의 심각성을 감소시키는 데 그 목적이 있다. 따라서 규제를 수립·집행하면서 위협을 식별·분석·심사하는 위험평가는 규제의 정당성에 대한 근거를 제시할 뿐만 아니라 규제의 강도, 범위 등을 결정하는 데 효과적인 도구로 사용될 수 있다. 가장 대표적으로 식·의약품, 재해·재난관리 및 환경 영역에서 위험평가가 폭넓게 활용되고 있다. 예를 들어 국제식품규격위원회가 WTO 체제 아래 객관적이고 과학적인 식품안전관리 방법으로 위험평가 방법을 제안한 이후, 위험평가는 국가적 안전관리 규제를 위한 정책 결정 단계에서 그 역할이 확대되고 있다(김현정, 2013: 27). 이에 해외 여러 국가에서는 식품안전관리나 의약품 첨가제 등에 대한 위험평가 가이드라인을 배포하여 활용하고 있다.

재해 및 재난관리 분야에서도 위험평가가 활발히 도입·활용되고 있다. 예를 들어 우리나라의 경우 반도체 사업장에서의 사고 시 환경에 미칠 수 있는 영향에 대한 위험평가(윤여홍 외, 2015), 지하철 역사 내 미세먼지에 대한 위험평가(오윤희 외, 2013), 터널 화재에 대한 확률론적 위험평가(곽상록 외, 2003) 등 다양한 재해 및 재난관리 분야에 대한 위험평가의 학문적·실증적 연구가 진행되고 있으며, 이를 통해 도출된 결과를 정책에 반영하고 있다.

이처럼 위험평가를 단순히 위험의 수준을 측정·평가하는데 그치지 않고, 위험관리를 위한 유용한 정보를 도출하고 이를 정책에 반영하고자 하는 움직임이 늘고 있다. 특히 우

리나라와는 달리 해외 주요 기관에서는 위험평가를 규제정책에 적용하려는 노력이 지속해서 증가하고 있다. 예컨대, 최근 환경보호를 위한 규제 활동에서 위험평가가 적극적으로 활용되고 있는데, 화학물질 관련 규제의 경우 위험평가—위험 인식(hazard identification), 용량 반응 평가(dose-response assessment), 노출평가(exposure assessment)는 물론 위험관리—결과를 토대로 가장 최적의 정책 기준을 마련하는 행위를 규제 활동 전반에 적용하려는 움직임 일어나고 있다(ACS, 2016: 1). 다음에서는 위험평가와 규제정책을 연계하기 위한 노력을 OECD와 미국을 중심으로 살펴본다.

1) OECD의 위험평가와 규제정책 연계

OECD는 1990년대 후반부터 위험평가와 규제정책을 연계하여 규제의 품질을 높이려고 시도하고 있다. OECD(2002)의 보고서에서는 정량적인 위험평가를 통해 발생 가능한 위협에 대한 우선순위를 판단할 수 있으며, 이를 통해 가장 중요한 위협요소를 최소한의 비용으로 제어할 수 있다고 하였다(OECD, 2002: 130; 김신, 2007: 41 재인용).

OECD는 위험평가와 규제정책의 연계 중요성에 대한 인식 아래, 회원국이 위험평가를 수행하기 위한 제도와 역량을 확보하고 있는지와 이를 규제정책에 활용하고 있는지에 대한 연구·조사를 수행하였다(김신, 2007: 41). 한편 OECD는 2006년 회원국 간 규제정책과 연계한 위험평가의 활용 정도에 차이가 큼을 확인하고, 회원국의 위험·규제의 연계에 대한 인식 제고와 관련 정보·지식의 제공을 목적으로 "위험정책과 정부의 역량(Risk Policy and the Capacity of Governments)" 프로젝트를 진행하는 등 회원국이 위험평가를 규제정책의 수립·집행에 활용할 수 있도록 지속적인 지원을 추진하고 있다(김신, 2007: 41). 또한, OECD는 회원국의 위험평가와 규제정책의 연계 수준을 파악하기 위한 설문을 개발하였으며, 이를 바탕으로 연계의 수준이 낮은 회원국에 대한 위험평가 활용 강화를 주문하고 있다.

2) 미국의 위험평가와 규제정책 연계

미국에서는 1995년 예산관리국(OMB, Office of Management and Budget)과 과학기술정책실(OSTP, Office of Science and Technology Policy)이 합동으로 환

경, 건강, 안전에 위협을 일으킬 가능성이 있는 정책을 분석·평가하는데 활용할 수 있는 원칙을 설정하였다(김신, 2007: 44-5). 「위험분석의 원칙(Principles for Risk Analysis)」이라고 불리는 이 지침은 규제정책의 수립·집행에 있어서 활용해야 할 원칙을 위험평가(risk assessment), 위험관리(risk management), 위험 커뮤니케이션(risk communication), 우선순위 설정(priority setting) 등으로 나누어 제시하고 있으며, 연방 규제기관에 의해 활용되고 있다. 이후 미국은 여러 분야에 위험평가를 지속해서 적용하고 있으며, 이를 바탕으로 OMB는 2006년 규제 전 분야에 대한 위험평가 적용 지침인 「위험평가의 지침안(Proposed Risk Assessment Bulletin)」을 마련하여 전문가와 관련 기관을 대상으로 의견을 수렴하였다.

OMB가 미국 내 연방 규제기관의 위험평가 수행에 있어서 중요한 기준을 제시하는 역할을 수행한다면, 정보규제실(OIRA, Office of Information and Regulatory Affairs)은 위험 분석·심사·평가·관리에 관련된 모든 업무를 수행한다. 미국 대통령령 12866에 따라 OIRA의 직원은 규제 입안단계에서 기관들이 위험평가를 적절하게 시행하고 있는지를 확인하기 위해 모든 중요 규제에 대해 위험평가의 적절성을 검토한다.

한편 미국의 환경보호청(EPA, Environmental Protection Agency)에서 실시하고 있는 절차는 위험평가와 규제정책을 연계하는 대표적인 사례로 꼽힌다. EPA는 1970년대부터 환경 영역에서의 위험평가의 필요성을 인식하여, 염화비닐·발암물질 등에 대한 위험평가를 자체적으로 실시한 바 있으며, 오늘날 "규제 과정(regulatory process)의 일부분으로서 건강상의 위험이나 환경에 대한 영향을 대상으로 엄밀한 위험평가가 시행되어야 함"을 기관의 기본적 가치로 설정하고 있다(EPA, 2020). EPA는 특히 의회에서 통과된 환경법의 세부적 규제 내용을 마련하는 과정에서 위험평가 결과를 활용하고 있으며, 규제 개정 과정에서도 위험평가의 결과를 반영하고 있다.

미국에서는 신기술·신산업 관련 규제에 대해서도 위험평가를 활발히 연계하여 활용하고 있다. 예를 들어 3D 프린트 기술은 패션, 로봇, 의료 등 다양한 영역에서의 활용도가 클 것으로 예상되는 영역으로, 기술 발전의 순기능과 함께 무기제작, 지적 재산권 침해, 의료윤리 저하 등 다양한 역기능을 발생시킬 가능성이 있다(NIST, 2015: 4-5). 이에 따라 미국국립표준기술연구소(NIST)를 중심으로 신기술의 발달에 따라 대두되는 다양한 위험요인에 대해 평가를 시행하고 기존의 관리체계가 관련 위험을 얼마만큼 효과적으로

상쇄시킬 수 있는지 분석하여, 그 결과에 따라 향후 신사업에 대한 규제 기준을 마련하려는 노력이 이뤄지고 있다.

III. 신산업 분야 규제개선을 위한 위험평가 적용 방안

다양한 신산업 분야의 위험과 연계된 규제수단을 도출하기 위해서는 해당 분야에서 발생할 수 있는 위협을 식별하고 위험 수준을 평가하여 이에 대응하는 적절한 규제수단을 선정하는 과정이 필요하다. 본 연구에서는 NIST의 위험평가 방법인 SP800-30를 응용·적용하여 신산업 분야의 위험을 평가하고 이와 연계된 규제수단을 도출하는 방법을 제시해보고자 한다.

본 연구에서는 우선 신산업 분야의 특정 제품·서비스 관련 활동에 있어서 발생할 수 있는 위협을 식별하고, 이를 바탕으로 위협 시나리오를 구성하는 방법을 제시한다. 이후 시나리오와 관련된 위협의 발생 가능성과 영향의 확인을 통해 위험 수준(위험도)을 평가하는 작업과 시나리오와 연관된 규제와 시나리오에서 확인된 위험 수준의 차이(gap) 분석을 통해 적절한 규제수단을 도출하는 방법을 알아본다. 본 연구의 위험평가는 〈표 1〉과 같은 흐름도를 따른다.

〈표 1〉 위험평가 흐름도

단 계	내 용	방 법
1 대상 선정 및 관련 정보 수집·분석	문헌연구, 전문가 자문 및 브레인스토밍을 기반으로 위험평가 대상 분야를 선정하고 관련 정보 수집·분석	문헌연구 전문가 자문 브레인스토밍
2 위협사건의 식별과 시나리오 작성	위협사건을 의도적(악의적) 사건과 비의도적(비적대적) 사건으로 유형화하고 관련 위협 시나리오 작성	문헌검토 전문가 자문
3 위협사건의 평가	① 발생 가능성 평가 • 위협사건이 (자산에) 악영향을 발생시킬 가능성 ※ 5단계 평가: 1(매우 낮음)-2(낮음)-3(보통)-4(높음)-5(매우 높음)	설문 조사
	② 영향도 평가 • 위협이 실현될 경우 초래할 수 있는 영향 정도 ※ 5단계 평가: A(매우 낮음)-B(낮음)-C(보통)-D(높음)-E(매우 높음)	설문 조사

단 계	내 용	방 법
4 위험 수준 및 위험 수준 평가 기준의 도출	① 위협적 사건의 발생 가능성과 영향도 평가를 결합하여 위협사건의 위험 수준 도출 • 각 평가 결과를 결합하여 위험 수준의 정도 도출 ※ A1, A2, A3, …, E3, E4, E5 ② 위험도 산정을 위한 평가 매트릭스 작성 • 위험도를 기준으로 정렬 ※ 5단계 평가: VH-H-M-L-VL	설문 조사
5 관련 규제 파악 및 수준 정리	위협사건의 위험 관련 규제의 파악 및 수준(강도) 정리 • 위협사건의 위험과 관련된 규제와 규제 강도의 확인	문헌검토
6 규제 개선책 제시	도출된 위험과 현 규제와의 차이(gap) 분석을 통해 규제 개선책 제시	전문가 검토

1) 대상 선정 및 관련 정보 수집·분석

이 단계에서는 신산업 분야 중 위험평가를 하고자 하는 대상 분야를 선정한다. 이때 대상으로 선정된 분야가 지나치게 포괄적이면 관련 위협을 모두 식별하기에 어려움이 따를 수 있으므로, 위험평가의 대상은 되도록 세부분야가 되도록 한다. 예를 들어, 신산업 분야 중 사물인터넷 전체를 위험평가의 대상 분야로 선정하는 경우, 그 범위가 지나치게 광범위하여 관련 위협을 모두 식별하는데 과도한 시간·비용이 소요되므로, 사물인터넷 중 스마트카, 스마트헬스, 스마트홈 등과 같이 세부분야를 위험평가의 대상으로 선정하는 것이 바람직하다. 또한, 문헌연구, 전문가 자문, 브레인스토밍을 통해 위험평가를 시행하고자 하는 대상 분야의 특성을 파악하고, 세부분야의 유형자산(시스템 자산, 인력, 물리적 자산)과 무형자산(데이터, 소프트웨어 등)에 대한 정보를 수집·분석한다.

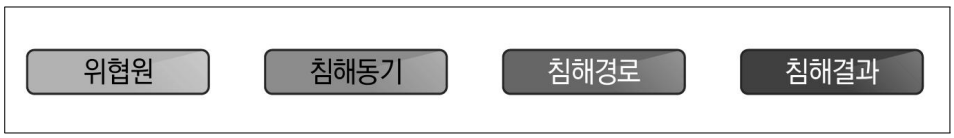
2) 위협사건 식별과 시나리오 작성

2단계에서는 신산업 분야 중 대상 세부분야에서 식별된 각 자산에 바람직하지 않은 결과 또는 영향을 초래할 가능성이 있는 사건 또는 상황, 즉 위협사건을 신문기사, 보고서, 논문 등의 문헌검토와 전문가 자문을 통해 식별한다. 위협사건에는 자연재해, 화재 등과 같이 물리적 안전의 침해로 인해 발생하는 사건과 민감한 정보의 유출, 해킹 등과 같이 사이버 안전의 침해로 인해 발생하는 사건이 있다. 이러한 위협사건은 다시 악의적이고

의도적인 위협과 비적대적이고 비의도적 위협으로 구분할 수 있다.

위협사건이 식별되면 이를 바탕으로 구성요소 세트(위협원, 침해 동기, 침해경로, 침해결과 등)를 확인한다(〈그림 3〉 참조). 위협원은 자산에 악영향을 줄 가능성이 있는 위협을 발생시키는 원천을 말한다. 위협원은 개인, 조직, 국가, 사고, 자연재해, 기기결함, 소프트웨어 취약성 등 매우 다양한 형태를 띠고 있다. 침해 동기는 위협원이 발생시키는 위협이 의도성과 악의를 지니고 있는지를 판단하기 위한 요소이다. 이의 유형은 우연히 기술적 실패 혹은 인적 실패를 발생시키는 비의도적·비악의적인 동기와 범죄 혹은 테러와 같이 특정 목적을 달성하기 위한 의도적·악의적 성격을 지닌 동기로 나눌 수 있다. 침해경로는 위협원이 어떤 접근법을 사용하여 위협을 발생시키는지를 확인하기 위한 요소이다. 침해경로는 크게 네트워크를 통해 위협을 발생시키는 네트워크적 접근과 물리적인 방법을 통해 위협을 발생시키는 물리적 접근이 있다. 침해결과는 위협사건의 발생이 자산에 미치는 결과를 보여준다. 일반적으로 침해결과는 중요한 정보의 오·남용을 발생시키는 정보유출과 자산에 물리적 피해가 발생하는 손실·파괴가 있다.

〈그림 3〉 위협사건의 구성요소 세트



위협사건의 구성요소 세트에 포함되는 구체적인 항목은 관련 문헌의 검토, 전문가 자문 등을 통해 도출한다. 특히, 신산업 분야의 경우 기술·제품·서비스의 완전한 도입이나 전면적인 시장화가 이뤄지지 않은 상황인 경우가 많아 현실성 있는 구성요소 세트를 확인하기에는 어려움이 있을 수 있으므로, 비슷한 성격을 지닌 타 분야의 관련 문헌에 대한 폭넓은 조사가 필요하다.

식별된 위협사건, 관련 구성요소 세트 및 문헌 조사·전문가 자문을 바탕으로 실제 발생 가능한 위협사건을 구체화하는 위협 시나리오를 〈표 2〉의 양식에 따라 작성할 수 있다. 시나리오는 위험평가 과정에서 활용될 수 있도록 시나리오 제목, 위협의 유형, 위협 발생에 따른 침해 분야, 사건의 상세설명 등 필요한 정보를 모두 포함하도록 한다.

〈표 2〉 위협 시나리오 양식

시나리오 제목		해당 시나리오에 대한 간단한 설명
시나리오 구성요소		해당 시나리오에 해당하는 요소
사례 기반 추론	위험 발생원인	위험 발생원인에 대한 상세설명
	발생위험	위험 발생의 결과에 대한 설명
사건의 상세 시나리오		사고 혹은 일련의 사건에 대한 상세 시나리오의 제시
참고 자료		보고서 등 학술자료, 혹은 신문기사 등

위협 시나리오의 개발에 있어서 가장 중요한 사항은 해당 시나리오가 실현 가능성을 가진 구체적인 위협의 서술이어야 한다는 것이다. 따라서 위협 시나리오의 개발을 위해 연구진의 지속적인 브레인스토밍 및 토론과 함께 해당 분야 전문가의 의견수렴이 무엇보다 중요하다고 하겠다. 〈표 2〉의 양식을 이용하여 임시운행 자율주행차에 운전자가 미탑승하는 경우의 위협 시나리오의 예시를 제시하면 다음 〈표 3〉과 같다.

〈표 3〉 임시운행 자율주행차의 운전자 미탑승 행위 위협 시나리오 (예시)

시나리오 제목		임시운행 자율주행차의 운전자 미탑승 행위
시나리오 구성요소		내부자 ▶ 비악의적·비의도적 ▶ 물리적 접근 ▶ 손실·파괴
사례 기반 추론	위험 발생원인	돌발상황 등 특정한 상황에서 수동개입 등의 대처능력 부족
	발생위험	차대차 혹은 차대인 사고로 인한 부상·사망과 재산피해 발생
사건의 상세설명		자율주행차의 출시를 준비 중인 C 사는 고시에 따라 자율주행차의 시험운행을 위한 허가를 취득하는 과정에서 B를 운전자로 지정하였다. 하지만 자율주행을 앞두고 B가 참여할 수 없게 되어, 운전자 없이 시험운행을 진행하였다. 시험운행 도중 커넥티드 카의 오작동으로 인하여 무단횡단 중이던 보행자를 감지하지 못하여 보행자를 치는 사고가 발생하였다.

3) 위협사건의 평가

3단계에서는 식별된 위협의 발생 가능성과 영향도를 위협 시나리오를 통해 평가한다. 발생 가능성은 위협사건이 자산에 악영향을 발생시킬 가능성을 의미하나 엄격한 통계적 의미의 가능성을 의미하지는 않는다. 발생 가능성은 가능한 증거, 경험, 전문가의 판단에 근거하여 점수를 부여한다. 발생 가능성 평가는 전문가 조사를 통해 이뤄지며 〈표 4〉와

같이 5단계의 질적 평가 척도를 활용하는 것이 일반적이다.[4)]

〈표 4〉 위협사건의 발생 가능성

수준	설명
매우 높음 (5)	위협사건이 매우 “분명하게(almost certain)” 발생할 경우 • (예시 1) 위협사건이 1년에 100회 이상 발생 • (예시 2) 해커의 공격 혹은 내부자의 정보유출 등으로 위협사건이 분명히 발생
높음 (4)	위협사건이 “높은 가능성(highly likely)”으로 발생할 경우 • (예시 1) 위협사건이 1년에 10회에서 100회 사이 정도로 발생 • (예시 2) 해커의 공격 혹은 내부자의 정보유출 등으로 위협사건이 발생할 높은 가능성 존재
중간 (3)	위협사건이 “어느 정도의 가능성(somewhat likely)”으로 발생할 경우 • (예시 1) 위협사건이 1년에 1회에서 10회 사이 정도로 발생 • (예시 2) 해커의 공격 혹은 내부자의 정보유출 등으로 위협사건이 발생할 어느 정도의 가능성 존재
낮음 (2)	위협사건이 발생할 가능성이 “거의 없는(unlikely)” 경우 • (예시 1) 위협사건이 1년에 1회 미만 발생하지만 10년에 1회 이상은 발생 • (예시 2) 해커의 공격 혹은 내부자의 정보유출 등으로 위협사건이 발생할 가능성이 거의 없음
매우 낮음 (1)	위협사건이 발생할 가능성이 “전혀 없는(highly unlikely)” 경우 • (예시 1) 위협사건이 10년에 1회 미만 발생 • (예시 2) 해커의 공격 혹은 내부자의 정보유출 등으로 위협사건이 발생할 가능성이 전혀 없음

위협사건이 실제로 발생하면 초래될 수 있는 영향(손해)의 정도 역시 발생 가능성과 마찬가지로 5단계의 질적 척도 평가를 통해 조사할 수 있으며, 자세한 평가 기준은 〈표 5〉와 같다.

4) 정성적 평가 외에도 정량적(quantitative) 및 준-정량적(semi-quantitative) 방법의 평가도 가능하다(NIST, 2012: 14). 특히, 사이버보안, 산업안전, 환경 등과 같은 분야에서는 기존의 통계치를 활용한 정량적 평가의 활용이 폭넓게 이루어지고 있으나, 신기술·신산업 분야는 이러한 통계자료의 확보가 어려우므로 일반적으로 전문가 판단에 기반한 정성적 평가가 이루어지는 것이 일반적이다.

〈표 5〉 위협사건의 발생 영향도

수준	설명
매우 높음 (E)	위협사건이 자산, 개인, 집단, 기관, 국가 등에 여러 심각하고도 재앙적 수준의 역효과를 불러올 수 있음 • (예시 1) 위협사건 발생이 대규모로 일어나고 손실이 매우 큼 • (예시 2) 해커의 공격이 시스템에 영향을 미침
높음 (D)	위협사건이 자산, 개인, 집단, 기관, 국가 등에 심각한 또는 재앙적 수준의 역효과를 불러올 수 있음 • (예시 1) 위협사건 발생의 손실이 매우 큼 • (예시 2) 해커의 공격이 대부분 시스템에 영향을 미침
중간 (C)	위협사건이 자산, 개인, 집단, 기관, 국가 등에 중요한 역효과를 불러올 수 있음 • (예시 1) 위협사건 발생이 손실을 일으킴 • (예시 2) 해커의 공격이 일부 시스템에 영향을 미침
낮음 (B)	위협사건이 자산, 개인, 집단, 기관, 국가 등에 제한적 역효과를 불러올 수 있음 • (예시 1) 위협사건 발생이 경미한 손실을 일으킴 • (예시 2) 해커의 공격이 소수의 시스템에 영향을 미침
매우 낮음 (A)	위협사건이 자산, 개인, 집단, 기관, 국가 등에 무시할 수 있는 수준의 역효과를 불러올 수 있음 • (예시 1) 위협사건 발생이 매우 경미한 손실을 일으킴 • (예시 2) 해커의 공격이 극소수 시스템에 영향을 미침

4) 위험 수준 및 위험 수준 평가 기준의 도출

이 단계에서는 우선 위협사건의 전반적인 발생 가능성(1, 2, 3, 4, 5)과 영향도(A, B, C, D, E)를 결합하여 위협 시나리오의 위험조합(A1, A2,…, E4, E5)을 작성하며, 각 위협이 재산·인명의 손실, 피해 등 역효과를 일으킬 수 있는 위험 수준을 평가한다. 위험 수준은 매우 낮음(VL)에서 매우 높음(VH)까지 5단계로 평가하며 각 단계가 의미하는 바는 〈표 6〉과 같다.

〈표 6〉 위험 수준의 평가 척도

질적 평가	설명
매우 높음(VH)	위협사건이 자산, 개인, 기관, 국가 등에 여러 심각하고도 재앙적 수준의 역효과를 불러올 수 있는 경우
높음(H)	위협사건이 자산, 개인, 기관, 국가 등에 심각한 또는 재앙적 수준의 역효과를 불러올 수 있는 경우

중간(M)	위협사건이 자산, 개인, 기관, 국가 등에 중요한 역효과를 불러올 수 있는 경우를 의미
낮음(L)	위협사건이 자산, 개인, 기관, 국가 등에 제한적 역효과를 불러올 수 있는 경우를 의미
매우 낮음(VL)	위협적 사건이 자산, 개인, 기관, 국가 등에 무시할 수 있는 수준의(negligible) 역효과를 불러올 수 있는 경우를 의미

※ 출처: NIST(2012).

실제 위협사건의 위험 수준 평가는 〈표 7〉에 제시된 바와 같이 NIST 등 타 기관에서 활용하는 위험 수준 평가 행렬표를 바탕으로 할 수 있으나, 신산업 분야의 경우 이전에는 존재하지 않았던 새로운 위협이 발생할 가능성이 있으므로, 전문가 조사를 통해 대상 분야 위협의 발생 가능성(1, 2, 3, 4, 5)과 영향도(A, B, C, D, E)를 결합한 위험조합(A1, A2,…, E4, E5)이 가지는 위험 수준을 직접 도출하여 평가 기준을 설정하는 것도 고려해 볼 수 있다.

〈표 7〉 위험 수준의 평가 기준(발생 가능성과 영향도의 조합)

발생 가능성	영향도				
	A	B	C	D	E
1	VL	VL	VL	L	L
2	VL	L	L	L	M
3	VL	L	M	M	H
4	VL	L	M	H	VH
5	VL	L	M	H	VH

출처: NIST(2012).

5) 관련 규제 파악 및 수준 정리

이 단계에서는 위협 시나리오의 위험에 대응하는 현행 규제를 파악하고 그 수준을 확인한다. 구체적으로 위협 시나리오의 위험에 대해 관련 규제가 존재하는지, 규제가 존재한다면 그 강도(약함, 보통, 강함)는 어떠한지, 그리고 위험 수준에 적절히 대응할 수 있는 강도의 규제인지 검토한다.

규제의 강도는 연구에 따라 다양하게 분류되나, 본 연구에서는 일반적으로 사용되는

분류 방법의 하나인 사전승인규제, 기준규제, 정보규제를 사용하였다(이종한, 2013: 106-107). 아래 〈표 8〉에서 확인할 수 있듯이, 사전승인규제는 개인·기업이 정부의 사전승인 없이 상품 혹은 서비스를 개발·판매·공급하는 것을 법적으로 금지하는 규제로 상대적으로 다른 규제방식에 비해 매우 높은 규제 부담을 피규제자에게 발생시킨다고 할 수 있다. 대표적인 유형으로는 허가, 인가, 면허, 특허, 승인, 지정, 추천, 동의 등이 있다(이종한, 2013: 106).

기준규제는 위험을 발생시킬 가능성이 있는 다양한 요인에 대해 이의 위험성을 감소시키거나 제거할 수 있도록 개인·기업의 행동기준을 구체적으로 제시하는 방식의 규제(투입기준규제)와 개인, 기업 등 규제대상 집단이 달성해야 할 목표치(행정의무)를 설정하고, 이의 충족을 강제하는 규제(산출기준규제)가 있다(최동진 외, 2013: 245-246). 투입기준규제의 대표적인 예로는 시험, 검사, 인정, 확인, 증명이 있고, 산출기준규제의 대표적인 예로는 결정, 명령, 지도, 단속, 고용의무, 기준설정 등이 있다(이종한, 2013: 106). 이러한 기준규제는 일정한 고정적 비용이 발생한다는 점에서 보통의 강도를 가진다고 할 수 있다.

마지막으로 정보규제는 개인, 기업 등 피규제집단이 다양한 활동 과정에서 획득·생성한 정보를 정부 등에 제출하도록 의무를 부과하는 규제로 위의 규제유형에 비해 적은 규제 부담을 발생시킨다는 점에서 가장 약한 형태의 규제라고 할 수 있다. 그 예로는 신고의무, 보고의무, 등록의무, 통지의무, 제출의무가 있다(이종한, 2013: 106).

〈표 8〉 규제의 강도별 분류

규제 유형	설명	대표적 규제 형식	강도
사전승인 규제	정부의 사전승인 없이 특정 행위를 하는 것을 법적으로 금지하는 것으로 가장 강한 형태의 규제	허가, 인가, 면허, 특허, 승인, 지정 등	강함
기준 규제	경제·사회활동 과정에서 충족시켜야 하는 기준을 설정하는 규제(투입기준),	시험, 검사, 인정, 확인, 금지, 증명 등	보통
	행정의무의 이행을 충족(산출기준)하기 위한 규제	결정, 명령, 지도, 단속, 조사, 고용의무, 기준설정 등	
정보 규제	경제·사회활동 과정에서 관련 정보를 정부 등에 제공하도록 의무를 부과하는 규제	신고, 보고, 등록, 통지, 제출 등	약함

출처: 이종한(2012: 8-10), 최동진 외(2013: 245-246)를 참고하여 저자 재구성

위협 시나리오의 위험 수준에 대응하는 적절한 규제수단은 위험 수준이 높아질수록 강도가 높은 규제가 적절하며, 위험 수준이 보통이면 강도가 중간인 규제가, 그리고 위험 수준이 낮은 경우에는 강도가 약한 규제나 규제가 없는 것이 적절하다고 할 수 있다. 이러한 기준을 바탕으로 위험 수준에 대응하는 적절한 규제의 강도를 도출하면 〈표 9〉와 같다.

〈표 9〉 시나리오별 위험 수준과 규제 강도에 따른 규제개선 전략

구분	위험 수준				
	매우 낮음(VL)	낮음(L)	보통(M)	높음(H)	매우 높음(VH)
적정 규제수준	규제 없음	정보규제	기준규제	기준규제	사전승인규제

6) 규제 개선책 제시

마지막으로 위협 시나리오의 위험 수준과 관련 규제의 강도를 조합하여 현행 규제의 적절성 여부를 확인하고 규제개선 방안을 제시한다. 구체적으로 시나리오 내 위협사건의 위험 수준이 매우 높음(VH)으로 평가된 경우에는 이러한 위험을 감소시키기 위해 강한 규제가 필요하며, 이에 따라 현행 규제의 강도가 약한 경우 이를 강하게 하는 규제개선전략을 제시할 수 있다. 위협사건의 위험 수준이 높음(V)이나 중간(M)이면 규제의 강도를 중간 정도로 유지하는 규제개선전략을 제시할 수 있으며, 낮음(L)인 경우에는 규제의 강도를 약함으로 유지하는 방안을 사용한다. 마지막으로, 위협사건의 위험 수준이 매우 낮음(VL)으로 평가된 때에는 규제를 없애는 개선전략을 제시할 수 있다. 이러한 규제개선전략을 정리하면 〈표 10〉과 같다.

만약 현행 규제의 강도가 평가된 위험 수준에 비추어 적정하다면, 규제를 그대로 유지하는 전략이 적절하지만, 그렇지 않다면 규제의 폐지, 완화, 신설 혹은 강화 전략을 제시하였다. 이는 위협 시나리오의 위험 수준이 높은 경우에 관련 규제가 없거나, 있다고 하더라도 규제의 강도가 충분히 강하지 않으면 위험 감소를 위한 규제 신설·강화가 이루어질 필요가 있지만, 위협 시나리오의 위험 수준이 낮은 경우에는 규제를 없애거나 완화하는 전략을 취하는 것이 적절하다는 것을 의미한다.

〈표 10〉 위협 시나리오의 위험 수준과 대응 규제의 강도에 따른 규제개선 전략

위험 수준	현행 관련 규제수준			
	없음	정보규제(약함)	기준규제(보통)	사전승인규제(강함)
VL	유지	폐지	폐지	폐지
L	신설	유지	완화	완화
M	신설	강화	유지	완화
H	신설	강화	유지	완화
VH	신설	강화	강화	유지

V. 결론 및 시사점

신산업은 기존에 경험하지 못했던 새로운 기술과 사업 방식을 통해 우리 경제의 활성화를 위한 성장엔진이 되리라 기대된다. 따라서 정부는 미래 자동차, 바이오 등 미래먹거리 산업육성을 위한 정책을 활발히 추진 중이다. 그러나 신산업에 담긴 새로움은 필연적으로 불확실성을 발생시키는데, 많은 경우 이러한 불확실성은 기존의 법과 제도로 대응이 불가능하다. 신산업에 따른 불확실성에 대응하기 위해, 특히 그것이 초래할 위험을 관리하기 위한 제도 정비가 필요한 시점이다. 그간 정부도 신기술·신산업의 육성과 국민의 생명·안전·환경 등 공익적 가치 사이의 균형을 꾀하고자 노력하였는데, 지난 2019년 도입된 '규제샌드박스'는 그러한 노력의 대표적 예이다.[5] 그러나 여전히 신산업·신기술이 발생시킬 수 있는 위험을 체계적으로 평가하고 그러한 평가의 결과를 규제설계에 도입하고자 하는 연구는 부족한 실정이다. 본 연구는 신산업 분야의 규제 합리화를 위한 위험평가 프레임워크의 적용 방안을 탐색하였다.

오늘날 4차 산업혁명은 인공지능, 로봇, 빅데이터, 사물인터넷, 블록체인 등 다양한 첨단기술이 CPS를 통해 상호 연결되어 융·복합적으로 활용되는 신기술·신산업의 등장으로 특징지을 수 있다. 이러한 4차 산업혁명의 발현은 산업의 부가가치 증대와 신산업·신서

5) 규제샌드박스에서는 ①국민의 생명·안전·환경 등에 끼치는 영향을 점검하여 우려가 있는 경우 규제 특례 부여를 제한, ②실증테스트 진행 과정을 지속적으로 점검하여, 문제가 예상되거나 발생할 경우 규제 특례 취소, ③책임보험 가입 의무화, 손해 발생 시 고의나 과실 없음을 사업자가 입증토록 하는 등 손해배상 책임 수준 강화의 이른바 '안전장치 3종 세트'를 통해 신사업이 발생시킬 수 있는 위험을 최소화하고자 한다.

비스 창출의 기회를 제공하고 있다. 한편, 4차 산업혁명의 가장 큰 특징인 기술·서비스·산업의 혁신적 융·복합 현상은 산업구조와 시장환경, 그리고 기업의 생산방식과 경영전략 등 시장 전반에 급격한 변화를 일으키고 있으며, 이에 적절히 대응하여 글로벌 경쟁력을 확보하기 위한 전략이 필요하다.

하지만 우리나라의 4차 산업혁명 관련 기술은 최고 기술 보유국에 비교하여 낮은 수준에 머물러 있으며, 국내 기업들 역시 현재 보유하고 있는 관련 원천기술 및 응용기술이 해외 주요기업과 비교하여 상당한 격차가 존재하여 세계 시장에서의 선도적인 역할을 하지 못하고 있다.

따라서 우리 정부는 4차 산업혁명을 선도할 주요 혁신성장동력을 지정하고 선제적·적극적인 발전 전략의 마련을 위해 힘쓰고 있으며, 학계에서도 관련 연구를 활발히 수행하고 있다. 특히 혁신성장을 견인하기 위한 규제개혁은 정부와 학계에서 높은 관심을 받고 있으며, 이미 다양한 전략이 추진되고 있다.

하지만 이러한 전략들은 몇 가지 한계점을 지닌 것으로 생각된다. 첫째, 현재 추진 중인 규제개혁 전략은 4차 산업혁명 관련 기술 분야를 중심으로 포괄적 네거티브 규제 등 최근 규제혁신 키워드로 주목받고 있는 규제전략에 집중하여 과학적 근거 없이 규제개선을 추진하고 있다. 즉, 규제개선 전략으로 단순히 네거티브 방식을 적용한 민원 해결성 규제 개선안을 제시하거나, 규제샌드박스의 적용을 추진하는 것이다.

둘째, 대부분 전략이 단기적인 일회성 규제개선만을 고려하고 있어 정부가 제시한 전략이 규제 이슈에 탄력적으로 대응하지 못하고 단기적 미봉책에 머무는 한계를 발생시킨다. 특정 기술·서비스 및 시장·산업의 발전을 위해서 규제개선은 단편적·일회적 활동이 아닌 반복적인 활동으로 진행되어야 하며, 정부는 전략의 추진에 있어 이를 고려해야 한다.

셋째, 현재 정부가 추진하는 대부분의 규제개선 전략은 제품·서비스의 특정 단계(예: 개발단계, 판매단계 등)에 초점을 맞추고 있으며, 제품·서비스가 향후 상용화되고 발전을 이뤄나가는 과정에서의 지속적인 규제개선 방안에 대한 고려가 부족하다.

따라서 본 연구에서는 이러한 한계점을 극복하기 위해 신산업 분야의 위협 시나리오를 도출하고, 이의 위험에 대해 과학적 분석을 시행하여 시나리오의 현실화에 따라 발생 가능한 위협의 위험 수준을 과학적으로 평가하는 방법을 제시하였다. 또한, 도출된 위험 수준을 현행 관련 규제의 강도와 비교하여 적절한 규제개선을 이루는 방안을 제안하였다.

특히, 본 연구는 기존의 혁신성장동력 및 4차 산업혁명 관련 규제전략 개발이 주로 민원해결성 정책에 초점을 맞춰 이뤄진 한계점을 인식하고, 향후 다양한 신기술·신산업의 규제개선을 위한 정책 개발에 활용할 수 있는 실증적 위험평가 및 규제개선을 위한 연구 및 분석 프레임워크를 마련·제시하고, 이를 활용하여 규제개선 방안을 도출하였다는 데 의의가 있다.

마지막으로 본 연구에서 제시한 위험평가는 기술 및 위험의 불확실성이 높은 다양한 융·복합 신산업·신기술 분야의 규제개선 방안 도출에 활용될 수 있다. 본 연구에서 수행한 방법을 적용하여 다양한 신산업·신기술 분야의 이슈에 관한 신문기사 등을 시나리오화하여 이에 대해 위험평가를 하고, 관련 규제의 강도를 확인하여 향후 규제가 어떤 방향으로 개선되어야 하는지를 확인할 수 있다. 또한, 본 연구와 같이 신산업·신기술 분야의 개별 정책 사안에 대해 위험평가를 하는 것뿐만 아니라 다양한 정책 사안의 위험 수준에 대한 상대적인 비교를 통해 규제 도입의 우선순위 결정이나 보다 조화로운 규제수단의 활용이 가능할 것으로 기대된다.

참고문헌

곽상록·홍선호·왕종배·조연옥. (2003). 확률론적 기법을 활용한 철도터널의 화재사고 시나리오의 구성. 철도저널, 7(4): 88-92.

김신. (2007). 위험분석에 기반한 규제정책의 활성화 방안. 한국행정연구원.

김현정. (2013). 식품안전관리를 위한 미생물 위해평가. 식품과학과 산업, 46(1): 26-35.

오윤희·남인식·김신도·김동술·박덕신·김지환·손종렬. (2013). 일부 지하철 역사내 실내공기 중 미세먼지에서의 중금속 노출에 의한 건강위해성평가. 한국생활환경학회지, 20(1): 29-36.

윤여홍·박교식·김태옥·신동민. (2015). 반도체 산업설비의 사고시 사업장외에 미치는 영향 평가. 한국위험물학회지, 3(1): 59-64.

이종한. (2013). 규제성과의 측정 및 활용에 관한 연구. 한국행정연구원.

최동진·김종성·정연주·손흥선·이연정. (2013). 좋은 규제로의 전환을 위한 환경규제 로드맵 연구. 국토환경연구소.

ACS. (2016). Chemical Risk Assessment and Regulatory Decision Making. Public Policy Statement.

EPA. (2020). History of Risk at EPA. Retrieved December 2, 2020, from https://www.epa.gov/risk/about-risk-assessment#tab-2

Macaulay, T. (2016). Riot Control: Understanding and Managing Risks and the Internet of Things. MA, Burlington: Morgan Kaufmann.

NIST. (2012). Information Security. NIST Special Publication 800-30 Revision 1.

NIST. (2015). Risk Management for Replication Devices NISTIR 8023.

OECD. (2002). Regulatory Policies in OECD Countries: From Interventionism to Regulatory Governance.

Journal of Regulation Studies Vol.29 No.2

An Exploratory Study on Risk Assessment for Rationalization of Regulations in the New Industry Sectors

Shim, Woo-Hyun & Park, Jung-Won[6)]

The regulatory policy of the Korean government in new industry sectors is a mixture of deregulation to revitalize the industry and reinforcing regulation to minimize damages and risks. The pursuit of the two-track policy is inevitable when simultaneously considering the 'potential of industrial development' and 'various uncertainties and risks in technology and services' of new industry sectors. The issue is how to determine an appropriate level of regulation between the revitalization of new industries and risk minimization. Between the two ends, this study examined the measures to implement a risk assessment framework for rational regulatory design. Specifically, this study applied and utilized the risk assessment method of the U.S. National Institute of Standards and Technology (NIST) to propose methods of risk identification and composition of risk scenarios. Moreover, regulations related to the work and scenarios of evaluating risk level by confirming the likelihood of threats and the influence thereof regarding scenarios were organized and presented, in addition to the methods of deriving appropriate regulatory

6) Corresponding author

measures via the analysis of risk level differences identified from scenario-related regulations and scenarios. In conclusion, this study discussed the limitations of various regulatory reform strategies being implemented by the government to lead innovative growth and the necessity of applying risk assessment frameworks and regulatory improvement in new industry sectors.

Keywords: risk assessment, regulatory design, scenario, regulation, new industry