연구
보고서

2021
07

금융산업의 디지털 전환과 운영리스크

- 은행과 보험산업 중심으로 -

정광민

KiRi 보험연구원

머리말

금융산업은 COVID-19의 위기 속에서 현재 급격한 디지털 전환의 파고를 경험하고 있다. 고객과의 접점을 확대하고, 고객경험 향상을 성취하기 위한 금융서비스의 디지털화뿐만 아니라 가치사슬의 전면적인 디지털 전환은 빅테크와의 경쟁관계가 형성되고 있는 금융산업 내에서 생존을 위한 필수적인 수단이 되고 있다.

이러한 전면적인 디지털 전환의 실행은 금융산업이 경험할 수 있는 디지털 사업환경 속 잠재적 리스크에 관한 불확실성이 존재한다. 전통적 리스크와 비교하여 동적이고, 그 원인을 정확히 파악하기 어렵기 때문에 금융기업 입장에서 리스크 관리 전략의 재고가 필요한 시점이다.

본 연구는 전통적 리스크 관리 프로세스 관점에서 디지털 운영리스크의 탐지 및 분석, 최적 관리 전략의 선택 문제를 고찰하고 있다. 특히, 금융산업의 전반적인 디지털 전환 양상을 개략적으로 제시하면서, 기존 운영리스크 분류체계를 보완할 수 있는 디지털 운영리스크 분류체계 제안 및 잠재적 손실유형 분석을 통한 디지털 운영리스크 관리방안의 시사점을 도출하고 있다. 본 보고서의 연구결과가 이머징 리스크로서의 디지털 운영리스크에 관한 이해 제고 및 금융산업 리스크 관리 제도 개선에 도움을 줄 수 있기를 바란다.

마지막으로 본 보고서의 내용은 연구자 개인의 의견이며 우리원의 공식적인 의견이 아님을 밝혀둔다.

2021년 11월

보험연구원 원장 **안 철 경**

목 차

표 차례

그림 차례

Abstract

Digital Transformations of the Financial Services Industry and Operational Risk: Banking and Insurance

This study examines how rising technologies apply to the financial business models amid the current digital transformation facing the financial services industry, and represents digital and cyber operational risk classification with a three-step approach. The study provides better understanding of potential risk scenarios by showing examples of digital and cyber operational loss events. It also investigates theoretical frameworks on how to control extreme digital and cyber risks, and proposes a risk map showing the levels of loss frequency and severity.

This study contributes to the discussion of operational risk management as follows: First, it can call the financial industry's attention to potential digital risks by providing the overall picture of how information technologies leading the digital transformation can apply to the value chain of banking and insurance industries. Second, it can help the industries develop an action plan to construct an enterprise digital risk management system by providing specific classification of digital risk. Third, it can be used as a benchmark for digital and cyber risk analytics by providing an analytical tool to estimate the risk impact with a large scale cyber risk dataset.

The current digital transformation of the financial industry is a structural phenomenon, where the value chain is significantly changing and a concern on the role of the industry is rising. Financial firms may be highly exposed to newly emerging risks without any solution or management strategies amid rapid digital transformation to survive in the market. In this regard, this study is in part useful to develop a framework to understand and mitigate such emerging risks.

요 약

본 보고서는 현재 금융산업이 경험하고 있는 디지털 전환(digital transformation)의 파고 속에서 금융 비즈니스 모델로의 정보기술 적용 양상을 살펴보고, 그 빈도와 심도가 점차 상승하고 있는 디지털 및 사이버 운영리스크를 3단계(대분류-소분류-리스크 요인) 분류체계를 통해 분석하였다. 디지털 및 사이버 운영리스크로 인한 손실사건의 사례를 통해 잠재적인 리스크 실현 시나리오에 관한 이해를 돕고 있으며, 리스크 관리 이론을 토대로 대규모 손실을 유발할 수 있는 디지털/사이버 리스크의 통제 방법에 대해 고찰하였다. 또한, 사이버 리스크 데이터를 기반으로 통계적 분석을 진행하여 리스크 유형에 따른 손실 빈도 및 심도 수준을 도식화할 수 있는 리스크 맵을 제안하였다.

본 연구는 금융산업의 운영리스크 관리 측면에서 다음과 같은 의의를 제공한다. 첫째로, 디지털 전환 시 활용 기술 및 금융 가치사슬(value chain) 적용 양상을 은행 및 보험산업 전반에 걸쳐 제공함으로써 향후 발생 가능한 잠재적 리스크 요인들에 대한 주의를 환기시킨다. 둘째, 바젤 Ⅱ의 운영리스크 분류체계와 연계하여 디지털 및 사이버 리스크 관련 기존 문헌들을 종합한 세부적 분류체계를 제안함으로써 전사적 디지털 리스크 관리체계 확립을 위한 시행계획(action plan) 구성의 기반을 제공할 수 있다. 셋째, 디지털 및 사이버 리스크와 관련한 대규모 데이터를 통해 해당 리스크의 잠재적 영향력을 추정할 수 있는 분석도구(analytical tool)를 제안함으로써, 계량적 방식을 통한 디지털 및 사이버 리스크 수준 분석의 참조점을 제공할 수 있다.

현 디지털 전환은 금융산업의 가치사슬을 전반적으로 변화시키고, 금융산업의 역할을 근본적으로 고민하게 만드는 구조적 현상이다. 금융기업들은 디지털 전환의 파도를 피할 수 없는 상황에서 급격한 변화에 휩쓸려 대안과 관리대책이 마련되지 않은 채 새로운 유형의 이머징 리스크(emerging risk)에 무방비 상태로 노출될 수 있다. 본 보고서는 이러한 금융기업들의 우려를 일부나마 해소할 수 있는 방안을 마련하는 데 도움이 될 것으로 기대한다.

I 서론

1. 연구 배경 및 목적

2020년 1월 이후 지난 2년여의 시간은 가히 위험사회, 위험세계로 기억될 만큼 일상에서의 위험이 개개인의 인식 속으로 깊이 자리 잡은 기간이었다. COVID-19 팬데믹(pandemic)이 우리 일상의 평범한 환경을 극도의 위험회피적 환경으로 심각하게 바꿔놓았음은 누구도 부정하지 않을 것이다. 사람들은 마스크 없이 사회 속에서 노출되는 것을 회피하게 되었고, 사회적 관계 형성과 일상의 업무에서 과거에는 고려하지 않았던 전염위험(contagion risk)을 가장 먼저 우려해야 하는 생활방식 속에 살아가게 되었다. 이러한 전염위험으로부터 노출을 최대한 피하기 위해 비대면 방식의 업무 환경이 짧은 기간 가속화되었다. 체계화되지 않은 비대면 업무 문화가 급작스럽게 요구되면서 COVID-19 팬데믹 초기 어느 정도의 사회적 혼란이 발생하였으나 금세 새로운 환경에 적응하게 되었고, 이제는 비대면 방식의 경제활동이 대면 방식과 혼재되어 자연스러운 일상으로 인식되고 있다.

금융산업에서는 2020년 이전부터 비대면 방식의 금융서비스, 보험계약절차 등을 제공하기 위해 사업 운영에서의 변화를 추구해왔고, 많은 기업이 실제 그러한 방식으로 금융 서비스를 제공하고 있다. 금융산업의 디지털 전환(digital transformation)이라고 부르는 온라인 사업환경으로의 진입은 2020년 이후 위험사회를 거치면서 거부할 수 없는 현실로서 모든 금융 관련 기업이 경험하고 있다. 문제는 전반적인 기업운영에서의 디지털 전환이 이루어짐에 따라 효율성과 생산성은 증가하였지만, 이로 인해 파생될 수 있는 새로운 위험(이머징 리스크: emerging risk)에 대한 인지와 대처는 여전히 미숙하다는 점이다.

여기서 주목할 개념은 바로 이머징 리스크(emerging risk)이다. 이머징 리스크는 일반적으로 과거에는 인식하지 못했거나 관심이 높지 않았으나, 주목받기 시작한 리스크 유형을 통칭한다.[1] Flage and Aven(2015)은 이머징 리스크를 다음과 같은 4가지 개념으로 정의하였다.

1) 영국의 로이즈(Lloyd's)는 이머징 리스크를 "완전하게 이해할 수 없지만 잠재적으로 심각한 위협이 되는 리스크"라고 정의하고 있으며, 스코르재보험(Scor Re)은 "정량적 평가 및 미래 손실 예측이 힘든, 매우 큰 불확실성"이라고 정의함. 스위스에 기반을 둔 세계경제포럼(World Economic Forum)은 매년 글로벌 이머징 리스크 순위를 평가하여 기

1. 새롭게 생성된 리스크(newly created risk)

2. 새롭게 인지된 리스크(newly identified/noticed risk)

3. (위협이) 증가하는 리스크(increasing risk)

4. 널리 알려지고, 점차 확고해지는 리스크(risk becoming widely known or established)

Flage and Aven(2015)은 이머징 리스크 개념에 관해 체계적인 분석을 진행하였는데, 이 리스크를 설명하기 위한 핵심으로 지식(knowledge)의 정도에 주목하였다. 이머징 리스크의 본질에는 약한 또는 부족한 지식(weak knowledge)이 존재한다. 부족한 지식은 이머징 리스크로 인해 특정 사건에 관한 징조가 발생할 수 있음에 대한 인식은 가능케 하지만, 그로 인한 결과와 구체적인 양상은 전혀 알지 못한다고 설명할 수 있다. 결국 이머징 리스크는 '알려진 무지(known unknown)'[2]라는 개념으로 설명될 수 있는데, '무지'의 개념은 정보의 양(또는 수준)에 따라 상대적으로 다르게 인식될 수 있으므로 이머징 리스크는 상대적인 개념이 될 수 있다. 즉, 정보의 양이 증가할수록 이머징 리스크에 대한 이해도도 자연스럽게 증가하기 때문에 누군가에게는 정보의 양이 충분해지는 특정 시점에 기성 리스크로 편입될 수 있다. Flage and Aven(2015)의 관점과 다르게 International Risk Governance Council(2011)[3]은 이머징 리스크를 아래와 같은 세 가지 유형으로 분류하였다.

1. 과학기술의 발달로부터 기인하는 불확실성을 내포하는 리스크(Risks with uncertain impacts, with uncertainty resulting from advancing science and technological innovation)

2. 기술적인 시스템 발전에 따라 증가하는 네트워크 상호의존성에 의해서 발생할 수 있는 시스템 리스크(Risks with systemic impacts, stemming from technological systems with multiple interactions and systemic dependencies)

3. 진화하는 환경에서 기존 기술의 사용으로 인해 예상치 못한 손실이 발생할 수 있는 리스크(Risks with unexpected impacts, where new risks emerge from the use of es-

---

업의 영업 및 국가 운영 환경에서 직면할 수 있는 가장 위협적인 리스크들을 판단하고 관리할 수 있도록 돕고 있음

2) 알려진 무지(known unknown)는 단편적으로 우리가 모르는 것이 있다는 것을 안다는 개념을 가리킴. 전 미국국방장관 도널드 럼스펠트(Donald H. Rumsfeld)가 2002년 2월 이라크 정부와 테러리스트들 간 연관성이 있는지 여부에 대한 기자회견 질문의 답으로 이 개념을 사용하면서 회자되기 시작하였음

3) 이하 IRGC(2011)로 기술함

tablished technologies in evolving environments or contexts)

관련 참고문헌들을 종합해보면, 이머징 리스크는 전통적 관점에서의 리스크(classical risk)와 비교했을 때 정의와 분류가 모호하고(부족한 지식), 통제 및 전가에 대한 의사결정을 위해 필요한 데이터가 불충분하다는 특징을 가진다(〈표 Ⅰ-1〉 참조). 정의, 분류의 모호성과 데이터의 부족 문제로 인해 이러한 리스크에 대한 이해가 불충분해지고, 이로 인한 손실을 모형화하여 향후 발생 가능한 손실 수준을 추정하는 방법의 발전 속도가 늦어지게 되어 시장이 해당 리스크를 거래할 수 있는 여건을 제공하지 못하는 상황이 발생하게 된다.

〈표 Ⅰ-1〉 전통적 리스크와 이머징 리스크 비교

구분	정의의 명확성	분류의 명확성	데이터 가용성	분석모형	부보 가능성
전통적 리스크 (classical risk)	○	○	○	○	○
이머징 리스크 (emerging risk)	×	×	×	△	△

주: ○는 해당 기준을 만족함, △는 일부 만족하지 않는 요인이 존재함, ×는 만족하지 않음을 의미함

금융산업이 디지털 전환의 파고 속에서 경험하게 되는 이머징 리스크로는 디지털화 된 시스템과 프로세스를 통해서 발생할 수 있는 디지털 운영리스크(digital operational risk), 기업 내·외부에서 연결되어 있는 네트워크상 발생할 수 있는 사이버 리스크(cyber risk) 등이 대표적이다.[4] 이러한 리스크들은 IRGC(2011)에서 분류한 이머징 리스크 유형과 일관된다. 기존 연구는 정보기술 발달에 따른 새로운 형태의 리스크를 일반적인 운영리스크의 범주로 정의(Ⅰ-2장 선행연구 참조)함으로써 이를 관리하기 위한 기업의 전략 및 행동방안을 제시해왔다. 하지만 기존 금융기관의 운영리스크는 국제결제은행(BIS)의 바젤 Ⅱ(Basel Ⅱ)에서 규정한 리스크 분류(〈표 Ⅰ-2〉 참조)하에서 디지털 전환으로 인한 리스크 동인에 대한 포괄성이 제한적이며, 산업환경의 변화를 반영하지 못한다는 점에서 한계가 존재한다.

4) 본 보고서에서는 디지털 전환 시대 금융산업에 경험하는 이머징 리스크를 디지털 운영리스크로 통칭하여 사용함. 디지털 운영리스크라는 표현은 현재 운영리스크와 관련한 학술적 측면에서 일반적으로 통용되는 용어는 아니지만 사이버 리스크 및 기타 디지털 전환으로 발생 가능한 운영리스크를 포괄할 수 있는 개념으로서 활용 가능하다고 판단됨

〈표 Ⅰ-2〉 Basel Ⅱ/Solvency Ⅱ의 운영리스크 분류

외부사취	외부 절도 및 사기	내부자의 도움 없이 의도적으로 행한 사취(악의적 피해는 제외)
	시스템 보안	외부자가 이익을 얻기 위해 전산자료에 권한없이 접근(악의적 피해 제외)
내부사취	내부 절도 및 사기	내부자가 개입된, 의도적으로 행한 사취
	권한없는 행위	고의적 미보고, 권한없이 행한 거래, 고의적 포지션 오류표기 등의 내부자 실패
	시스템 보안	이익을 목적으로 또는 회사에 손해를 끼칠 목적으로 전산자료에 권한없이 접근
고용 관행 및 사업장 안전	고용관계	해고 절차 중 발생하는 특정 실수 혹은 금지행위 또는 노사분규로 인해 발생하는 사건
	사업장 안전	강제 고용보험 및 사업장 안전규제와 관련
	평등 및 차별	노사 관련 법 또는 회사 내규에서 정한 사업장 내 평등 및 차별에 관한 사건
	인적 자원 관리	부적절한 인력관리로 인한 사건
고객, 상품 및 영업 관행	적합성, 공시 및 신의성실 의무	규정 위반 또는 고객/의뢰인/협력업체에게 영향을 주는 불이행으로 인한 사건
	부적절한 업무 관행	부적절한 업무처리로 간주될 수 있는 관행으로 인한 사건
	상품 결함	부적절한 상품 설계 또는 부적절한 가격 설정으로 인한 사건
	거래상대방	판매채널 등 제3자 행동으로 인한 사건
	후원 익스포져	계획되지 않은 비용으로 인한 사건
	선택	내부 지침에 따른 고객조사를 제대로 하지 못해 발생하는 사건
	자문 활동	의무 이행의 실패로 인한 사건
유형자산 손실		자연재해/산업재해, 악의적 피해로 인한 사건
영업중단 및 시스템 장애	시스템 장애	시스템 또는 인프라 장애로 인한 사건
	운송 및 기타 장애	회사에 손해를 입히는 운송 장애 및 기타 장애로 인한 사건

〈표 Ⅰ-2〉 계속

집행, 전달 및 절차의 관리	거래의 포착, 실행 및 유지	정보수집 및 문서화 실패로 인한 사건
	고객 계좌 관리	고객기록 및 상환기록의 부정확성으로 인한 사건
	모니터링과 보고	의무적인 내·외부 보고의 부정확성으로 인한 사건
	공급업체와 아웃소싱	벤더 또는 서비스 공급업체의 서비스 제공 실패 또는 분쟁으로 인한 사건
	계약과정상의 고객 문서	신계약 체결 시 부족한 또는 부적합한 데이터 입수로 인한 사건

자료: 보험개발원(2017)의 〈표 26.1〉을 재구성함

구체적으로 한계점은 다음과 같다. 현 바젤하 리스크 관리체계는 운영리스크 측정방법에 있어 질적 및 양적 기준을 요구하는데, 질적 기준의 경우 리스크의 효율적 통제를 위한 지배구조 및 리스크 관리 프로세스의 확립이 있다(선우석호·전은영 2006). 양적 기준의 경우 8개의 사업부문과 7개의 손실사건하에서 각 셀(cell)별 손실분포를 추정하여 필요자본 규모 산출을 요구한다(선우석호·전은영 2006). 문제는 양적 기준하에서 규정된 7개의 손실사건을 유발하는 원인이 4가지의 개괄적인 요소(내부절차, 내부인력, 내부시스템, 외부사건)로만 규정되어 있고, 손실을 실제 유발하는 구체적인 동인(또는 원인)을 이해하기 위한 하위 분류는 존재하지 않는다. 리스크의 결과로서 20가지 정도로 분류된 손실사건의 하위유형이 사건의 동인와 관련된 근거를 제공한다.

이러한 문제는 잠재적 손실에 대비하기 위한 자기자본량 추정에 초점이 맞춰진 소위 사후손실(post-loss) 관리 중심의 체계하에서 발생한다. 이에 따라 운영리스크 관리의 질적 체계상 리스크 탐지 및 평가도 이러한 사후 손실 관리체계에서의 단순 손실 원인 분류 및 손실사건 유형에 맞춰 이루어질 수밖에 없다. 현재의 디지털 전환에 따른 리스크 환경의 불확실성에 대비하기 위해서는 사후 손실 관리 중심의 체계를 개선하여 좀 더 구체적인 손실 유발 요인들을 탐지·분류하고, 이를 금융산업의 전반적인 비즈니스 환경에 적용하여 선제적인 사전 손실(pre-loss) 관리체계로 변화할 필요가 있다.

이러한 한계를 일부 극복하기 위하여, 본 보고서는 바젤 Ⅱ의 운영리스크 분류의 기본 골격 및 기존 연구결과들을 기반으로 디지털 운영리스크 요인을 포괄할 수 있는 분류체계를 제안하는 데 그 목적을 둔다. 또한, 잠재적인 손실사건에 관한 사례 분석과 함께 디지털

리스크 관리방안을 고찰함으로써 금융기관이 디지털 전환을 통해 금융서비스의 질적 향상뿐만 아니라 기업가치를 효율적으로 증가시킬 수 있는 리스크 관리체계까지 갖춰나갈 수 있는 틀을 제공하고자 한다.

2. 선행연구

디지털 운영리스크에 대한 정확한 용어정리와 분류체계를 연구한 문헌은 현재까지 많지 않다. 특히, 디지털 운영리스크라는 포괄적 개념보다는 사이버 리스크를 운영리스크의 일부로 정의하여 디지털화, 사이버 경제활동 등을 통한 리스크를 포괄하여 분석하는 경향이 있다. 디지털/사이버 운영리스크 관련 참고자료는 크게 학술연구와 산업리포트로 구분할 수 있다. 이 중 학술연구의 경우 컴퓨터과학(또는 공학), 경제학, 재무학, 보험학, 보험계리학 등의 다양한 영역에서 사이버 리스크라는 주제로 연구가 이루어지고 있다. 컴퓨터과학(공학) 분야에서는 공격자의 침투 프로세스 및 리스크 발생확률에 대한 수리적, 통계적 모델링을 주로 연구하고 있다(예를 들어, Schroeder and Gibson 2009; Mukhopadhyay et al. 2013). 경제학 또는 재무학 관점에서는 사이버 리스크의 잠재적 피해 기업의 보안시스템에 대한 최적 투자수준을 결정하는 문제를 다루고 있는 Gordon and Loeb(2002)의 모형을 중심으로 관련 연구가 이어지고 있다. 또한, 기업의 재무상태, 보안수준 등을 분석하여 어떤 기업이 사이버 공격 피해에 상대적으로 더 많이 노출되어 있는지 관한 연구(Kamiya et al. 2021)도 있다.

보험학 또는 보험계리학 영역에서 이루어지는 연구에는 주로 사회 및 산업 부문에 대규모 영향(극단적, 시스템적 영향)을 가져올 수 있는 디지털/사이버 리스크에 관한 연구에 초점이 맞춰져 있다. 디지털/사이버 리스크에 관한 보험시장의 활성화를 위해 부보 가능성을 평가하거나(Biener, Eling and Wirfs 2015), 디지털/사이버 운영리스크로 인한 극단적 손실을 설명할 수 있는 모형을 제안(Eling and Wirfs 2019)하는 연구가 있다. 사이버보험 시장의 공급 측면 연구로서, 리스크 요인 간 의존관계를 고려하여 예상 보험료를 추정한 연구(Eling and Jung 2018)나 데이터 유출 건수의 재정적 영향을 분석하여 보험가능액을 추정할 수 있는 모형을 제안한 연구(Jung 2021)도 존재한다.

본 보고서에서는 이러한 여러 분야의 연구 중 운영리스크 관점에서의 학술연구와 산업보

고서 중심으로 살펴보고자 한다. 우선, Bharadwaj et al.(2009)은 IT시스템상 장애가 발생하면 전체적인 기업 가치에 부정적인 영향을 끼친다는 것을 실증적으로 분석하였다. 운영리스크의 일부로서 사이버 리스크가 유발한 IT시스템 장애는 평균 2%의 비정상적인(abnormal) 주가 하락을 초래했다. 특히, IT 장애의 심도 크기가 클수록 더 큰 주가 하락이 초래되고, 과거에 IT장애 이력이 있는 기업일수록 사건이 발생했을 때 더 크게 하락함을 보였다. 이 결과를 바탕으로 Bharadwaj et al.(2009)은 투자자가 투자 결정 시 기업의 시스템 운영 능력을 고려하며, 따라서 기업이 사이버 보안에 더 관심을 가져야 한다고 주장한다.

Pate-Cornell et al.(2018)은 국가 기반 시설(인프라 시설)에 사이버 공격이 발생할 수 있는 시나리오를 가정하여 예상 결과를 분석하였다. 사이버 공격의 목표가 될 수 있는 국가 기반 시설로는 전력망, 항만, 항공 교통 통제 및 국가 경제에 필수적인 인프라 시설로 한정하고 있으며, 만약 사이버 공격이 GPS에 심각한 영향을 미친다면 통신, 금융, 운송 등 많은 분야에서 상당한 규모의 손실을 유발할 것으로 예측하고 있다. 특히, 2016년 우크라이나 전력발전소를 목표로 한 사이버 공격 사례를 통해, 국가 주도의 사이버 보안 대응책이 존재하더라도 해당 공격으로 인해 1시간 이상 수도 키예프 지역의 정전이 발생한 것은 민관협력 대응책이 필요함을 시사한다고 주장한다.

Eling and Wirfs(2019)는 가장 큰 운영리스크 손실 데이터베이스 중 하나인 SAS OpRisk 자료를 활용하여 전 세계 사이버 운영리스크 손실 사건들을 분류하여 통계적으로 분석하였다. 이를 통해 사이버 운영리스크과 일반 운영리스크의 손실액 통계량을 비교하였으며, 사이버 운영리스크 손실사건이 크게 일상 속의 사이버 운영리스크(cyber risks of daily life)와 극단적 형태의 사이버 운영리스크(extreme cyber risks)로 구분하였다. 데이터 유출 손실자료 중심으로 로그정규분포(log-normal distribution)를 따르는 손실 심도를 분석한 기존 연구들과 다르게 실제 운영리스크 손실자료로부터 분류한 사이버 리스크 손실 심도는 일반화된 파레토 분포(generalized Pareto distribution)가 더 적합함을 확인하였다. 해당 연구는 특히 사이버 운영리스크 손실사건이 주로 인적 위험으로 인해 발생한다는 것을 확인하였다.

Aldasoro et al.(2020)은 2008년 금융위기 이후 급증했던 금융산업의 운영리스크 손실액이 최근 들어 감소하는 추세를 띄고 있음을 확인하였는데, 이는 금융위기 이후 대형은행의 부적절한 영업 관행을 통제한 노력의 결과로 해석할 수 있다. 반면, 운영리스크의 한

종류인 사이버 리스크 손실사건은 일반 운영리스크에 비해 상대적으로 적은 빈도로 발생하지만 최근 들어 심도가 증가하고 있음을 보였다. 운영 리스크 전체 빈도 측면에서는 적은 비중을 차지하지만, 전체 손실액 대비 1/3이 사이버 리스크에 의해서 발생한다는 것을 확인하였다. 이는 금융산업의 전체적인 비즈니스 프로세스 및 서비스 측면에서의 디지털화와 연결하여 운영리스크 분류 하 디지털/사이버 리스크의 비중이 향후 더욱 증가할 수 있음을 시사한다.

Eisenbach et al.(2020)은 상호연결성(interconnectedness)이 강한 금융산업 내 대형 은행의 결제 시스템을 목표로 한 사이버 공격이 발생시킬 수 있는 파급 효과(spillover effect)를 분석하였다. 해당 연구에 따르면 미국 내 네트워크가 가장 큰 5개 대형 은행 중 한 곳의 결제 시스템이 사이버 공격으로 인해 하루 동안 마비되었을 때, 평균적으로 미국 전체 은행의 38%의 자산이 영향을 받을 것으로 예측하였다. 또한, 사이버 공격의 특징으로 공격자가 취득한 정보의 수준에 따라서 공격에서 발생하는 시스템 리스크(systemic risk)의 규모가 결정될 수 있다고 주장한다. 예를 들어, 지급 활동이 증가하는 특정 요일에 발생하는 공격은 다른 요일에 비해 더 심각한 손실을 유발하며, 평균적으로 11% 더 큰 파급력을 보인다는 것을 확인하였다.

Lloyd's(2018)는 클라우드 컴퓨팅 서비스 공급자에게 사이버 공격이 발생했을 경우 예상되는 손실에 관해 분석하였다. 해당 연구는 클라우드 서비스 장애로 인해 손실을 입은 미국 기업과 Fortune 선정 기업들을 중심으로 e-비즈니스 중단 비용에 대한 추정치를 제공한다. 본 연구는 제조업과 도소매업이 클라우드 서비스 장애로 인해 가장 큰 영향을 받는다는 것을 보였으며, 제조업의 경우 최소 42억 달러에서 최대 86억 달러, 도소매업은 최소 14억에서 최대 36억 달러의 잠재적 손실에 노출되어 있음을 보였다. 특히, 추정된 손실의 규모는 피해 클라우드 서비스를 사용하는 기업의 수와 클라우드 장애 지속시간에 따라 달라지며, 대기업에 비해 소규모 기업의 클라우드 서비스 사용 비율이 높아 공격에 더 노출되어 있음을 분석하였다. 클라우도 서비스 의존성이 높음에도 불구하고 소규모 기업들의 사이버보험 가입률은 상대적으로 낮아, 사이버보험 상품 내 리스크 분포의 모니터링 강화를 제공함으로써 시장 확대가 필요함을 주장한다.

본 보고서는 앞서 기술한 선행연구의 흐름을 참고하여 금융산업의 디지털/사이버 운영리스크 유형 분류, 손실의 빈도/심도에 따른 리스크 관리 전략, 실증자료를 통한 특정 디지털/사이버 리스크의 분석도구 등을 제안한다.

3. 연구 내용 및 구성

본 보고서는 다음과 같이 구성되어 있다. 먼저, Ⅰ장 서론에서 정의한 이머징 리스크로서의 디지털 운영리스크를 바탕으로 Ⅱ장에서는 현재 금융산업이 경험하고 있는 디지털 전환의 양상을 개괄적으로 보여준다, 금융산업을 은행과 보험회사로 분류하여 각 금융서비스 생산자의 프론트, 미들, 백오피스에서 이루어지고 있는 디지털화를 사례 중심으로 보여준다.

Ⅲ장에서는 디지털 운영리스크를 바젤 Ⅱ의 기본 분류체계를 기반으로 리스크 요인(동인)까지 세분화하여 분류한다. 분류체계는 기본적으로 가장 포괄적 유형의 리스크 대분류(Risk core category), 대분류별 세분화된 리스크 소분류(Risk sub-category)와 소분류별 리스크를 유발시킬 수 있는 요인들(Risk factor)로 구성되어 있다. 이를 바탕으로 Ⅱ장에서 논의한 은행 및 보험사의 디지털 전환 사례와 운영리스크 요인을 매핑하였으며, 바젤의 분류체계 매핑 결과와 비교 분석하였다.

Ⅳ장에서는 Ⅲ장에서 분류된 리스크 요인들을 기반으로 잠재적 손실 빈도와 심도에 따른 네 가지 유형(저빈도-저심도, 고빈도-저심도, 저빈도-고심도, 고빈도-고심도) 중 금융기업 및 보험사의 관리 초점이 맞춰진 저빈도-고심도, 고빈도-고심도 유형 사례들을 분석한다. 이와 함께 각 유형에 해당하는 리스크를 관리하기 위한 전략을 이론적으로 고찰하고, 현실적인 방안에 대해서 논의한다.

Ⅴ장에서는 디지털 운영리스크로 인해 발생한 손실 정보를 담고 있는 실증 데이터를 금융기업과 비금융기업으로 구분하여 통계적 방법을 통해 분석하고, 금융기업이 직면할 수 있는 미래의 디지털/사이버 운영리스크 손실 빈도 및 심도 수준을 평가한다. 바젤 Ⅱ에서 허용하고, 다수의 금융기관이 적용하고 있는 손실분포접근법(Loss Distribution Approach; LDA)[5]을 기반으로 손실 빈도와 심도에 대한 분포 추정을 진행하며, 해당 결과를 바탕으로 잠재적 디지털/사이버 운영리스크를 평가하는 리스크 매트릭스(또는 리스크 맵)의 구성을 논의한다.

---

5) 손실분포접근법은 2016년 개정된 바젤 Ⅱ 운영리스크 규정에서는 더 이상 허용되지 않고, 표준측정접근법(Standardized Measurement Approach)으로 대체되었으나, 이에 대한 학술적 논쟁이 여전히 존재함. Dionne(2019)는 새롭게 요구되는 표준측정접근법이 운영리스크 측정의 유연성을 제한함으로써 개별 은행의 위험환경 및 특수성을 고려하지 못한다고 주장하였음. 이에 더하여, 표준측정접근법의 안정성(stability) 또는 견고성(robustness)이 아직 증명되지 않았으며, 운영리스크를 관리하기 위한 인센티브가 감소할 수 있음을 지적하였음

마지막으로 Ⅵ장에서는 본 보고서에서 기술한 내용을 바탕으로 효과적인 리스크 관리 전략 중 보험이 가지는 역할을 논하기 위해 디지털/사이버 리스크의 부보 가능성 분석과 민관협력 방안에 관해서 기술한다. 이와 함께 국내 금융산업이 갖춰야 할 디지털 운영리스크 관리체계, 나아가 전사적 디지털 리스크 관리체계 구축의 필요성을 강조한다.

Ⅱ 금융산업의 디지털 전환 양상

1. 개요: 핀테크의 정의와 금융산업의 환경변화

금융산업의 디지털 전환을 논의하기 전에 우선 금융산업 내 디지털 혁명을 가속화하는 핀테크(FinTech)에 대한 정의가 필요하다. 금융안정위원회(Financial Stability Board)[6]는 핀테크를 '금융시장과 기관, 금융서비스 제공에 있어 상당한 영향을 끼칠 수 있는 새로운 사업모형, 응용, 과정, 상품을 이끄는 실용적이고 획기적인 금융 기술'로서 정의한다.[7] 이러한 정의에 따르면 핀테크는 최근에서야 주목받는 기술이 아닌 과거에도 존재했던 금융산업 내 새로운 기술적 패러다임으로서의 역할을 해왔다고 볼 수 있다. Stulz(2019)는 1960년대 은행들이 ATM 기계를 도입하고 컴퓨터를 광범위하게 활용하기 시작한 시기를 핀테크의 황금기로 지칭하였다. 1992년에는 Merton Miller가 1960년대 금융계의 변혁을 '전자컴퓨터 활용을 통한 정보 혁명이 이끈 혁신적인 움직임'으로 정의하면서 그 당시까지 전혀 보지 못한 혁신적 사건이었음을 인정하였다(Stulz 2019). 핀테크는 금융산업 내 기술적 발전과 함께 과거에도 관찰된 산업 활동의 결과물이라고 할 수 있다.

그러한 맥락에서 우리가 목격하고 있는 현 시점의 핀테크 혁명은 과거로부터 누적된 기술발전과 함께 꾸준히 진행되어 온 현상이라고 생각할 수 있다. 무어의 법칙(Moore's Law)으로 대변되는 정보기술의 발전은 방대한 데이터의 축적과 고급화된 모형의 발달을 이끌게 되고, 이는 1960년대에 발생한 핀테크 혁명으로부터 금융시스템과 시장에서의 효율성 제고, 시장 확대 등의 목표하에서 실용적 디지털 기술과 빅데이터 분석을 기초로 한 새로운 전환으로 이어지게 되었다.

특히, 이러한 혁신적 전환이 소위 금융 혁명이라고 불릴 만큼 시대적 변화를 가져오게 된 계기로서 비대면 업무환경과 비대면 서비스 발전을 통한 고객 경험(customer experi-

6) 금융안정위원회는 1999년 설립되었던 G7 국가 중심의 금융안정포럼(Financial Stability Forum)이 확대·개편된 G20 수준의 국제 금융 감독 업무를 담당하는 조직임. 우리나라 금융위원회를 포함한 16개국의 위원회와 IMF, BIS 등의 국제기준 설정기구 10곳이 참여하여 총 24명의 운영위원회가 구성되어 있음

7) Financial Stability Board(2017)를 참조함

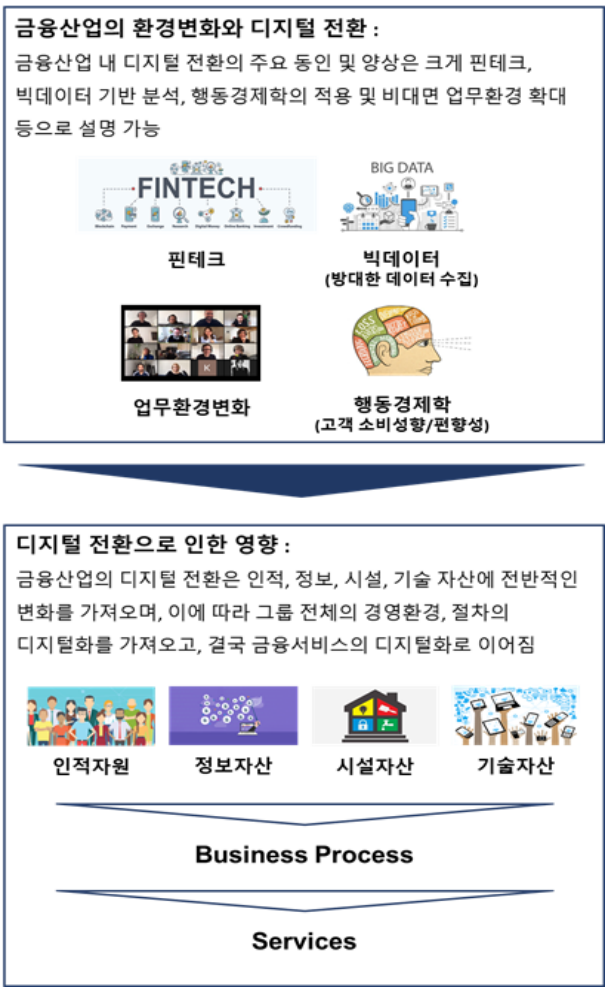
ence/customer journey)의 변화도 빼놓을 수 없다(〈그림 Ⅱ-1〉 참조). COVID-19으로 인해 기업 내·외부 네트워크 환경하 비대면 업무가 빠르게 일상화 되었고, 스마트폰, 사물인터넷 등을 활용한 금융서비스의 활성화 및 가상현실/증강현실(Virtual Reality/Augmented Reality; VR/AR), 메타버스(Metaverse) 등의 신기술로 인해 편의 중심의 긍정적 고객 경험이 증가하면서 경쟁적으로 최신 기술을 적용하고자 하는 시장 환경이 만들어지게 되었다.[8)]

디지털 전환을 통한 혁명적 변화는 금융산업 내 인적자원, 정보자산, 시설자산 및 기술자산에 이르기까지 경영환경 전반에 영향을 끼치고 있다(〈그림 Ⅱ-1〉 참조). 사업부문 전반에서 디지털화에 대한 기업 내 인적자원의 높은 이해가 요구되고, 시장에서의 변화양상을 꾸준히 모니터링하면서 신속하게 적용할 수 있는 능력이 점점 더 요구되고 있다. 또한 금융산업 내 디지털 전환은 마이데이터, 데이터 3법 등의 법제화와 함께 확대된 정보자산, 디지털 연결성이 확보된 시설자산, 블록체인 등 고급화된 기술자산 등을 통해 사업 프로세스 전반의 디지털화로 이어지고, 과거에는 시장화되지 못했거나, 새로운 형태의 금융서비스로 확대되는 효과로 이어지게 되었다.

이 장은 금융산업 중 은행과 보험산업 중심으로 디지털 전환 양상이 어떻게 나타나고 있는지 요약한다. 먼저, 금융산업의 최근 디지털 전환 간에 활용되는 기술의 종류와 그 의미에 관해 간략하게 살펴본다. 이를 바탕으로 은행 및 보험산업의 가치사슬과 기능 측면에서의 디지털 전환 양상을 살펴본다. 은행의 세 가지 기능으로서 프론트 오피스(front office), 미들 오피스(middle office), 백 오피스(back office)별 디지털 전환 양상에 대해 요약한다. 보험산업과 관련해서는 먼저 인슈어테크를 소개하고, 크게 생명 및 손해보험의 가치사슬 구조상 디지털화 양상에 대해 간략히 기술한다. 이 장에서 기술할 금융산업 내 디지털 전환 양상은 빠르게 발전하고 실용화되고 있는 가장 최신 기술들까지 포괄하고 있지 않을 수 있으나, 전반적인 핀테크 및 인슈어테크 환경에 대한 이해와 금융산업이 직면한 이머징 리스크 요인 분류를 돕는다는 점에서 참고가 될 것으로 기대한다.

8) 고객 경험의 변화는 소위 경험 경제로 대표되는 디지털 경제 시대에서 기업이 상품의 시장성을 높이기 위해 분석하고 이해해야 할 가장 중요한 요인 중 하나가 되었음. 이를 분석하기 위한 방법으로 행동경제학(Behavioral economics) 분야에서 주로 활용되는 휴리스틱(heuristics, 또는 발견법)이 있으며, 이를 활용하여 고객이 상품 또는 서비스를 경험하면서 어떤 소비 여정을 겪는지 분석 가능함

〈그림 Ⅱ-1〉 금융산업의 환경변화와 디지털 전환의 영향



2. 금융산업 디지털 전환 시 주요 활용 기술[9)]

금융산업의 디지털 전환과 관련하여 가장 많이 언급되는 용어 중 하나는 빅데이터(big data)이다. 빅데이터는 말 그대로 과거의 데이터베이스 관리 도구 능력을 넘어서는 대규모의 데

9) 주요 활용 기술에 관한 요약은 〈표 Ⅱ-1〉을 참조 바람

이터 크기를 의미한다(De Mauro, Greco and Grimaldi 2016). 빅데이터의 대표적인 3V(Volume, Velocity, Variety) 특징으로는 폭발적인 증가를 의미하는 Volume, 시간에 따라 빠른 속도로 변화한다는 의미를 지닌 Velocity, 데이터 구조와 형태가 다양하다는 의미를 지닌 Variety가 있다.[10] 빅데이터 기술은 데이터를 단순히 수집하는 것뿐만 아니라 필요한 데이터를 추출하여 가치를 생산해내는 기술이기 때문에 마이데이터 시장 형성 및 디지털 전환 환경에서 그 중요성은 더욱 커지고 있다. 또한, 빅데이터 기술은 수익개선 및 비용의 효율화 등 기업의 수익성 증대와 관련한 문제뿐만 아니라, 데이터 속에서 찾은 새로운 가치를 통해 기존의 상품 및 서비스 구조를 개선·향상 시키는 데 유용하다.

〈표 Ⅱ-1〉 디지털 전환에 활용되는 주요 정보기술 요약

기술	요약	효과
빅데이터	대량의 데이터로부터 가치를 추출하고 결과를 분석하는 기술	대규모의 새로운 정보를 효율적, 효과적으로 추출/활용 가능
오픈 API	누구나 온라인상에서 응용 프로그램을 작성할 수 있게 하는 인터페이스	프로그램 개발 소요 시간 및 비용 단축
인공지능/머신러닝	기계가 데이터를 학습하여 인간의 의사결정을 대신하는 기술	인적비용 절감, 서비스 효율화 및 속도 개선, 고객 만족도 향상
디지털 플랫폼	공급자가 제공하는 가상 플랫폼 안에서 생산자와 소비자가 상품 및 서비스를 거래하는 기술	사업 확장성 및 제품·서비스 질의 향상
클라우드	ICT 자원을 포함하는 데이터 센터로부터 정보통신망을 통해 유료로 서비스를 이용하는 방식	빅데이터 환경하 제한된 ICT 자원의 비용 효율적 활용 가능
암호화 기술	정보를 암호문으로 변환하는 기술	생체인증 등의 보안성 향상으로 금융서비스 안정성 확보
분산컴퓨팅 기술	컴퓨터 처리 능력을 분산시킴으로써 고성능 컴퓨팅 파워를 가능하게 하는 기술	대량의 데이터 및 애플리케이션을 처리하는 데 효율적임
가상현실/증강현실	실제와 유사한 가상환경 및 실제와의 조화가 가능한 환경을 통해 경험의 향상을 가져올 수 있는 기술	복잡한 금융서비스의 효과적인 시각화 가능
양자컴퓨팅	큐빗을 정보단위로 하여 연산능력을 고도화할 수 있는 기술	압도적인 연산능력을 통한 금융리스크 관리 효율화 가능
메타버스	현실과 가상의 상호작용을 통해 새로운 가치를 창출하는 가상공간	새로운 디지털 금융시장 확대 및 고객 경험 향상

자료: 본문 인용 자료를 활용하여 저자가 재정리함

10) 한국정보통신기술협회 용어사전을 참조함; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=037016-8

API(Application Programming Interface)는 운영체제, 프로그래밍 언어 등에 있는 라이브러리를 응용 프로그램 개발 시 이용할 수 있도록 규칙들을 정의해 놓은 인터페이스이다.[11] API는 소프트웨어로 실현된 기능 구현물인 애플리케이션 계층과 미들웨어(middleware) 서비스[12] 계층 사이에 존재하여 프로그램들이 서로 상호작용 할 수 있도록 도와주는 매개체 역할을 한다. 즉, 만약 특정 사이트에서 데이터를 공유할 경우, 데이터 요청 및 수신 방식에 대한 규칙을 의미한다. 특히, 오픈 API는 누구나 사용할 수 있도록 공개된 API로서 접근성과 활용성이 높다는 장점이 있고, 이를 이용해서 프로그램을 개발한다면 이에 소요되는 시간과 비용을 줄일 수 있다(Qui et al. 2016)(〈그림 Ⅱ-2〉 참조).

〈그림 Ⅱ-2〉 Amazon API Gateway의 구조(오픈 API 사례)

자료: AWS의 Amazon API Gateway 웹사이트를 참조함(https://aws.amazon.com/ko/api-gateway/)

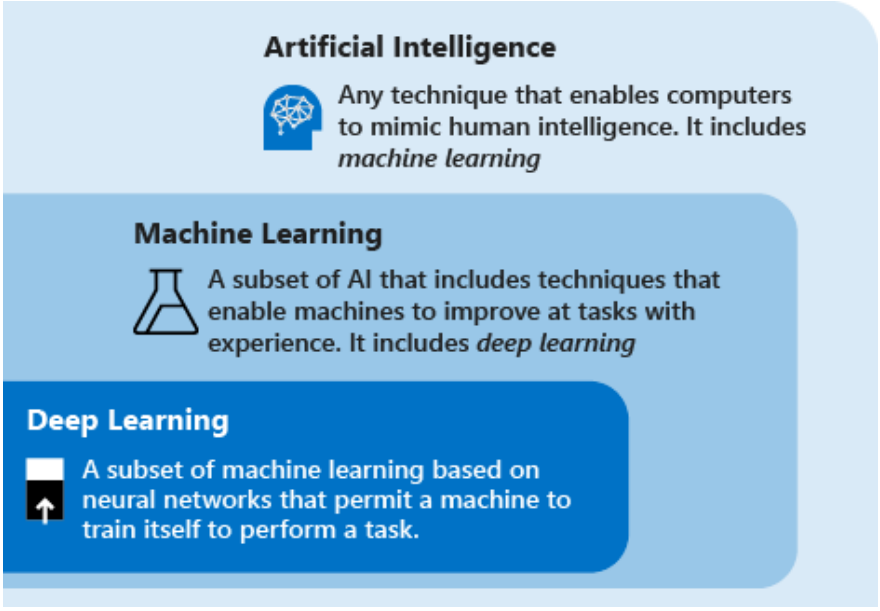
4차 산업혁명을 논할 때 가장 많이 언급되는 인공지능(Artificial Intelligence; AI)은 기계가 인간의 지능을 모방할 수 있는 방법을 개발하는 것과 관련이 있다(Hull 2020). 인공지능의 대표적인 분야로서 머신러닝 및 딥러닝을 많이 활용하는데, 이는 빅데이터를 학습함으로써 지능을 창출하는 것을 포괄한다(〈그림 Ⅱ-3〉 참조). 초기 머신러닝은 컴퓨팅 파워의 한계로 인해 침체기를 겪었지만, 최근 들어 컴퓨팅 파워가 개선되고 알고리즘 성능이

11) 한국정보통신기술협회 용어사전을 참조함; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=036061-3

12) 응용 프로그램이 다른 응용 프로그램, 네트워크, 하드웨어 또는 운영체제와 상호 작용하거나 통신을 할 수 있도록 지원하는 소프트웨어를 의미함(Bishop and Karne 2003)

비약적으로 상승하면서 산업 전반에서 활용도가 높아지고 있다(Hwang 2018). 인간의 의사결정을 대신할 수 있는 기계 알고리즘이 상용화되면서 금융산업의 디지털 전환에 있어서도 인적비용 절감, 서비스의 효율화 및 속도 개선, 고객 만족도 향상 등의 효과를 경험하고 있다.

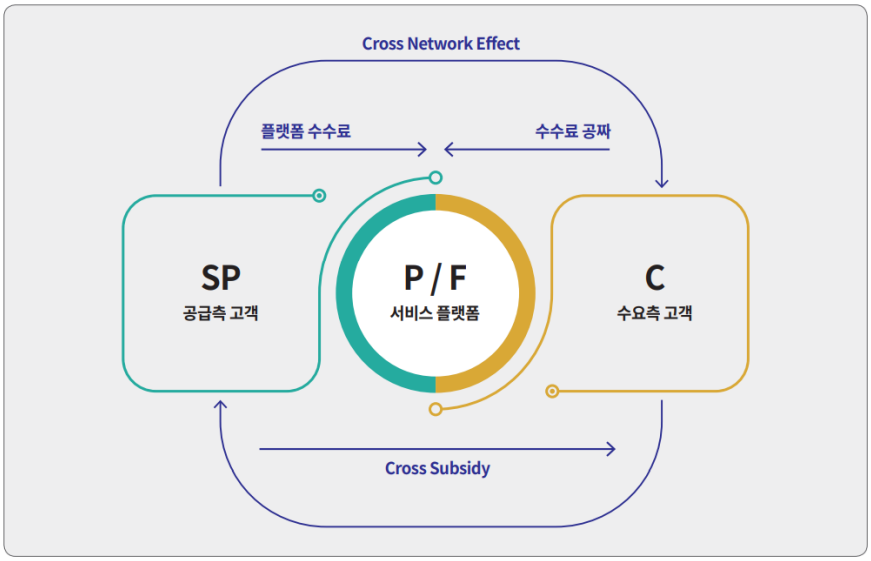
〈그림 Ⅱ-3〉 인공지능, 머신러닝 및 딥러닝 관계성



자료: Microsoft Azura 웹사이트를 참조함(https://docs.microsoft.com/ko-kr/azure/machine-learning/concept-deep-learning-vs-machine-learning)

디지털 플랫폼(digital platform)은 소비자와 생산자처럼 구별되는 사용자들 간의 상호작용을 촉진하는 양면 네트워크를 의미한다(Koh and Fichman 2014). 예를 들어, Airbnb, Uber와 같이 플랫폼 공급자가 제공하는 가상 공간 안에서 생산자와 소비자의 거래가 이루어진다. 공급 측면에서 생산자는 디지털 플랫폼의 공유인프라로 인해 초기 투자비용을 절감할 수 있으며 시장 수요를 효율적으로 증가시킬 수 있다. 반면, 수요 측면에서 소비자는 플랫폼을 통해 양질의 상품과 서비스를 제공받을 수 있으며, 여러 상품을 동시 비교하며 맞춤형 상품을 탐색할 수 있다(〈그림 Ⅱ-4〉 참조). 특히, 디지털 플랫폼을 활용한 기업은 디지털의 무료와 완전성이라는 특성을 통해 확장성과 네트워크 측면에서 상당한 이점을 얻을 수 있다.

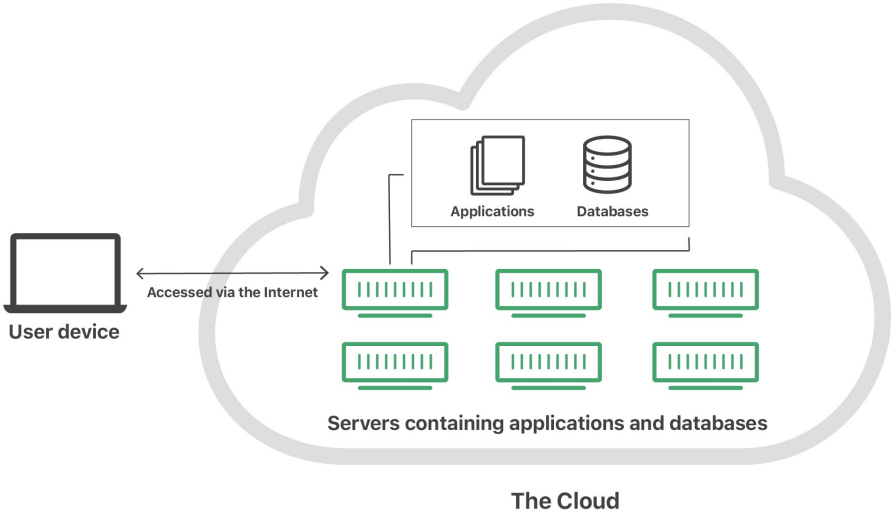
〈그림 Ⅱ-4〉 디지털 플랫폼 내 공급자-수요자 관계 구조



자료: 김학용(2021)의 〈그림 1〉을 참조함

클라우드는 사용자가 인터넷에 자료를 업로드 한 후에 필요한 때, 필요한 정보를 인터넷 접속만으로 이용할 수 있게 도와주는 서비스를 의미한다(KPMG 2019)(〈그림 Ⅱ-5〉 참조). 클라우드 서비스의 종류에는 크게 3가지가 있는데 서버, 저장장치 등의 장치를 서비스로 제공하는 서비스형 인프라 구조(Infrastructure as a Service; IaaS), 응용프로그램을 쉽게 개발할 수 있도록 개발 환경을 서비스로 제공하는 서비스형 플랫폼(Platform as a Service; PaaS), 그리고 응용프로그램 자체를 서비스로 제공하는 서비스형 소프트웨어(Software as a Service; SaaS)가 있다(KPMG 2019). 사용자 입장에서는 필요한 ICT 자원을 직접 구입하여 설치하는 방식에 비해 클라우드 서비스가 경제적으로 더 효율적일 수 있으며, 아마존의 AWS, 구글, 네이버 등 많은 빅테크 기업에서 비용효율적인 클라우드 서비스를 제공하고 있다(KPMG 2019).

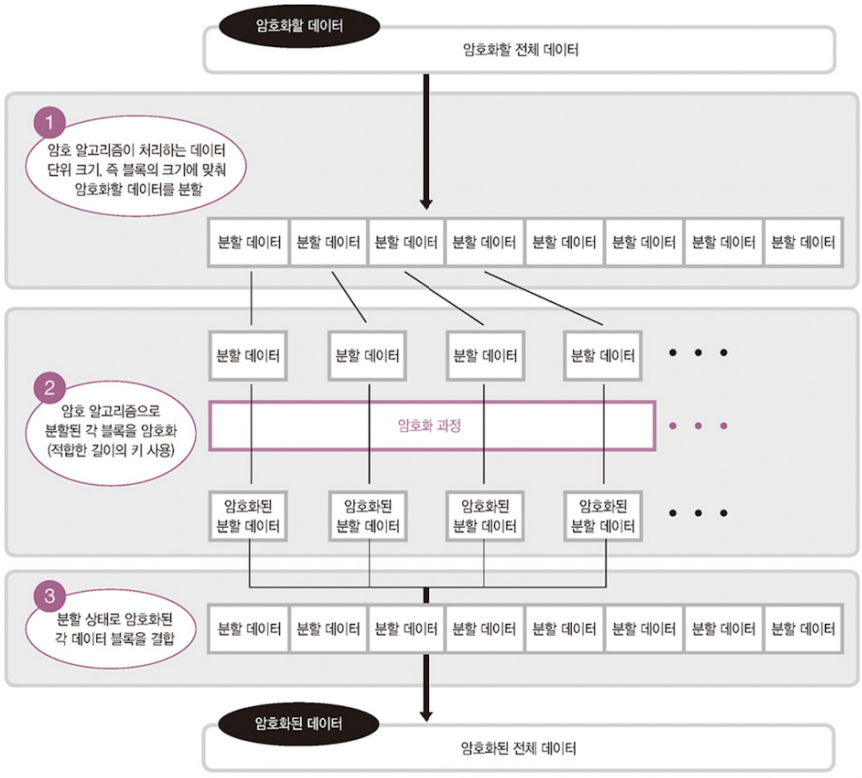
〈그림 Ⅱ-5〉 클라우드 플랫폼 구조



자료: 김학용(2021)의 〈그림 1〉을 참조함

암호화 기술(encryption technology)은 일반 메시지를 암호 텍스트로 바꾸어주거나 암호 해독을 위해 사용되는데 해당 과정을 인코딩(encoding; 암호화) 및 디코딩(decoding; 복호화) 과정이라고 한다(Hall et al. 2003)(〈그림 Ⅱ-6〉 참조). 인코딩 및 디코딩 과정은 비밀 키를 활용해서 수행되며, 해당 키가 없는 다른 사용자는 메시지를 해독할 수 없기 때문에 암호화는 정보 보안에 있어 필수적인 역할을 수행한다(Murray 1995; Heckerman 2008). 암호화 방법에는 크게 대칭키 암호와 비대칭키 암호로 구분된다. 대칭키 암호화는 암호화 과정과 암호 해독 과정에서 하나의 단일 키를 사용하는 방법이며(Delfs and Knebl 2015), 비대칭키 암호화는 두 개의 키를 가지고 각각 암호화 및 암호 해독 과정에 사용한다(Pinckney et al. 2017). 최근 지문, 홍채, 안면 인식 등의 생체인증을 이용한 암호화 기술이 비약적으로 성장하면서 보안 수준이 크게 향상되었으며, 따라서 안전성을 보장할 수 있는 디지털 금융 서비스 제공이 가능해지게 되었다.

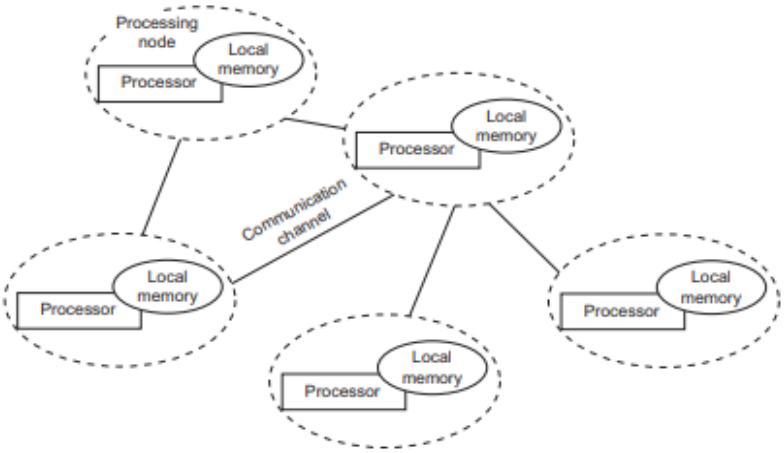
〈그림 Ⅱ-6〉 데이터 암호화 구조



자료: 김덕수·이석우(2016)의 p. 50을 참조함

분산컴퓨팅 기술(distributed computing technology)은 네트워크로 연결된 여러 대의 컴퓨터 처리 능력을 이용하여 계산량이 복잡한 문제를 해결하는 방법이다(Sitaram and Manjunath 2011). 하나의 대형컴퓨터에서 수행하던 기능을 분산된 여러 대의 컴퓨터에서 분담하도록 설계된 네트워크 기반의 구조로서, 이를 활용하면 컴퓨팅 파워와 안정성을 향상시킬 수 있다(Sitaram and Manjunath 2011)(〈그림 Ⅱ-7〉 참조). 최근 블록체인과 분산컴퓨팅 기술이 접목되어 새로운 서비스들이 출시되고 있는데, 일례로 분산원장(distributed ledger technology) 기술이 활용되고 있다. 분산원장은 탈중앙화된 시스템을 통해 사용자가 자신의 자산과 부채의 거래 또는 소유에 대한 기록을 안전하게 유지하고 갱신할 수 있도록 도와준다(IMF 2017).

〈그림 Ⅱ-7〉 분산 컴퓨팅 시스템 구조



자료: Sitaram and Manjunath(2011)의 〈그림 9-16〉을 참조함

최근 금융산업의 디지털 전환에 있어 가장 주목받고 있는 기술 중 하나는 가상현실(Virtual Reality)과 증강현실(Argumented Reality)이다. 가상현실은 정보통신기술을 활용하여 실제와 유사한 특정 환경이나 상황을 만들어낸 것이나 그 기술 자체로서 정의한다.[13] 증강현실은 가상현실의 일부로서 실제 환경 속에 가상의 사물이나 정보를 합성하여 실제에 존재하는 것처럼 보이도록 하는 컴퓨터 그래픽 기법을 말한다.[14] 가상현실이 가상의 객체들로 둘러싸인 환경 속에서 사용자에게 실제를 인식할 수 없는 몰입을 제공한다면, 증강현실은 사용자가 가상 객체와 함께 실제 현실을 볼 수 있다는 차이점을 갖는다(윤혜영 2018). 최근 금융권에서는 복잡한 콘텐츠를 시각적 요소와 함께 전달할 수 있는 가상현실 및 증강현실의 특징을 통해 다양한 영역에서 고객경험을 향상하는 데 활용하고 있는데, 예를 들면, AR 앱을 통해 주변 영업점 및 ATM 등의 서비스를 확인할 수 있는 서비스가 있다.[15]

곧 실현될 수 있을 것으로 기대되는 미래 기술로서 양자 컴퓨팅(quantum computing)은 양자(quantum)의 역학적 특징인 중첩(superposition)과 얽힘(entanglement) 등의 현상

13) 한국정보통신기술협회 용어사전을 참조함; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=103970-2

14) 한국정보통신기술협회 용어사전을 참조함; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=097129-1

15) 김회민(2018)을 참조함

을 이용하여 연산을 수행하는 기술을 뜻한다.[16] 0 또는 1을 갖는 비트(bit)를 사용하여 연산을 수행하는 기존 디지털 컴퓨터의 연산 방식과 달리, 양자 컴퓨팅은 0과 1을 동시에 가질 수 있는 성질(양자중첩)을 갖는 큐빗(qubit)을 정보 단위로 사용하기 때문에 정보 단위(비트 및 큐빗)의 수가 증가함에 따라 연산 능력이 기존 컴퓨팅 방식 대비 월등히 증가한다는 특징을 갖는다. 이러한 월등한 연산능력을 바탕으로 금융권에서는, 예를 들어, 금융리스크 정량분석 시 많은 소요가 발생하는 시뮬레이션 과정을 양자컴퓨팅을 통해 고속화할 수 있다(이혁성 2019).

메타버스(metaverse)는 현실세계를 의미하는 '유니버스(universe)'와 가공 및 추상을 의미하는 '메타(meta)'의 합성어로서 자신을 나타내는 아바타를 통해 활동하는 3차원 가상세계를 의미한다(한상열 2021). 메타버스는 그간 가상현실과 혼용되어 왔으나, 최근에는 단순 3차원 가상세계를 넘어 현실 사회의 개념과 합쳐져 범위를 확장하여 '현실과 가상이 상호작용을 통해 새로운 산업, 사회, 문화적 가치를 창출하는 세계'로서 정의된다(한상열 2021). 현재 금융산업에서는 이러한 메타버스 기술을 활용하여 금융소비자들이 가상세계에서 금융서비스를 영위하는 고객여정(customer journey)을 설계하고 있으며, 메타버스 세계에서의 디지털 지점 등을 제안함으로써 가상세계에서의 금융상품 시장을 형성하고자 계획 중이다.

3. 은행의 디지털 전환 양상

가. 프론트 오피스(Front office)

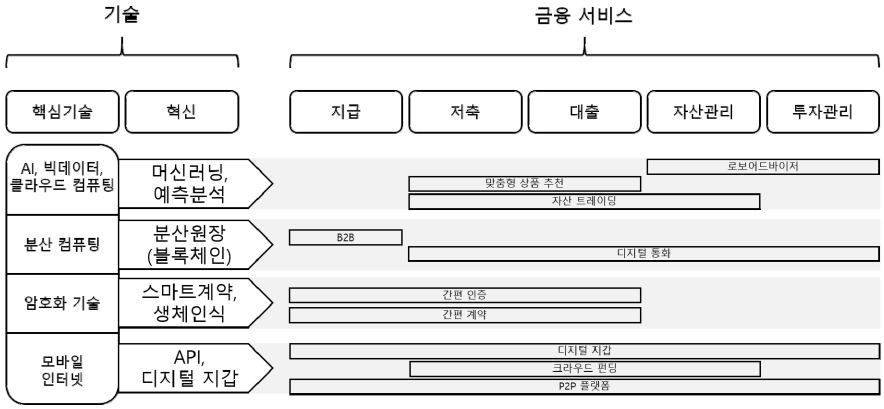
은행의 프론트 오피스(front office)는 수익을 창출해내는 기능을 담당함에 따라 고객들과의 직접적인 거래가 주로 이루어진다. 따라서, 미들 오피스(middle office) 및 백 오피스(back office)에 비해 비즈니스 프로세스 및 서비스 측면에서의 디지털 전환이 다양하게 이루어지고 있다. 특히, 금융 서비스의 간편성 및 편의성을 추구하는 밀레니얼 세대의 니즈에 맞춰 금융 서비스의 개인화 및 맞춤화가 이루어지고 있으며, 그 외 다양한 고객의 니즈를 충족시키기 위한 플랫폼화, AI 기술의 적극적 활용, 핀테크 기업과의 제휴 등이 복합

16) 한국정보통신기술협회 용어사전을 참조함; http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=061030-2

적으로 진행되고 있다. 은행은 이러한 변화를 통해 금융 서비스 제공에 들어가는 비용과 시간을 감소할 수 있고, 다양한 채널을 통해 고객과의 접점을 강화할 수 있다.

〈그림 Ⅱ-8〉은 프론트 오피스에서의 디지털 혁신 기술 활용 범위에 관한 사례들을 도식화한 것이다. 앞서 논의한 인공지능/머신러닝, 분산원장, 암호화 기술 등이 지급, 결제, 저축, 대출 및 자산/투자 관리 영역까지 전반적으로 활용되고 있는 양상이다. 예를 들면, 인공지능이 제공하는 챗봇(Chatbot)을 통한 고객 응대 서비스 또는 인공지능 음성비서를 사용하여 목소리로 서비스를 제공하는 보이스 뱅킹 등이 이미 상용화되어 있다(KPMG 2021). 또한, 모바일 뱅킹이 일상화됨에 따라 지점을 찾는 고객의 수가 감소하고, 다양한 비대면 채널의 활용이 중요해졌다. 이에 따라, 고객의 편의성, 경험을 명확히 파악하여 맞춤형 또는 개인화된 상품 및 서비스를 제공할 수 있는 기술(즉, 머신러닝, 예측분석 등)을 적극 활용하여 상용화하고 있다.

〈그림 Ⅱ-8〉 은행 프론트 오피스에서의 디지털 전환



자료: IMF(2017)의 〈Figure 4〉를 참조하여 프론트 오피스에 관해 재구성함

고객 경험 향상을 통한 시장 수요 증진 등의 목표를 달성하기 위한 프론트 오피스의 디지털 전환 노력은 많은 곳에서 관찰되고 있으나, 현실적이고 어려운 도전 앞에 더 적극적이고 근본적인 생존전략이 필요한 상황이다. 즉, 카카오페이 및 뱅크, 네이버 파이낸셜과 같은 빅테크 기업들의 금융 서비스업 진출은 은행의 프론트 오피스가 디지털 전환 및 혁신 경쟁의 중심에서 압박을 받을 수 있는 환경에 직면해 있음을 의미한다. 빅테크 기업들이 플랫폼을 활용하여 가능한 모든 금융서비스를 제공할 수 있는 시장 참여자가 된다면, 기

존 은행들은 사실상 승산없는 경쟁을 벌이게 될 수 있는 암울한 전망도 존재한다. 〈표 Ⅱ-2〉의 프론트 오피스 디지털화 양상과 같이 은행들은 디지털 플랫폼을 강화하고 고객경험 향상 및 맞춤형 서비스 탐색/개발에 역량을 집중하여 금융 소비자들의 수요가 여전히 기존 은행들의 서비스에 머무를 수 있도록 해야 할 것이다.

〈표 Ⅱ-2〉 프론트 오피스 디지털 전환 양상

양상	기술	효과	예시
금융 서비스 개인화 및 맞춤화	빅데이터	개인 맞춤화로 수요 창출	고객 금융 데이터를 기반으로 고객별 맞춤형 서비스를 제공
AI 도입 본격화	머신러닝	새로운 비즈니스 모델을 통한 수익 창출	전통적인 분류 방식의 한계를 극복하기 위해 머신러닝을 활용한 ETF 출시
플랫폼화	오픈 API	새로운 비즈니스 모델을 통한 수익 창출	여러 제휴사에 당사의 오픈 플랫폼을 제공하여 새로운 금융서비스 개발
플랫폼화	디지털 플랫폼	멀티 채널을 통한 고객 접점 강화	온라인 플랫폼을 중심으로 멀티 채널 제공 및 서비스 통합. 이를 통해 고객과의 접점 강화

자료: KPMG(2019; 2021)

나. 미들 오피스(Middle office)

은행의 미들 오피스 업무는 주로 거래의 적절성을 모니터링하고 통제하는 것이다. 즉, 시장·신용·운영 리스크 관리, 유동성 관리 및 규제 관련 지원 업무를 담당하는 미들 오피스의 경우 디지털 전환을 위해 핀테크 기업과 적극적인 제휴가 이루어지고 있는 양상이다. 업무 효율화 솔루션과 같은 서비스뿐만 아니라 투자위험관리, 리서치 및 데이터 분석과 같은 서비스를 제공하는 핀테크 기업들이 시장에 등장하면서 이러한 기능을 활용하기 위한 제휴가 증가하고 있다(KPMG 2019).

실제로 골드만삭스는 인공지능 솔루션 시스템 Kensho를 도입하여 거시 경제지표 및 주가 동향 등을 자동화된 문서로 생성 및 보고하는 프로세스를 구축하여 미들오피스 핵심업무의 효율성을 향상시켰다(KPMG 2019). JP 모건의 경우 비지도 학습(unsupervised learning) 알고리즘을 기반으로 한 머신러닝 플랫폼인 COiN(Contract Intelligence)을 도입하여 법률 문서상 주요 정보와 조항들을 추출하는 등의 업무 자동화를 구축하였다.(금융보안원 2017)

이와 더불어 다른 산업에 비해 엄격한 금융 규제과 관련하여 레그텍(RegTech) 기술에 대

한 투자가 확대되고 있다. 〈그림 Ⅱ-9〉의 기술 적용 사례를 살펴보면 미들 오피스에서는 인공지능/머신러닝, 빅데이터, 디지털 플랫폼 기술 등이 주로 활용되고 있으며, 레그텍의 경우 머신러닝 기술을 통해 준법감시와 내부통제를 강화하여 다양한 규제에 대응하는 방식으로 발전하고 있다(〈표 Ⅱ-3〉 참조). 그 외에도 위험평가와 관련하여 Bank of America는 신용리스크 산정 시간 단축 및 손실 예측 향상, 비정형 신용리스크 데이터 분석 등의 문제를 머신러닝 기술을 통해 해결해 나가고 있다(KPMG 2019).

〈그림 Ⅱ-9〉 은행 미들 오피스에서의 디지털 전환

자료: IMF(2017)의 〈Figure 4〉를 참조하여 미들 오피스에 관해 재구성함

〈표 Ⅱ-3〉 미들 오피스 디지털 전환 양상

양상	기술	효과	예시
핀테크 기업과의 제휴	디지털 플랫폼	포트폴리오 통합관리 및 모니터링	다수 금융사로의 포트폴리오 분산관리 중인 초부유층 투자자 대상 통합 플랫폼 제공
핀테크 기업과의 제휴	머신러닝	리서치 역량 강화 및 서비스 비용 감소	고객 포트폴리오 통합 관리 및 모니터링이 가능한 투자 관리 플랫폼을 핀테크 스타트업으로부터 제공받음
핀테크 기업과의 제휴	빅데이터 머신러닝	리서치 역량 강화	시장 이벤트가 금융시장에 미치는 영향력에 관한 인공지능 금융분석 서비스 제공
레그텍(RegTech) 투자 확대	머신러닝	서비스 비용 감소 및 업무 효율화	AI 및 빅데이터 기반 약관 심사 솔루션을 도입하여 수만 건의 문서를 자동으로 해독. 규정 위반 사항을 손쉽게 진단 가능

자료: KPMG(2019) 및 이효섭(2019)을 참조함

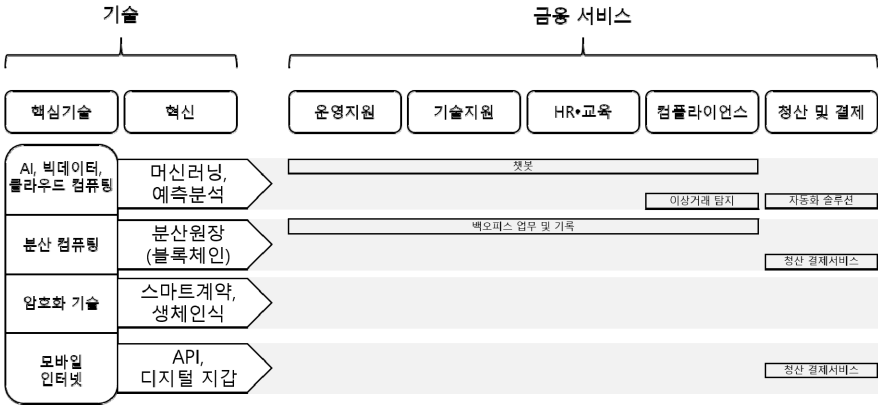
다. 백 오피스(Back office)

은행의 백 오피스에서는 거래 사후 관리, 회계 업무 및 인사관리와 같은 지원 업무가 주를 이룬다. 이는 정확하고 투명한 처리가 요구되는 업무들로서, 미들 오피스와 마찬가지로 디지털 전환을 위해 핀테크 기업과의 제휴가 많이 이루어지고 있다. 특히, 자금세탁방지(Anti-Money Laundering; AML) 및 고객 확인 의무(Know Your Customer; KYC) 등의 수칙을 이행하기 위한 고객 개인정보 관리, 신원확인, 개인정보 이용 동의서 작성/관리 등의 서비스를 머신러닝 기술을 통해 자동화한 핀테크 기업과의 협업이 관찰된다(KPMG 2019). 이러한 서비스를 활용하게 되면 백 오피스 업무 과정에서의 비용 및 시간을 단축시킬 수 있는 효과를 가져오지만, 기업의 핵심역량을 유지하기 위해 기업 내부적으로 개발하는 사례(In-house)도 점차 증가하고 있는 현실이다.

백 오피스에서의 디지털 전환 또한 앞서 다른 부서의 양상과 유사하게 빅데이터 기술, 인공지능/머신러닝, 클라우드, 디지털 플랫폼, 블록체인 기술 등을 통해 실현되고 있다(〈그림 Ⅱ-10〉 참조). 예를 들면, Fenergo의 경우 금융기관을 대상으로 인공지능/머신러닝 기술을 활용한 솔루션을 활용하여 금융기관의 고객 계좌 생성, 경영정보 관리, 규제 준수 등을 통합적으로 지원한다(KPMG 2019). 이를 통해 제휴사는 추가적인 고객 확인 의무 절차를 거칠 필요가 없어 업무의 효율성을 향상시킬 수 있다. 미국의 Digital Reasoning 또한 AI기술을 활용하여 내부직원의 이메일, 메신저 및 전화 등을 모니터링함으로써 내부자 거래 및 기타 부적절한 행위 등을 포착하는 보안서비스를 제공한다(KPMG 2019). 이를 통해 제휴사들은 직원들이 내부 컴플라이언스를 준수하는지 쉽게 모니터링이 가능하다.

인공지능/머신러닝 기술 적용뿐만 아니라, 다수의 거래소 중심으로 블록체인 기반 청산결제서비스가 계획 및 활용되고 있다(〈표 Ⅱ-4〉 참조). 캐나다의 토론토 증권거래소 및 런던 증권거래소, 일본 증권거래소 등에서 블록체인 도입을 위한 워킹 그룹을 구성하여 진행 중에 있으며, 일반 금융기업 중에도 골드만삭스 등에서 블록체인 기반 원장 시스템을 개발 중에 있다(KPMG 2019).

〈그림 Ⅱ-10〉 은행 백 오피스에서의 디지털 전환



자료: IMF(2017)의 〈Figure 4〉를 참조하여 백 오피스에 관해 재구성함

〈표 Ⅱ-4〉 백 오피스 디지털 전환 양상

양상	기술	효과	예시
핀테크 기업과의 제휴	머신러닝	자금세탁 방지(AML) 이행 효율화	핀테크 스타트업 기술을 활용하여 자금세탁 및 테러자금 등을 감지 및 예방하는 솔루션을 제공받음
핀테크 기업과의 제휴	머신러닝	내부 통제 시 비용 및 시간 감소	핀테크 스타트업의 AI 기술을 활용하여 직원의 이메일, 메신저, 전화 등을 다각도로 모니터링하고 이를 기반으로 내부자 거래 등을 포착하는 서비스를 제공 받음
내부통제 효율화	빅데이터	내부 통제 시 비용 및 시간 절감	내부 직원의 인터넷 사용 기록과 이메일, 전화 통화 기록 등을 분석하여 비리 혐의 포착
핀테크 기업과의 제휴	블록체인 오픈 API	청산결제 서비스 제공 탈중앙화	다수 거래소 중심으로 블록체인 기반 청산결제 서비스 활용 계획 오픈 API를 통한 클라우드 서비스 활용 청산결제 업무 상용화

자료: KPMG(2019)를 참조함

4. 보험사의 디지털 전환 양상

보험산업은 금융산업 내에서 보수적인 업종 중 하나로서, 아직까지 대부분의 업무들이 대면으로 이루어지고 있다. 그러나 최근 핀테크와 함께 인슈어테크(InsurTech)로 대표되는 보험산업의 디지털 전환이 적극적으로 실현되고 있는 상황이다. 이 장에서는 보험산업의 디지털 전환 사례들과 함께 인슈어테크 적용 양상을 간략하게 살펴본다.

가. 인슈어테크 요약[17)]

인슈어테크란 보험(Insurance)과 기술(Technology)의 합성어로 인공지능/머신러닝 등의 최신 IT기술을 활용하여 보험산업의 가치사슬 변화를 가져오는 기술을 총칭한다. 인슈어테크라는 단어가 나오기 이전에는 기존 보험 프로세스의 효율적인 개선에 초점이 맞춰져 있었다면, 인슈어테크는 기술을 통해 새로운 비즈니스 모델을 창출하고, 소비자 맞춤형 상품을 제공하는 것을 목표로 한다. 이 장에서는 다양한 형태의 인슈어테크 적용 사례 중 Braun and Schreiber(2017)에서 제안한 9가지 인슈어테크 유형에 초점을 맞춰 소개하고자 한다(〈표 Ⅱ-5〉 참조).

먼저, 비교 플랫폼(comparison portal)의 경우 고객들의 효율적인 의사결정을 위해 여러 보험상품 및 보험사의 정보를 제공한다. 소비자는 비교 플랫폼에 있는 정보를 토대로 자신의 상황에 가장 알맞은 보험 보장을 선택하고, 경제적인 의사결정을 할 수 있다. 비교플랫폼의 해외 사례로, 특히, 독일의 Check24와 스위스의 Comparis는 보험뿐만 아니라 통신, 전력 등 다른 제품들까지도 비교할 수 있어 많은 수요를 유치할 수 있다. 디지털 브로커(digital brokers)는 원수 보험사와 협약을 맺고, 온라인이나 모바일 앱을 통해 고객들에게 맞춤형 추천 상품들을 제공하는 보험 중개 서비스를 제공한다. 또한, 원수 보험사와 고객을 연결하는 중개 역할뿐만 아니라, 보험 정보를 투명하게 파악할 수 있는 디지털 플랫폼 및 보험 상담 서비스도 제공한다. 대표적인 디지털 브로커로는 독일의 GetSafe와 미국의 Coverwallet and Embroker 등이 있다(〈그림 Ⅱ-11〉 참조).

교차 판매(cross-selling) 서비스 유형 또한 인슈어테크로 분류할 수 있는데, 이는 고객이 구매한 상품과 연계하여 보험상품을 묶어서 판매하는 전략이다. 예를 들면, 아마존 등의

17) 이하 내용은 Braun and Schreiber(2017), 박소정·박지윤(2017) 및 해외 보험사들의 홈페이지를 참고하여 구성함

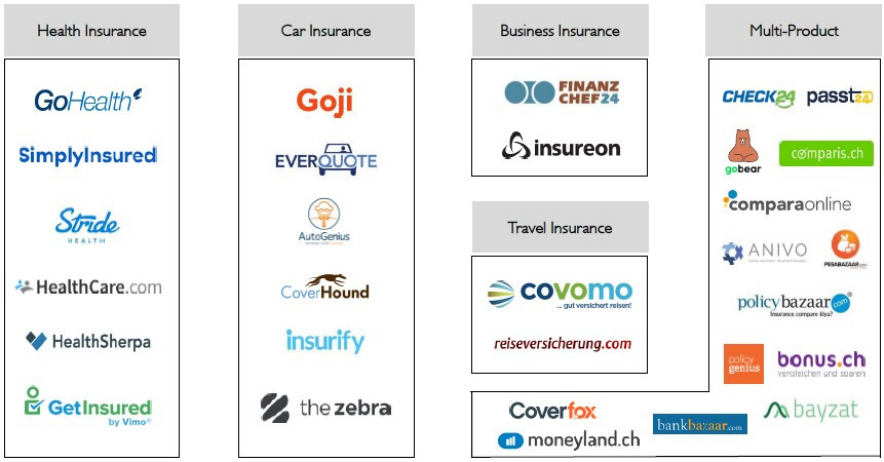
온라인 쇼핑 플랫폼 업체들이 주요 상품에 대해 보험상품을 묶어서 판매하는 것처럼 다른 온라인 채널을 통해 보험 판매가 이루어지는 형태이다. 교차판매를 통해 보험사는 새로운 수요를 창출할 수 있고, 고객은 구매 시점에 해당 상품에 대한 위험을 전가할 수 있는 서비스를 복잡한 서류 작업없이 구매할 수 있다. 인슈어테크와 함께 최근 새로운 시장으로 주목받는 P2P(Peer-to-Peer) 보험은 기존 보험사를 거치지 않고 동질적인 위험을 보유한 개인들이 온라인 플랫폼에서 위험을 공동 부담하는 형태이다. P2P 보험사는 직접 위험을 인수하는 것이 아니라, 고객들에게 플랫폼을 제공하고 이에 대한 수수료를 취한다. P2P 보험의 경우 보험계약자가 보험료 환수를 위해 전가 위험에 의한 사고를 스스로 조심함으로써 도덕적 해이를 효과적으로 경감할 수 있다는 특징이 있다. 독일의 Friendsurance, 일본의 justInCase, 중국의 핑안그룹과 우리나라의 미래에셋생명 등 P2P 보험상품을 운영하는 다양한 보험사들이 늘어나고 있는 추세이다(〈그림 Ⅱ-12〉 참조).

〈표 Ⅱ-5〉 인슈어테크 분류

인슈어테크 유형	설명
비교 플랫폼 (Comparison portal)	온라인상에서 보험상품의 가격 비교 서비스 제공
디지털 브로커 (Digital brokers)	원수 보험사와의 파트너십을 통해 고객과 원수 보험사를 연결하는 중개 서비스 제공
보험 교차판매 (Insurance cross-selling)	상품 및 서비스 판매 시 보험을 포함하여 판매
P2P 보험 (Peer-to-Peer)	동질적 위험을 가진 보험계약자들 간 상호 보장하는 형태
온디맨드 보험 (On-demand)	고객이 원하는 시기에 특정 위험에 관한 보장여부를 선택할 수 있는 보험
디지털 보험사 (Digital insurers)	보험산업의 가치사슬을 디지털화하여 온라인 채널을 통해서만 거래하는 보험회사
빅데이터 분석 및 보험 소프트웨어 (Big data analytics & Insurance software)	내부 및 외부 데이터를 보다 효과적으로 관리하고 활용할 수 있는 서비스를 제공. 해당 소프트웨어 안에서 보험 가입 지원
사물인터넷 (Internet of Things)	인터넷을 통해 서로 통신할 수 있도록 연결된 장치 및 센서 등의 네트워크. 실시간 데이터를 통해 도덕적 해이 통제 가능
블록체인 및 스마트 계약 (Blockchain & Smart contracts)	블록체인은 탈중앙화 특징을 가지고 있어 위조가 불가능하고 도덕적 해이를 방지하는 데 활용 가능. 블록체인 기술을 활용하여 스마트 계약도 진행 가능

자료: Braun and Schreiber(2017)의 〈Table 6〉를 재구성함

〈그림 Ⅱ-11〉 보험상품 비교 플랫폼 제공 스타트업 사례



자료: Braun and Schreiber(2017)의 〈Figure 18〉을 참조함

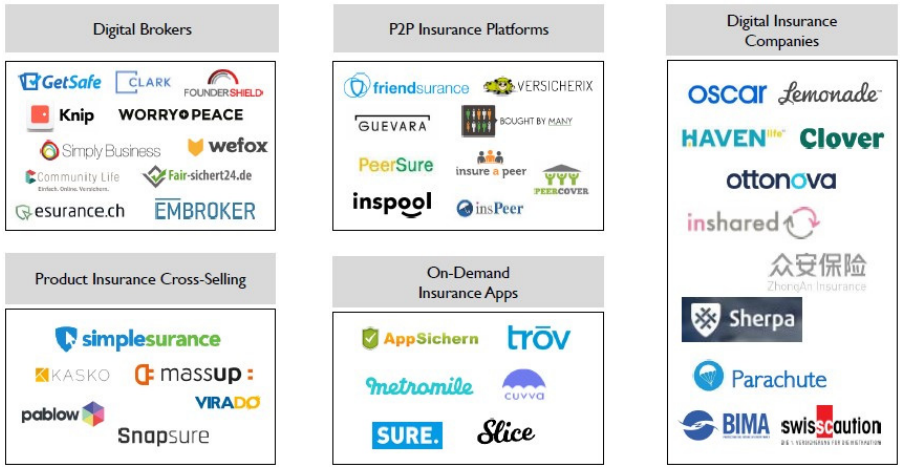
온디맨드(on-demand) 보험 또한 P2P 보험과 같이 인슈어테크 시대에 대표적인 혁신 보험상품으로 주목받고 있다. 이 보험의 특징은 보험계약자가 원하는 기간 동안 특정 위험에 관한 보장 서비스를 제공받을 수 있는 선택권을 가진다는 점이다. 예를 들면, 여행자 보험이나 일일 운전자 보험 등에 주로 적용되어 상용화되고 있는데, 기존 보험보다 보험가입자에게 유연성을 제공하며, 고객은 더 적은 비용으로 위험을 전가할 수 있다. 미국의 보험 스타트업인 Slice는 고객이 플랫폼을 통해 주택을 공유하기로 결정했을 때, 해당 주택에 대해 원하는 기간 동안 적절한 보험을 가입할 수 있는 온디맨드 보장 서비스를 제공한다.

Slice와 같이 온디맨드 보험을 제공하는 회사들은 주로 온라인 기반의 비즈니스 모델을 구축하고 있는데, 이러한 디지털 보험사들이 인슈어테크 상용화를 주도하고 있다. 디지털 보험사는 보험사업의 가치사슬의 전면적 디지털화를 추구하는 유형으로서, 디지털 플랫폼을 통해서 운영한다. 디지털 보험사의 예로서, 미국의 Oscar는 건강보험 판매뿐만 아니라 고객의 건강관리/헬스케어 서비스까지 제공하고 있으며 중국의 중안보험은 보험금 청구 절차 자동화 등의 디지털 프로세스를 통해 다양한 손해보험 상품을 판매하고 있다(최창희 외 2017). 이러한 디지털 보험사들은 적극적으로 빅데이터 분석 기술 및 보험 소프트웨어를 개발하여 활용하고 있다. 데이터 기반으로 가치를 생산해내는 보험산업의 특성상 활용 데이터 규모의 증가는 더 정확한 보험료 산출 및 위험평가를 가능하게 한다. 최근

다수의 보험 스타트업들이 내부 및 외부 데이터를 보다 효과적으로 관리하고 활용할 수 있는 빅데이터, 인공지능/머신러닝 기반 소프트웨어를 개발하여 디지털 보험사 및 기존 보험사들에게 제공함으로써 인슈어테크 기술의 적용이 빨라지고 있다(Braun and Schreiber 2017).

사물인터넷을 활용한 서비스를 제공하는 인슈어테크 스타트업도 시장에서 관찰된다. 웨어러블(wearable), 텔레매틱스(telematics), 드론(drone) 등 기술을 활용하여 실시간 데이터를 수집할 수 있으며, 이를 통해 보험계약자의 위험 수준을 더 정확하게 측정 및 판별할 수 있게 도와준다. 이러한 사물인터넷 기술은 역선택 및 도덕적 해이를 효과적으로 제어할 수 있도록 도와주기 때문에 많은 보험사들은 사물인터넷 기술을 적극 활용하여 보험계약자들을 모니터링한다. 마지막으로, 블록체인을 활용한 스마트 계약 솔루션을 제공하는 인슈어테크 보험사들도 관찰되고 있다. 앞서 언급했듯이 블록체인의 탈중앙화 특성과 모든 참여자들에 관한 검증과 추적이 가능하다는 점을 활용하여 보험사들은 보험 부정행위를 방지할 수 있다.

〈그림 Ⅱ-12〉 다양한 인슈어테크 관련 스타트업 사례



자료: Braun and Schreiber(2017)의 〈Figure 19〉을 참조함

나. 생명·건강보험

생명 및 건강보험시장에서 인슈어테크 및 디지털 전환 기술은 역선택과 도덕적 해이를 통제하는 데 효과적으로 활용된다. 예를 들어, 생명보험사의 경우 사물인터넷을 이용하여 지속적으로 보험가입자의 위험 정보를 수집하고, 건강관리 서비스를 제공함으로써 손실 발생 가능성을 낮춘다. 예를 들어, 웨어러블이나 스마트폰 애플리케이션을 활용한 디지털 어시스턴트(digital assistant) 서비스 등이 제공됨으로써 시장 내 위험평가 수준 향상 및 보험상품 구매에 관한 고객경험을 향상시키는 효과를 가져오고 있다. 특히, 미국 내 많은 보험회사에서 디지털 디바이스를 활용한 웰니스(wellness) 프로그램을 운영함으로써 보험가입자에게 예방 접종 및 금연을 지원하거나 건강을 증진시킬 수 있는 시설을 이용할 수 있게 지원한다. 일례로, 다수 보험사에서 운영하는 Vitality 프로그램은 웨어러블 기기를 통해 수집한 고객의 건강 데이터를 기반으로 건강에 따라 포인트를 지급하고, 해당 포인트를 기준으로 회원 등급이 정해서 차별적인 혜택을 지급한다(박소정·박지윤 2017).

미국의 오스카(Oscar)의 경우 웨어러블 기기를 통해 보험가입자의 생활습관을 모니터링하고, 이를 기반으로 리스크 관리 및 보상을 실시한다. 또한 보험 가입자의 위치에 기반하여 의료전문인 정보를 제공하거나 원격진료 혹은 예약 기능을 제공하는 등 고객의 편의성 증대를 위한 서비스를 제공하고 있다(문장원 외 2019). 미국의 클로버(Clover) 역시 스마트폰 모바일 앱 기반의 디지털 어시스턴트 기능을 통해 의사 상담 서비스를 제공하고 있으며(김은석·김영준 2019), 환자들의 분산된 의료 데이터를 통합·분석하여 개인 가정 방문을 통한 맞춤형 의료 서비스를 제공한다(장효미 2019). 프랑스 앨런(Alan)의 경우 소규모 사업자와 스타트업을 대상으로 보험상품을 판매하는 디지털 건강보험회사로서, 온라인 플랫폼을 통해 고객들에게 보험정보를 제공한다. 특히, Alan map 서비스를 통해 고객 맞춤형 의사 찾기 서비스 및 진료 예약 서비스를 제공한다.

이처럼 빅데이터 분석 및 디지털 플랫폼, 사물인터넷 등의 인슈어테크 기술이 적극 활용되면서 생명·건강보험사들의 위험평가 능력이 향상되고, 맞춤형 고객여정을 설계할 수 있는 환경이 만들어지게 되었다. 이를 통해 실손보험의 손해율을 낮추고, 종합 리스크 관리 서비스 제공자로서의 역할을 적극 수행하게 되었으며, 전반적으로 시장 수익성을 높이는 효과를 경험하고 있다.

다. 손해보험

손해보험사의 경우에도 역선택과 도덕적 해이 문제를 해소하기 위한 방안으로 인슈어테크 기술을 활용하고 있는 추세이다. 특히, 자동차보험에서 인슈어테크 기술을 통한 맞춤형 데이터 수집 및 운전자 습관 파악을 통한 위험 평가 등에서 효과를 보고 있다. 일례로 미국 자동차 보험사인 Progressive는 텔레매틱스 기기에 축적된 데이터를 기반으로 보험계약자의 운전 습관을 파악하고 이를 점수화하여 보험요율을 책정하고 있다. 또다른 미국 자동차 보험사인 Root Insurance의 경우 스마트폰 애플리케이션을 통해 보험가입자의 운전습관을 파악하여 합리적 자동차 보험료 책정 및 도덕적 해이 통제가 가능해졌다. 또한, 해당 애플리케이션을 통해 가입자에 대한 추가적인 정보를 계속 업데이트 함으로써 역선택을 방지하는 데 도움을 받고 있다.

영국의 자동차 보험사인 큐바(Cuvva)의 경우 온디맨드 보험을 통해 차량 운행 시에만 보장을 선택함으로써 저렴한 비용으로 자동차보험 혜택을 누릴 수 있는 기회를 제공하고 있다(김은석·김영준 2019). 이러한 보험은 주행시간이 적은 자가 운전자인 경우 보험료를 50% 이상 줄일 수 있는 것으로 알려져 있다(조영현·이혜은 2018). 미국의 레모네이드(Lemonade)는 챗봇을 활용하여 세입자보험 및 주택보험을 주력 상품으로 판매하고 있으며, 해당 인슈어테크 기술을 통해 보험인수, 보험금 산정, 지급 등의 절차에 소요되는 시간을 비약적으로 단축시켰다(정민기·김중한 2020). 독일 최초의 디지털 브로커인 클라크(Clark)의 경우 머신러닝을 통해 고객의 기존 보험상품을 분석 및 평가하고 고객 맞춤형 상품을 추천하는 서비스를 제공하고 있다. 해당 알고리즘은 독일 내 160개 이상의 보험회사 상품 중에서 해당 고객에게 가장 잘 맞는 보험상품을 추천하며, 고객의 요청이 있을 경우 컨설팅 서비스까지 제공하는 등 디지털 기술을 이용하여 고객의 편의성을 극대화하고 있다(조영현·이혜은 2018).

국내에서도 다수 보험사들이 적극적인 디지털 전환을 시행하고 있으며, 이는 조직개편 및 기업의 비전을 설정함으로써 나타나고 있다. 예를 들어, 삼성화재의 경우 디지털 전환 관련 컨트롤 타워 역할을 하는 디지털 본부를 새로 신설하였으며, 하나손보는 디지털 손해보험회사로 전환할 것을 공표하였다(김규동·김윤진 2021). 실제로 이러한 노력들은 〈표 Ⅱ-7, 8〉에서 확인할 수 있듯이 다양한 디지털 서비스 및 인슈어테크 적용 사례들로서 현실화 되고 있다. 앞서 언급한 해외 보험사들의 빅데이터 기술, 사물인터넷 등을 활용해서 정확한 위험평가, 맞춤형 정보 수집, 보험상품 비교플랫폼 개발 등을 진행하고 있다.

〈표 Ⅱ-6〉 전 세계 대표 인슈어테크 기업 및 기술정보 요약

분류	기업	요약
맞춤형 손해보험	중안보험(ZhongAn, 중국)	• 온라인 쇼핑으로 구매한 상품에 대해 보장하는 손해보험 상품 판매
헬스케어 및 건강보험	오스카(Oscar, 미국)	• 웨어러블 기기를 통해 개인별로 건강정보 제공 • 특정 목표 달성 시 혜택 제공(예: 금연, 몸무게 감량)
	클로버(Clover, 미국)	• 스마트폰으로 의사 상담 서비스 제공 • 약국으로 처방전 메일 발송 기능 제공 • 모바일 앱 기반 디지털 어시스턴트 서비스 제공
	리그(League, 캐나다)	• 스마트폰으로 개인에게 최적화된 건강관리 및 헬스케어 서비스 제공 • 재직 중인 회사의 복리후생과 헬스케어 업체정보 확인 가능 • 모바일 앱으로 디지털 결제 가능
	앨런(Alan, 프랑스)	• 소규모 사업자와 스타트업 대상 디지털 건강보험회사 • 온라인으로 가입 가능하며 쉽고 투명하게 보험정보 제공 • Alan map을 통해 최적의 의사 찾기 및 진료 예약 가능
판매 및 중개	컴패어유럽그룹 (CompareEuropeGroup, 영국)	• 빅데이터 기반의 보험상품 비교 플랫폼 제공 • 무료로 쉽고 빠르게 보험상품 정보를 제공하고 편리하게 가입 가능
	클라크(Clark, 독일)	• 독일 최초의 디지털보험중개회사 • 인공지능을 통해 고객의 기존 보험상품을 진단, 분석하고 최적화된 보험상품 추천
	커버 지니어스 (Cover Genius, 호주)	• 빅데이터 및 API를 이용하여 전 세계 주요 보험사의 보험상품을 실시간으로 추천, 비교분석 및 판매
	커버월렛 (CoverWallet, 미국)	• 소상공인 전용 보험상품 판매, 스마트폰 앱으로 상품 조회, 설계, 가입, 계약, 결제까지 편리하게 이용 가능
	셰파(Sherpa, 몰타)	• 빅데이터 및 인공지능 기술을 사용하여 개인 최적화된 특화보험상품 추천
자동차 보험	큐바(Cuvva, 영국)	• 스마트폰으로 차량사진 등록만으로 자동차보험 가입 가능 • 차량 운행 시에만 보험 가입 가능하고 비용 저렴
소액보험	그래스루트 (GrassRoots, 케냐)	• 보험가입이 어렵거나 소외된 계층을 대상으로 소액기반 손해보험상품 제공

자료: KPMG(2017) 및 김은석·김영준(2019)의 〈표 3〉을 참조함

〈표 Ⅱ-7〉 보험 가치사슬(value chain)과 인슈어테크(보험진단/상품기획)

가치사슬	서비스	분류	내용	보험사
보험 진단/분석	디지털 보험플랫폼	비교 플랫폼	• 가입 보험내역 실시간 확인, 자동 보장분석 및 추가 필요상품 추천	ING생명 교보생명 흥국생명
상품기획/ 설계	UBI보험	사물인터넷 빅데이터 및 소프트웨어	• 이통사 내비게이션 앱을 통해 안전운전 점수 측정. 점수에 따라 자동차보험료 할인 • 차량 내장 측정기기와 연동한 안전운전 습관 서비스를 활용하여 자동차보험료 할인 • 어플리케이션을 통해 운전자의 운전습관을 파악하고 자동차 보험료를 책정	DB손보 KB손보 현대해상 Root Insurance
	AI 기반 보험	빅데이터 및 소프트웨어	• 디지털 기술을 활용하여 보험 인수와 보험금 청구 및 사후 고객 서비스 등 오퍼레이션 모델 혁신	평안보험
	건강관리 헬스케어	사물인터넷	• 웨어러블 건강관리앱을 활용하여 건강관리 실적에 따라 각종 보험료 할인 등 제공. 당뇨 등 유병자 건강관리서비스로 확대	AIA생명 삼성화재 DB손보 교보생명
		빅데이터 및 소프트웨어	• 빅데이터를 활용해 추가 의사 진단 없이 고객 설문과 처방 기록 등을 활용하여 생명보험료 계산	Ethos
		빅데이터 및 소프트웨어	• 생명보험사는 건강 등급에 따라 보험료를 할인 • 손해보험사는 건강 나이에 따른 보험료 산출 및 적용	신한생명 ABL 생명 현대해상 DB손보

자료: 김은석·김영준(2019)의 〈표 4〉, 설태현·강대승(2020), 이재원·오상진(2020)을 참조함

〈표 Ⅱ-8〉 보험 가치사슬(value chain)과 인슈어테크(상품 조회/결제/보상청구/대출)

가치사슬	서비스	분류	내용	보험사
상품 조회/가입	보험 진단분석	비교플랫폼 디지털보험사	• 보험사 상품 조회 및 가격 비교, 가입, 결제처리	삼성생명 교보생명 신한생명
	역경매 보험 추천	비교플랫폼 디지털보험사	• 인공지능 분석 알고리즘을 활용하여 역경매 방식의 보험상품 비교 추천 제공	삼성화재 한화생명
	챗봇	디지털보험사	• 인공지능 기술을 활용한 자연어 기반 챗봇 상담서비스(상품 조회, 상품 추천, 가입, 각종 질의)	삼성생명 라이나생명 교보생명 DB손보
		디지털보험사	• 24시간 온라인 가상 응대 서비스를 운영	평안보험
보험료 결제/인증	간편결제	디지털보험사	• 이통사 간편결제 및 카카오톡 기반 간편 결제	DB손보 교보생명
	간편인증	디지털보험사	• 카카오톡 메신저 기반 간편인증 제공	DB손보 교보생명 KB손보
		디지털보험사	• 지문인증 기술을 통해 전자서명 시스템 제공	삼성생명
보상청구	실손보험 간편청구	디지털보험사	• 고객 동의하에 병원진료서류를 자동으로 보험사에 전송하는 스마트폰 앱 기반 실손보험 청구대행	KB손보 삼성화재
		디지털보험사 보험교차판매	• AI를 활용해 집주인과 세입자에게 90초 이내에 지급보험금을 확정하고 3분 내 청구 해결	Lemonade
		디지털보험사 빅데이터 및 소프트웨어 사물인터넷	• 공공데이터, 위성 사진, 스마트 홈 장치 등을 활용하여 보험 신청절차 간소화 및 청구절차 최소화	Hippo Insurance
	자동차사고 자동수리 견적	빅데이터 및 소프트웨어	• 인공지능 기반 자동차사고 수리비 자동견적 시스템	한화손보
대출	신용대출 약관대출	빅데이터 및 소프트웨어	• 빅데이터 분석 기반 대출신용평가 점수 모델링 정교화	DB손보 ING생명

자료: 김은석·김영준(2019)의 〈표 4〉, 설태현·강대승(2020), 이재원·오상진(2020)을 참조함

Ⅲ 디지털 운영리스크 분류체계

1. 개요

금융산업 내 진보하는 정보통신기술이 적용되기 시작하면서 자본시장에서 금융기업들이 경험하는 위험이 아닌 영업활동, 기업운영 측면에서의 위험환경이 변화하고 있다. 금융기업이 직면하는 운영리스크는 경영환경 전반에서 벌어지는 디지털 전환으로 인해 과거보다 불확실성이 커졌고, 그 양상과 동인에 대한 이해가 부족함에 따라 금융기업은 리스크 관리체계를 정립하는 데 큰 어려움을 겪고 있다. 운영리스크는 시장, 신용 또는 보험리스크에 비해 그 동인이 다양하고 산재되어 있어 금융기업은 프론트 오피스부터 백오피스까지 사실상 모든 업무에서 이 리스크에 노출되어 있다.

기업의 운영리스크 관리 목표는 기본적으로 기업가치의 제고에 있다. 즉, 하방리스크(downside risk)의 특성을 가지는 운영리스크를 효율적, 효과적으로 관리함으로써 잠재적 손실의 발생가능성과 크기를 줄이고, 이에 따라 잠재적 비용을 감소시킴으로써 주주가치를 높이고자 하는 노력이 운영리스크 관리체계의 목표가 된다. 이를 달성하기 위한 운영리스크 관리의 핵심은 운영리스크로부터 발생 가능한 손실 사건의 근본 원인(즉, 리스크 동인)이나 잠재적 손실사건을 인식 및 평가하는 것이다.

문제는 디지털 전환에 의한 산업 전반의 빠른 변화 양상으로 인해 리스크 동인 및 잠재적 손실사건의 양상에 대한 이해가 부족하다는 점에서 디지털 운영리스크는 이머징 리스크의 특성을 가지고 있다는 것이다(Ⅰ장 참조). 예를 들면, 기존 운영리스크에서는 내부 인적자원의 행위로부터 발생하는 손실사건이 빈번하고 큰 비중을 차지했으나, 디지털화된 사업부문에서는 과거에 비해 인적자원의 단순 오류나 실수에 의한 손실은 감소할 가능성이 있다.[18] 반면, 시스템 및 기술의 고도화로 인해 숙련되지 못한 인적자원 또는 정교화되지 못한 내부 프로세스 오류, 그리고 시스템 또는 기술 자체에서 발생할 수 있는 손실사건 등의 영향 범위와 그 비중이 과거 데이터로는 파악하기 힘든 수준으로 나타날 가능성이

18) McKinsey(2020)를 참조함

높다. 서론에서 언급했듯이, 현 바젤의 운영리스크 분류체계는 리스크의 원인을 단순히 4개의 개략적 유형으로 구분하고, 손실사건 유형의 구체화를 통해 동인에 대한 근거만 제시하기 때문에 선제적인 사전 손실 관리체계를 구축하는 데 한계가 있다.

이 장에서는 기존 바젤 Ⅱ에서 제안한 운영리스크 분류(〈표 Ⅰ-2〉 참조)를 보완하면서 Cebula and Young(2014)의 사이버 보안 운영리스크 분류를 참고하여, 디지털 운영리스크를 체계화한다.[19] 특히, 세가지 항목(대분류, 소분류, 리스크 요인)으로 분류하여 상하 관계를 구분하였으며, 그 중 가장 상위항목은 리스크 대분류(Core risk category) 명칭하에 바젤 Ⅱ에서 정의하는 핵심 리스크 동인을 구분하는 네 가지 범주(인적위험, 시스템 및 기술 실패, 내부 프로세스 실패, 외부사건)로 구성되어 있다. 두 번째 항목은 리스크 소분류(Risk sub-category)로 명명하고 각 대분류 요소별로 이질적 특성을 갖는 리스크 동인을 묶기 위한 기준점을 제공한다. 마지막 세 번째 항목인 리스크 요인(Risk factor)은 실제 디지털 전환에 의한 위험 손실사건들의 원인을 설명할 수 있는 세부요소들로 구성되어 있다. 제안한 분류체계를 바탕으로 Ⅱ장에서 기술한 은행 및 보험사의 디지털 전환 사례별 리스크 요인을 매핑하여 바젤 체계에서의 분류와 비교 분석한다. 이러한 비교는 앞서 언급한 리스크 동인 구체화 관점에서 바젤 체계의 한계를 보여준다.

본 보고서에서 제안하는 분류체계는 단순히 금융기업에게만 한정되지는 않는다. 비즈니스 모델 및 운영체계의 디지털 전환을 경험하는 어떤 기업이든 이하 분류된 요인에 의한 디지털 및 사이버 리스크에 노출되어 있다. 다만, 분류체계의 적용을 금융산업에 좀 더 초점을 맞추는 주요 이유는 금융산업의 국제 규제기준(즉, 바젤 Ⅱ)하에서 운영리스크 인식, 분류 및 관리체계가 표준적으로 사용되기 때문이다. 즉, 운영리스크는 사업을 운영하는 어떤 기업이든 일상적으로 경험하는 리스크이지만, 금융산업 규제기준의 변화에 맞춰 리스크 이해도 향상 및 대응방안 개선이 이루어지는 경향이 있다. 이하 내용은 각 분류체계를 구성하는 요소들을 간략하게 설명하고, 기존 운영리스크 체계와의 차이 및 다른 유형의 리스크와의 비교분석을 통해 디지털 운영리스크의 특성을 기술한다.[20]

---

19) 주요 참고문헌으로 활용한 Cebula and Young(2014)은 이미 디지털 및 사이버 리스크 관리에 관한 다수의 학술논문에서 리스크 분류체계의 주요 참조점으로 인용되고 있음(예를 들면, 리스크 및 보험분야에서는 Biener et al. 2015, Shetty et al. 2018, Böhme et al. 2019, Eling and Wirfs 2019를 참조, 사이버 보안분야에서는 Hahn et al. 2013, GhasemiGol et al. 2016, Humayed et al. 2017을 참조함)

20) 본 장에서 제안하는 디지털 운영리스크 분류체계는 각 요소에 대해 대략적인 소개 위주로 구성되어 있음. 해당 요소가 어떤 방식의 리스크 시나리오를 유발할 수 있는지의 여부는 소분류별 요약 표(즉, 〈표 Ⅲ-2〉, 〈표 Ⅲ-3〉, 〈표 Ⅲ-4〉, 〈표 Ⅲ-5〉)상에 예시를 제공하고 있음. 해당 분류체계는 디지털 전환으로 인해 새롭게 인식되는 운영리스크 요인이나 사이버 공간에서 발생 가능한 리스크 요인들을 이해하고 기업 내부적으로 원활한 리스크 소통(risk communication)을 제공하는 데 도움이 될 수 있을 것으로 기대함

2. 리스크 대분류(Core risk category)

가. 인적리스크(Actions of people)

이 리스크는 기업 내/외부의 개인이 초래하는 운영상 문제에서 발생할 수 있는 사건을 포괄한다. 특정 상황에서 개인의 행동이 적절하게 취해지지 않았을 때 생기는 운영리스크를 의미한다. 인적리스크에 의한 손실사건의 동인을 판단하기 위한 중요한 기준은 악의성과 의도가 포함된 사건인지 아닌지의 여부이다.

나. 시스템 및 기술 실패(Systems and technology failures)

이 리스크는 기술 자산의 비정상적, 또는 예상치 못한 오작동 등으로 인해 발생할 수 있는 사건을 포괄한다. 시스템의 복잡성이 증가할 수 밖에 없는 현 디지털 전환 양상에서는 시스템 및 기술 실패에 의한 운영리스크 손실사건 발생 횟수가 증가할 수 있으며, 특히, 급격한 디지털화를 유발하는 시장 경쟁하에서 확실하게 검증되지 않은 시스템의 상용화가 예상치 못한 손실 및 비용을 유발할 수 있다.

다. 내부 프로세스 실패(Failed internal processes)

이 리스크는 정상적으로 작동될 것이라고 기대되거나 요구되는 기업 내부의 절차(또는 과정)의 실패로 인해 발생할 수 있는 사건을 포괄한다. 앞서 시스템 및 기술 실패 리스크와 마찬가지로 급격한 디지털 전환하에 새로운 시스템 및 기술이 적용되면 기업 내부의 사용자 간 운영 프로세스상 리스크가 새롭게 관찰될 수 있다. 또한, 상용화된 디지털 금융 서비스를 통한 디지털 고객 경험 프로세스에서 실패가 발생하여 재정적 손실 및 비용 증가의 문제도 발생할 수 있다.

라. 외부사건(External events)

이 리스크는 기업의 통제 범위를 넘어서는, 외부의 예상치 못한 사건으로 인해 발생할 수 있는 내부의 사건을 포괄한다. 자연재해 및 외부 공공 서비스 실패로 인한 디지털 및 사이

버 관련 운영리스크 사건이 발생할 수 있으며, 특히 핀테크 스타트업 및 외부 디지털 서비스 공급자와의 교류가 다양화되고, 증가하면서 파트너 업체의 실패 및 공급서비스 실패 등의 문제가 새로운 리스크로서 현실화될 수 있다.

〈표 Ⅲ-1〉은 앞서 기술한 디지털 운영리스크의 4가지 대분류 유형에 관하여 요약하고 있다. 또한, 제안한 대분류 리스크 유형은 바젤 Ⅱ의 운영리스크 분류상에서도 적용되기 때문에 각 리스크 유형이 바젤 체계하에서 어떤 사건 유형을 포괄하는지도 제공하고 있다.

〈표 Ⅲ-1〉 디지털 운영리스크 대분류 유형 요약

유형	요약	기존 운영리스크하 관련 사건 유형
인적리스크 (Actions of people)	기업 내/외부의 개인에 의해서 초래되는 리스크	내부사취 외부사취
시스템 및 기술실패 (Systems and technology failures)	기술 자산에 의해서 초래되는 리스크	시스템 장애 고객, 상품, 영업실무[1)]
내부 프로세스 실패 (Failed internal processes)	기업 내부 프로세스로부터 초래되는 리스크	고용 및 사업장 안전 고객, 상품, 영업실무 집행전달, 처리절차
외부사건 (External events)	기업의 통제 범위 밖의 주체로부터 초래되는 리스크	유형자산 손실

주: 1) 디지털 전환에 따른 상품 다양화 및 고객 접점 확대 등은 디지털화된 시스템상 잠재리스크와도 연결될 수 있음

3. 리스크 소분류(Risk sub-category)와 동인분석

가. 인적리스크 하위 유형

1) 부주의 리스크(Negligent/Unintentional)

일반적으로 내부자의 실수나 의도치 않은 행위로 인해 발생 가능한 사건을 포괄한다. 이 리스크로 인한 손실사건의 경우 그 동인에 고의 또는 악의적 목적이 존재하지 않는다. 부주의 리스크하에서 손실사건을 발생시킬 수 있는 동인으로는 크게 세 가지로 분류가 가능하다.

- 실수(mistake): 업무 또는 과정을 정확히 이해하고 있는 내부자의 실수나 의도치 않은 행위로 인해 발생 가능한 사건을 포괄한다. 이 동인에 의한 손실사건의 경우 고의 또는 악의적 목적이 있는 사건은 포함하지 않는다.
- 오류(error): 업무 또는 과정에 대한 정확한 이해가 없는 내부자의 부정확한 행위로 인해 발생 가능한 사건을 포괄한다.
- 간과(omission): 내부자의 성급함으로 인해 적절한 행위를 하지 못하여 발생 가능한 사건을 포괄한다.

2) 악의 리스크(Malicious/Intentional)

내부 또는 외부자의 의도적, 악의적 목적을 달성하기 위해 발생한 행위로 인해 초래되는 사건을 포괄한다. 부주의 리스크와의 차이는 리스크를 유발하는 행위의 악의성 또는 부정적 의도성이 존재하는지 여부이다.

- 사기/기만(fraud): 기업을 희생양으로 하여 자신이나 협력자에게 이익을 주기 위해 취한 고의적 행동으로 인해 발생 가능한 사건을 포괄한다.
- 방해/교란(sabotage): 기업 자산이나 프로세스에서 실패를 유발하는 고의적인 행동을 취하는 경우, 일반적으로 대상 주요 자산에 대해 접근 권한을 가진 사람이나 내부 소유자의 의도적 행위에 의해 발생 가능한 사건을 포괄한다.
- 절도/파손(theft/vandalism): 기업 자산, 특히 정보 자산의 의도적이고 무허가 취득, 또는 기업 자산의 의도적인 손상(혹은 임의적 손상)에 의해 발생 가능한 사건을 포괄한다.

3) 무위 리스크(Inaction)

내부자의 경험 부족이나 무지 또는 적절한 인력배치 실패로 인해 발생 가능한 사건을 포괄한다.

- 기술 부족(unskillful): 업무 담당자에게 필요한 행동 수행 능력 부족으로 인해 발생 가능한 사건을 포괄한다.

• 상황판단 부족(unknowledgeable): 행동 필요성에 대한 개인의 무지로 인해 발생 가능한 사건을 포괄한다.

• 지도 부족(lack of guidance): 적절한 방향지도의 결여로 인해 발생 가능한 사건을 포괄한다.

• 인적자원 부족(lack of resources): 작업을 수행하는 데 필요한 적절한 자원을 사용할 수 없거나 존재하지 않음으로 인해서 발생 가능한 사건을 포괄한다.

〈표 Ⅲ-2〉 인적리스크 유형하 리스크 동인 분류 요약

소분류	리스크 동인	관련 리스크 사건 잠재유형
부주의 리스크 (negligent/ unintentional)	실수(mistake)	• 로컬 관리자 권한을 가진 직원이 보안 솔루션을 실수로 비활성화할 경우, 비활성화된 컴퓨터로부터 기업 전체로의 감염 확산 가능
	오류(error)	
	간과(omission)	
악의 리스크 (malicious/ intentional)	사기/기만(fraud)	• 해킹, 랜섬웨어 등과 관련한 사건은 모두 포함됨. 내부 직원이 외부인에게 접근권한을 부여하여 기밀 정보가 유출될 수 있음
	방해/교란(sabotage)	
	절도/파손 (theft/vadalism)	
무위 리스크 (inaction)	기술 부족(unskillful)	• 빅데이터가 활성화됨에 따라 외부 데이터 정보를 활용하는 빈도가 증가하는 추세. 외부 데이터 관리는 내부 데이터 관리 노하우만으로 검증하는 데 한계가 있음
	상황판단 부족 (unknowledgeable)	
	지도 부족 (lack of guidance)	
	인적자원 부족 (lack of resources)	

나. 시스템 및 기술 실패 하위 유형

1) 하드웨어 리스크(Hardware risk)

그 원인을 추적할 수 있는 물리적(또는 유형의) 장치에서 발생한 오류로 인해 초래될 수 있는 사건을 포괄한다.

- 생산능력 결여(lack of capacity): 장비의 부족한 생산능력으로 인해 주어진 정보량이나 부하를 처리할 수 없음으로 발생 가능한 사건을 포괄한다.
- 수행능력 결여(poor performance): 장비의 수행능력이 부족하여 허용된 하드웨어 생산능력 내에서 지침 또는 프로세스 정보를 완료할 수 없는 경우 발생 가능한 사건을 포괄한다.
- 관리 부족(lack of maintenance): 장비의 권장 유지보수를 수행하지 않아, 하드웨어의 능력이 하락함으로 인해 발생 가능한 사건을 포괄한다.
- 수명 초과(obsolescence): 권장 수명을 초과한 장비를 사용함으로 인해 발생 가능한 사건을 포괄한다.

2) 소프트웨어 리스크(Software risk)

모든 종류의 소프트웨어 자산(프로그램, 어플리케이션, OS 등)으로부터 발생 가능한 사건을 포괄한다.

- 호환성 문제(incompatibility): 사용하는 두 개 이상의 소프트웨어가 함께 작동되지 않아 발생할 수 있는 사건을 포괄한다.
- 환경설정 문제(configuration management error): 해당 소프트웨어의 설정 및 매개변수의 부적절한 적용 및 관리로 인해 발생할 수 있는 사건을 포괄한다.
- 설정변경 문제(change control issue): 내부 프로세스에 의해 사용하는 소프트웨어의 설정이 변경 되었을 때, 해당 변경 사항으로 인해 발생할 수 있는 사건을 포괄한다.
- 보안 취약성(security weakness): 사용하는 소프트웨어 내 제한적인 보안 설정 혹은 부

적절한 적용으로 인해 발생할 수 있는 사건을 포괄한다.

- 테스트 문제(testing issue): 응용 프로그램 및 프로그램의 설정에 대해 불충분한 테스트 및 이례적인 테스트로 인해 발생할 수 있는 사건을 포괄한다.
- 프로그래밍 설계(coding practice issue): 구문에 의한 프로그래밍 오류를 포함, 코딩 시 보안 코딩 관행을 따르지 않아 발생할 수 있는 사건을 포괄한다.

3) 시스템 오류 리스크(System errors risk)

정상적으로 작동될 것이라고 기대되는 통합 시스템상에서의 실패로 인해 발생 가능한 사건을 포괄한다.

- 시스템 부적합성(design error/unsuitability): 프로그램 사용 시 시스템이 제대로 적합되지 않아서 발생할 수 있는 사건을 포괄한다.
- 개발소통 부족(lack of specification): 부적절한 요구사항 또는 요구사항의 불충분한 정의 등으로 인한 요구사항 준수 실패로 인해 발생할 수 있는 사건을 포괄한다.
- 상호운용성 결여(integration failures): 시스템 내의 다양한 구성 요소가 함께 기능하지 못하거나 올바르게 접속하지 못해서 발생할 수 있는 사건을 포괄한다.
- 시스템 복잡성(complexity): 시스템 복잡성 또는 과다 구성 요소로 인해 발생할 수 있는 사건을 포괄한다.

〈표 Ⅲ-3〉 시스템 및 기술 실패 유형하 리스크 동인 분류 요약

소분류	리스크 동인	관련 리스크 사건 잠재유형
하드웨어 리스크 (Hardware risk)	생산능력 결여 (lack of capacity)	• 빅데이터를 활용한 데이터 분석 업무를 진행 혹은 딥러닝을 활용한 서비스를 구현 시, 방대한 양의 데이터 크기에 비해 데이터를 처리할 수 있는 컴퓨터의 성능이 떨어지는 경우
	수행능력 결여 (poor performance)	
	관리 부족 (lack of maintenance)	
	수명 초과 (obsolescence)	
소프트웨어 리스크 (Software risk)	호환성 문제 (incompatibility)	• 새로운 프로그램을 도입할 때, 기존 프로그램과 호환성 충돌 문제가 발생하여, 서비스 제공이 중단될 수 있음 • 기업에서 새로운 서비스를 출시하기 전에 충분한 테스트를 진행하지 않아, 실제 서비스가 제공 되었을 때 예상치 못한 오류가 발생할 수 있음
	환경설정 문제 (configuration management error)	
	설정변경 문제 (change control issue)	
	보안 취약성 (security weakness)	
	테스트 문제 (testing issue)	
	프로그래밍 설계 (coding practice issue)	
시스템 오류리스크 (System errors)	시스템 부적합성 (design error)	• 회사 간 합병 과정에서 시스템 정책 혼선이 발생하거나, 데이터베이스 간 통합이 부적합하여 잘못된 업무가 발생하는 경우(예, 고객 예금의 잘못된 계좌로 입금)
	개발소통 부족 (lack of specification)	
	상호운용성 결여 (integration failures)	
	시스템 복잡성 (complexity)	

다. 내부 프로세스 실패 하위 유형

1) 프로세스 설계 리스크(Process design or execution risk)

부적절한 설계로 인해 목적달성에 실패한 프로세스가 발생시킬 수 있는 사건을 포괄한다.

- 처리절차 실패(process flow failure): 프로세스 결과물을 처리하는 과정에서 잘못된 설계로 인해 발생할 수 있는 사건을 포괄한다.
- 설명 부족(insufficient process documentation): 프로세스 투입값, 출력물, 흐름 등 이해 당사자에 대한 불충분한 문서로 인해 발생할 수 있는 사건을 포괄한다.
- 역할의 불명확성(unclarity in roles and responsibilities): 프로세스 이해당사자들 간의 역할과 책임감에 대한 정의와 이해가 충분히 논의되지 않아 발생할 수 있는 사건을 포괄한다.
- 소통 실패(notifications and alerts failures): 프로세스 내에서 발생할 수 있는 문제에 대해 미공시/부적절한 알림 등으로 인해 발생할 수 있는 사건을 포괄한다.
- 의견불일치(service level disagreements): 서비스 기대치에 대한 프로세스 이해당사자 간의 의견 불일치로 인해 발생할 수 있는 사건을 포괄한다.
- 인수인계 실패(task hand-off failures): 프로세스 내의 업무에 대해 비효율적인 인수인계로 인해 발생할 수 있는 사건을 포괄한다.

2) 프로세스 통제 리스크(Process controls risk)

형편없는 시행, 부적합한 통제로 인한 프로세스 운영상 실패 등으로부터 초래될 수 있는 사건을 포괄한다.

- 검토의 부적절성(status monitoring failures): 프로세스 운영에 대한 통상적 정보의 부적절한 검토 또는 대응으로 인해 발생할 수 있는 사건을 포괄한다.
- 측정 오류(metrics error): 시간에 따른 프로세스 수행능력 측정 실패로 인해 발생할 수 있는 사건을 포괄한다.

- 주기적 검토 실패(periodic review failures): 프로세스 실행에 대한 검토 부족으로 인해 필요한 변경을 수행하지 않아 발생할 수 있는 사건을 포괄한다.
- 행정적 실패(process ownership failures): 프로세스에 대한 잘못된 소유권 정의 또는 잘못된 거버넌스 관행으로 인해 예상 결과를 제공하지 못하는 프로세스로부터 발생할 수 있는 사건을 포괄한다.

3) 프로세스 지원 리스크(Supporting process risk)

기업 내 적절한 자원을 지원하는 프로세스의 실패로 인해 발생 가능한 사건을 포괄한다.

- 재정지원 결여(funding issue): 적절한 재정 자원이 제공되지 않아 발생할 수 있는 사건을 포괄한다.
- 조달 실패(procurement failures): 영업 지원에 필요한 적절한 구매 서비스와 상품을 제공하지 못해 발생할 수 있는 사건을 포괄한다.

〈표 Ⅲ-4〉 내부 프로세스 실패 유형하 리스크 동인 분류 요약

소분류	리스크 동인	사례
프로세스 설계리스크 (Process design risk)	처리절차 실패 (process flow failures)	• 지나치게 민감한 사이버 보안 알림 시스템을 사용하는 경우, 악성 공격일 가능성이 낮거나 실제로 양성인 활동과 일치할 가능성이 낮은 이벤트에 대해 과도하게 경고할 수 있음. 이로 인해 불필요한 비용이 발생할 수 있음
	설명 부족 (insufficient process documentation)	
	역할의 불명확성 (unclarity in roles and responsibilities)	
	소통 실패 (notifications and alerts failures)	
	의견불일치 (service level disagreements)	
	인수인계 실패 (task hand-off failures)	
프로세스 통제리스크 (Process controls risk)	검토의 부적절성 (status monitoring failures)	• 신 모델을 구현할 때, 모델 검증에 사용되는 여러 지표들(F1 score, recall, prediction 등) 중 데이터에는 맞지 않는 지표를 사용하여 잘못된 결과를 도출할 가능성이 존재함
	측정 오류 (metrics error)	
	주기적 검토 실패 (periodic review failures)	
	행정적 실패 (process ownership failures)	
프로세스 지원리스크 (Supporting process risk)	재정지원 결여 (funding issue)	• 새로운 소프트웨어 업데이트 적용 불가로 인한 특정 컴퓨터 시스템 다운 등으로 기업휴지/사업방해 비용 발생이 가능함
	조달 실패 (procurement failures)	

라. 외부사건 하위 유형

1) 재난 리스크(Natural or man-made risk)

자연적 손인(natural perils) 또는 인적 손인(man-made perils)에 의해서 초래되는 요인들로 인해 발생 가능한 재난적 규모의 사건을 포괄한다.

- 날씨 리스크(weather events): 비, 눈, 토네이도 또는 허리케인과 같은 악천후 상황으로 인해 발생할 수 있는 사건을 포괄한다.
- 화재 리스크(fire events): 시설 내 화재 또는 시설 외부화재로 인한 장애가 원인이 되어 발생할 수 있는 사건을 포괄한다.
- 홍수(폭우) 리스크(flood/rainfall events): 시설 내의 물난리 또는 시설 외부의 홍수로 인한 붕괴가 원인이 되어 발생할 수 있는 사건을 포괄한다.
- 지진 리스크(earthquake events): 지진에 의한 조직 운영의 붕괴로 인해 발생할 수 있는 사건을 포괄한다.
- 사회불안 리스크(unrest): 시민 장애, 폭동 또는 테러 행위 등으로 인한 운영 중단에 의해 발생할 수 있는 사건을 포괄한다.
- 전염병 리스크(pandemic): 조직 운영을 방해하는 광범위한 의료 마비 상태(전염병)로 인해 발생할 수 있는 사건을 포괄한다.

2) 법적 리스크(Legal affairs)

기업에 잠재적으로 영향을 끼칠 만한 법적인 요인들로 인해 발생 가능한 사건을 포괄한다.

- 규정 위반(regulatory compliance): 디지털 전환과 관련한 정부의 새 규정 또는 기존 규정을 준수하지 않아 발생할 수 있는 사건을 포괄한다.
- 신규 법률(legislation): 디지털화된 서비스, 데이터 관리 등 기업의 디지털 전환에 영향을 끼치는 새로운 법률에 의해 발생할 수 있는 사건을 포괄한다.
- 소송(litigation): 직원과 고객을 포함한 모든 이해관계자가 조직에 대해 취한 법적 조치로 인해 발생할 수 있는 사건을 포괄한다.

3) 경영 리스크(Business affairs)

외부 공급자, 시장 상황, 거시경제적 여건 등에서의 문제로 인해 필요한 정보기술 자산 부족이 초래할 수 있는 사건을 포괄한다.

- 공급자 실패(supplier failures): 필요한 제품 또는 서비스를 기업에 제공하는 공급업체의 일시적 또는 영구적 무능력으로 인해 발생할 수 있는 사건을 포괄한다.
- 시장 경쟁력 결여(competitive disadvantage): 디지털 전환을 통해 고도화된 제품 또는 서비스가 기술적 열위로 시장 경쟁력이 낮아져서 발생할 수 있는 사건을 포괄한다.
- 외부 자금조달 실패(financing failures): 운영에 필요한 자금을 충분히 얻을 수 없어 발생할 수 있는 사건을 포괄한다.
- 거래상대방 실패(counterparty failures): 거래상대방(국외 또는 국내)의 결제, 이체, 오픈뱅킹 등의 시스템 장애/결함 등으로 서비스가 제공되지 않아 발생할 수 있는 사건을 포괄한다.

4) 제3자(교류) 리스크(Third-party involvement or service dependency)

사업운영의 계속성을 위한 제3자와의 필수적인 교류로부터 발생 가능한 사건을 포괄한다.

- 사회인프라 실패(critical infrastructure failures): 기업의 전력 공급, 급수 또는 통신 서비스의 고장으로 인해 발생할 수 있는 사건을 포괄한다.
- 공공서비스 실패(public service failures): 화재, 경찰, 응급 의료 서비스와 같은 공공 대응 서비스에 대한 의존성으로 인해 발생할 수 있는 사건을 포괄한다.
- 연료 공급 실패(fuel supply failures): 외부 연료 공급 장치 고장(예를 들어, 백업 발전기 전원 공급 장치)으로 인해 발생할 수 있는 사건을 포괄한다.
- 운송 시스템 실패(transportation failures): 외부 운송 시스템의 고장으로 인해 발생할 수 있는 사건을 포괄한다.

〈표 Ⅲ-5〉 외부사건 유형하 리스크 동인 분류 요약

소분류	리스크 동인	사례
재난 리스크 (Natural/ man-made perils)	날씨 리스크 (weather events)	• COVID-19과 같이 갑작스런 전염병으로 인해, 비대면 계좌 신규 거래가 증가하면서 과부하가 발생 • 이로 인한 전산 장애, 금융 거래 대량 발생에 의해 거래로그의 실시간 수집 및 탐지/분석 지연
	화재 리스크 (fire events)	
	홍수(폭우) 리스크 (flood/rainfall events)	
	지진 리스크 (earthquake events)	
	사회불안 리스크 (unrest)	
	전염병 리스크 (pandemic)	
법적 리스크 (Legal affairs)	규정 위반 (regulatory compliance)	• 정부 기관이 사이버 보안에 대한 보안 정책 및 표준, 관행을 강화하면서 해당 법안을 만족시키기 위해 추가적인 비용이 발생할 수 있음
	신규 법률 (legislation)	
	소송 (litigation)	
경영 리스크 (Business affairs)	공급자 실패 (supplier failures)	• 클라우드 사업자의 정보 보호 안정성의 저하로 인해 악성 코드 유입 및 정보 유출이 발생할 수 있음
	시장 경쟁력 결여 (competitive disadvantage)	
	외부 자금조달 실패 (financing failures)	
	거래상대방 실패 (counterparty failures)	
제3자(교류) 리스크 (Thirdparty involvment/ service dependency)	사회인프라 실패 (critical infrastructure failures)	• 외부 공공 와이파이(즉, 정부기관/지자체에서 운영하는 와이파이)를 사용하여 접속하는 고객, 또는 임직원을 통해 외부 해킹 발생 가능
	공공서비스 실패 (public service failures)	
	연료 공급 실패 (fuel supply failures)	
	운송 시스템 실패 (transporation failures)	

4. 기존 운영리스크 체계와의 차이점 고찰: 디지털 전환 사례 매핑

〈표 Ⅰ-2〉에서 볼 수 있듯이, 바젤 Ⅱ에서 규정하는 운영리스크는 크게 4가지 손실 원인에 의한 7가지의 손실 사건 유형과 그 하위 유형으로서 20가지로 분류된다. 4가지 손실 원인은 본 보고서의 대분류 리스크 유형과 동일하며, 20가지의 사건 분류는 손실데이터를 7가지의 상위 유형으로 구분하기 위해 세분화되어 있다. 손실사건 중심으로 유형이 분류되어 있다는 점은 운영리스크에 의한 잠재적 손실을 방어하기 위한 자기자본 산출 편의성을 위한 것으로, 기존 손실 데이터를 사건 특성에 따라 분류함으로써 통계적 특성에서의 이질성을 고려한다. 즉, 8가지 사업유형에 7가지의 손실사건 유형을 적용하여 56개의 손실 측정단위를 설정하고 각각에 대해 통계적 방법론을 적용한다.

반면, 본 보고서는 전사적 리스크 관리체계 관점에서 잠재적 손실사건의 억제 또는 통제의 효율성 제고, 리스크 커뮤니케이션 제고 등의 목표하에 기존 참고문헌을 기반으로 디지털 운영리스크 분류체계를 제안하고 있다. 53가지의 세분화된 리스크 동인은 디지털 전환을 통해 사업 및 업무영역 전반의 디지털화에서 발생 가능한 리스크 유형을 설명하고, 세부 행동수칙을 개발하는 데 활용이 가능하다. 세부 행동수칙을 발전시키는 것은 핵심리스크 인자(Key Risk Indicators; KRI)를 통해 리스크 수준 계량화 및 리스크 커뮤니케이션의 효율성 제고 등으로 이어질 수 있다(〈표 Ⅲ-6〉 참조).

〈표 Ⅲ-6〉 기존 바젤 운영리스크 분류(사건유형)와의 비교

구분	바젤 운영리스크 유형분류	디지털 운영리스크 유형분류
분류체계	손실사건 중심 유형분류	리스크 동인 파악 중심 유형분류
대분류	4가지 손실원인 유형	4가지 리스크 유형
소분류	7가지 손실사건 유형	13가지 리스크 하위 유형
리스크 요인/동인	20가지 세부 손실사건 유형	53가지 리스크 동인
차이점	• 바젤에 의한 분류는 손실사건을 기준으로 자기자본 산출 활용에 초점(사업 유형에 따라 56개의 측정단위로 자기자본 추정량 산출) • 제안된 디지털 운영리스크 분류체계는 바젤에서 규정한 4가지 리스크 원인을 대분류로 하여 리스크 소분류(13가지)와 53가지의 동인을 세분화 • 리스크 동인의 세부적 분류를 통해 전사적 디지털 운영리스크 관리체계 확립을 위한 세부 행동수칙 개발의 효율성 제고	

또한, 기존 운영리스크 체계에서는 디지털화와 관련하여 추상적으로 규정된 유형을 발생 가능한 몇가지 동인으로 세분화하여 관리추적이 가능하도록 하고 있다. 예를 들면, 20가지의 손실 사건 유형 중 사이버 보안 또는 디지털 보안과 관련한 유형이 시스템 보안으로 통합되어 분류되어 있으나, 본 보고서의 분류체계는 하드웨어, 소프트웨어 및 시스템 자체 오류 가능성까지 세분화하여 파악이 가능하도록 구성되어 있다. 이는 기존 체계가 손실추정 목적의 분류체계로서의 한계점을 가지고 있고, 디지털 전환에 따른 리스크 환경변화를 반영하기 힘든 구조로 되어 있음을 시사한다.

그렇다면 금융기관의 디지털 전환 양상이 이 장에서 제안한 디지털 운영리스크 분류체계와 어떻게 연결될 수 있으며, 바젤 운영리스크 분류체계와는 어떤 차이가 존재할까? 〈부록 표 Ⅰ-1, 2, 3〉은 앞서 Ⅱ장에서 기술한 은행의 각 데스크별 디지털 전환 사례(〈표 Ⅱ-2, 3, 4〉 참조)를 중심으로 현재 산업의 디지털 변화와 디지털 운영리스크 분류체계 중 소분류 및 리스크 요인 간 관계성을 살펴본 결과이다. 〈부록 표 Ⅰ-4, 5, 6〉은 보험회사들의 디지털 전환 사례별 디지털 운영리스크 요인으로의 관계성을 살펴보았다. 디지털 전환 사례와 운영리스크 요인 간 매핑은 인적위험보다는 시스템 및 기술 실패, 내부 프로세스 실패 중심으로 기술 및 기술 적용 측면의 리스크 발생 가능성에 초점을 맞추었다.[21] 대부분의 디지털 기술 적용 사례에서 소프트웨어 및 시스템 오류 리스크(시스템 및 기술 실패 항목)에 노출될 가능성이 가장 높으며, 새로운 기술의 전사적 적용에 따른 내부 프로세스상의 잠재적 문제(개발소통 부족, 처리절차 실패, 검토의 부적절성 등)가 존재할 수 있다.

이 장에서 특히 초점을 맞추어 논의하고자 하는 내용은 바젤 운영리스크 분류체계와의 차이점이다. 〈부록 Ⅰ〉에 제시된 표에는 바젤 분류체계 기준 매핑 결과와 함께 두 분류체계 간 비교가 가능하도록 하였다. 〈표 Ⅲ-6〉에서 알 수 있듯이, 바젤 분류체계의 경우 제안된 디지털 운영리스크 분류체계와 달리 소분류-리스크 요인 항목이 따로 명시되어 있지 않아, 손실유형 및 하위유형을 이에 대응하는 분류요인으로 판단하였다. 디지털 리스크 관점에서 두 분류체계 간 가장 큰 차이는 시스템 및 기술 실패에 따른 세부 리스크 유형을 판단할 요인의 유무이다. 본 보고서의 분류체계의 경우 소프트웨어 및 하드웨어, 시스템 오류 리스크 분류하 다양한 형태의 디지털/사이버 시스템상 발생 가능한 손실 동인 판단이 가능한 반면, 바젤 체계의 경우 '시스템 장애' 요인으로 포괄적 분류만 가능하다.

21) 본 장에서 제시한 디지털 전환 사례와 운영리스크 분류체계 간 매핑 결과는 본 보고서의 평가에 따른 결과이므로, 분류체계를 바라보는 조직별 디지털 전환 특성 및 실제 적용 사례에 따라 매핑의 결과는 달라질 수 있음

이에 더하여, 제안된 분류체계에서는 개발소통 부족 및 프로세스 모니터링과 관련한 리스크 요인들이 세분화되어 있어 내부 프로세스상에서 발생할 수 있는 리스크들을 보다 정교하게 관리함으로써 리스크 커뮤니케이션의 효율성을 향상시키는 데 도움이 될 수 있으나, 바젤 체계의 경우 '모니터링과 보고' 항목으로 손실유형이 단순화 되어 있다. 마지막으로, 본 보고서의 분류체계와는 다르게 바젤 체계에서는 시장 경쟁력 결여나 신규 규정/법률에 관한 리스크 등은 고려하지 않는다. 이는 빅테크 기업들의 금융서비스 시장 진출 및 신기술 적용에 따른 새로운 규제 발전/적용, 법적 분쟁 등의 문제들이 예상됨에도 불구하고, 전사적 운영리스크(또는 전사리스크; enterprise risk) 관점에서 전략, 평판, 법적 리스크를 배제하고 있는 바젤 체계의 한계를 보여준다. 본 보고서에서 제안한 분류체계가 이러한 잠재적 리스크 요인들을 사전에 관리 가능하도록 시스템을 구축하는 데 일부 근거를 제공할 수 있을 것으로 기대한다.

5. 다른 유형의 리스크와 디지털 리스크 간 비교

이번에는 디지털 운영리스크와 보험시장에서 보장하는 대표적인 리스크들과의 차이점을 살펴보고자 한다. 운영리스크와 보험시장에서 보장하는 리스크는 기본적으로 하방리스크(downside risk)로서의 공통점을 가진다. 따라서, 리스크의 특성에서 유사한 점이 많고, 리스크 관리 측면에서 동일 또는 유사 전략을 통해 통제가 가능하다. 〈표 Ⅲ-7〉은 Eling and Wirfs(2016)를 참고하여 보험시장에서 다뤄지는 리스크 중 대표적으로 재물, 책임, 재해리스크와 일반적으로 인식되는 기업의 운영리스크, 디지털 운영리스크를 7가지 관점에서 비교하고 있다.

재물리스크와 책임리스크는 국내시장에서 자동차, 주택화재, 배상책임 등의 다양한 보험상품을 통해 보장이 되고 있다. 즉, 부보 가능성이 높고, 데이터가 충분하기 때문에 보험회사가 시장성을 담보받을 수 있으며, 기본적으로 경쟁시장의 특성을 보인다. 재물리스크의 경우 손실에 대한 보상이 이루어지기까지의 기간이 상대적으로 짧은 short-tail 특성을 보이고, 책임리스크의 경우 배상책임이 결정된 이후 보상이 이루어지기 때문에 상대적으로 긴 long-tail 특성을 보인다. 재해리스크는 재물 및 책임리스크를 보장하는 기존 보험상품을 통해서 일부 보장이 가능하나, 국내시장에서는 태풍, 홍수 등의 재해로 인한 손실에 초점을 맞춘 농작물재해보험 등을 통해 보장이 이루어지고 있는데, 통상적으로 재물리

스크와 같이 short-tail 특성을 보여준다.

일반적인 운영리스크와 디지털 운영리스크의 경우 데이터 유출과 같이 배상책임으로 이어지는 손실사건이 존재하고, 상대적으로 고빈도-저심도의 손실 유형도 포괄하고 있어 short-tail과 long-tail 특성 모두 가지고 있다. 위험대상 측면에서는 재물리스크, 재해리스크가 대체적으로 피해기업(또는 개인) 당사자에게 발생하는 경우가 많고, 책임리스크는 제3자에게 손실이 발생했을 때 보장이 이루어진다. 운영리스크는 피해 당사자와 제3자 모두에게 손실이 발생하는 경우를 포함하고 있다는 점에서 다른 리스크들과 차이점을 가진다.

〈표 Ⅲ-7〉 다른 유형의 리스크와 비교

구분	재물리스크	책임리스크	재해리스크	일반 운영리스크	디지털 운영리스크
손실보상 기간	short-tail	long-tail	short-tail	short & long-tail	short & long-tail
위험대상	당사자 (first party)	제3자 (third party)	당사자	당사자 및 제3자	당사자 및 제3자
손실 빈도	고빈도	고빈도[1)]	저빈도	저빈도 및 고빈도	저빈도 및 고빈도
손실 심도	저심도 및 고심도	저심도 및 고심도	고심도	저심도 및 고심도	저심도 및 고심도
측정가능성	높음	중간 (과거사례 가용 여부에 따라)	중간 (재해 종류에 따라)	중간 (손실자료 가용 여부에 따라)	낮음
상호연결성	중간 (위험 유형에 따라)	중간[2)]	높음	낮음	중간 (위험 유형에 따라)
표준화 가능성[3)]	높음	높음	높음	중간	낮음

주: 1) 국내시장에서 일반배상책임이나 자동차과실 배상책임보험의 경우 손실의 고빈도 특성을 나타냄
2) 예를 들어 손실의 빈도가 높은 자동차과실 배상책임보험의 경우, 단일 손실사건으로 인해 다수의 배상책임이 발생할 가능성이 충분히 존재함
3) 표준화 가능성(standardization)은 정의(definition)와 보장범위(coverage)로 구분하여 판단이 가능하나 여기서는 본 보고서의 분류체계 목적에 따라 정의에 대해서 수준을 평가함

자료: Eling and Wirfs(2016)의 〈Table 3〉을 재구성함

손실의 빈도와 심도 관점에서는 운영리스크가 다양한 빈도의 손실 유형을 포괄하고 있어 다른 리스크들에 비해 넓은 스펙트럼을 내재하고 있고, 심도 측면에서도 다양한 크기의 손실 유형을 포괄하고 있다. 위험사건에 의한 비용 및 잠재적 손실의 영향에 관한 측정가능성에 있어서 디지털 운영리스크는 다른 리스크 유형 및 일반적인 운영리스크와 달리 과거 사례, 손실자료 등이 불충분하고, 이머징 리스크로서 정의, 분류의 불명확성과 모형의 부재 등으로 측정이 어렵다는 문제를 가진다. 특히, 디지털 환경 또는 사이버 네트워크상의 초연결성(hyperconnectivity)으로 인해 손실사건 간의 연결성 또는 위험요인 간의 연결성이 매우 높다는 점에서 시스템 리스크(systemic risk)의 성질을 가지고 있다.

마지막으로, 보험상품화를 평가할 시장성 측면에서는 위험 인수절차에서의 표준화 작업이 중요한 과정 중 하나인데, 디지털 운영리스크는 그 유형 및 범위가 넓어 표준화가 쉽지 않은 특징을 가지고 있다. 이와 같이 다른 유형의 리스크와 비교분석을 통해 디지털 운영리스크의 특성을 판단하고, 리스크 관리에 있어서 전략의 다양화 및 고도화를 생각해볼 수 있다. 일반적으로 운영리스크 관리 전략은 리스크통제자가진단(Risk & Control Self Assessment; RCSA)을 통해 손실 사전관리 시스템(pre-loss management)을 구축하여 시행하고 있으나, 디지털 운영리스크는 이머징 리스크의 특성을 가진다는 점에서 전략의 다양화가 필요하다. 다음 장에서는 디지털 운영리스크의 잠재 손실 빈도와 심도를 기반으로 유형을 구분하여 그에 맞는 리스크 관리 전략에 대해 논의한다.

Ⅳ 사례분석 및 이론적 고찰

1. 개요

앞서 금융산업, 특히 은행과 보험사 입장에서 현재 진행되고 있는 디지털 전환의 양상들을 사례를 통해 살펴보고, 이러한 변화에서 파생될 수 있는 운영리스크 요인들을 체계적 관점에서 분류하였다. 제안된 분류체계는 Ⅲ장에서 언급하였듯이 디지털 리스크 관리체계를 위한 참조점으로서 세부적인 업무 조치계획들을 발전시키고, 최적의 리스크 관리 수단을 구성하여 잠재적 손실들을 억제하는 데 도움이 될 수 있다.

문제는 앞서 기술한 다양한 리스크 요인들에 의한 손실사건의 발생확률과 규모를 억제하는 것이 중요하지만, 좀 더 효율적이고 효과적인 관리체계를 구축하기 위해서는 영향력이 큰 손실을 유발할 수 있는 리스크 요인들을 고려하여 통제 역량을 집중할 필요도 있다. 발생 빈도가 적고, 영향력도 적은 유형의 손실사건에 통제 역량을 집중하는 것은 비용적으로 효율적이지 않고, 발생 빈도가 높지만 영향력은 적은 유형 또한 적절한 자기보호(self-protection) 기제의 활용을 통해 억제가 가능하다. 사이버 공격의 경우 과거에 비해 그 빈도가 압도적으로 증가하였는데, 예를 들어, 호주 사이버 보안 센터(The Australian Cyber Security Centre)가 2020~2021년 기간 동안의 사이버 공격 보고 횟수를 종합한 결과, 매 8분마다 한 건의 공격시도가 발생하였다는 사실을 확인하였다(Hurst 2021). 이러한 압도적 발생 횟수에도 불구하고, 다수의 공격이 소득 없는 시도에 그치거나, 시스템적 영향력을 가질만한 주체(예를 들면, 국가 또는 국경 없는 해커그룹)의 공격은 드물다.

이 장에서는 금융기업에서 관심을 가지고 통제 역량을 집중할 필요가 있는 고빈도-고심도 및 저빈도-고심도 손실유형의 잠재적 디지털 리스크 시나리오를 소개하고, 최적 관리 수단에 관한 이론적 배경을 고찰하고자 한다. 이론적 배경은 리스크 관리 및 보험 이론의 기본적 토대를 이루는 리스크 관리 전략에 관한 것으로 손실 빈도와 심도에 따라 리스크 보유, 통제, 전가, 회피 전략 중 최적 수단 또는 조합에 관한 고찰을 포함한다. 특히, 이를 기반으로 도출된 리스크 전가 전략으로서의 기업 보험 활용 가능성을 살펴보기 위해 디지털 운영리스크의 부보 가능성을 평가하고, 디지털 운영리스크 관리의 현실적 대안을 고찰해 보도록 한다.

2. 사례분석

이 장에서는 디지털 리스크에 의한 손실 빈도(frequency)와 심도(severity)에 따른 이하 네 가지 유형 중 금융기관에서 더 많은 역량을 투입할 유형(고빈도-고심도 및 저빈도-고심도)의 손실 시나리오들을 몇 가지 간략하게 소개하고자 한다.

- 저빈도-저심도(low frequency – low severity; LFLS) 유형
- 고빈도-저심도(high frequency – low severity; HFLS) 유형
- 저빈도-고심도(low frequency – high severity; LFHS) 유형
- 고빈도-고심도(high frequency – high severity; HFHS) 유형

손실 빈도와 심도에 따라 유형을 분류하여 사례를 판단하는 것은 리스크 관리 전략 및 수단의 최적 선택과 전사적 리스크 관리체계 확립 측면에서 효율적일 수 있다. 즉, 이를 뒷받침하는 이론적 배경을 기반으로 각 유형별로 리스크 보유, 통제, 전가, 회피 전략 중 저비용-고효율 전략을 선택하여 리스크 통제경감방안으로서 활용할 수 있다.

가. 저빈도-고심도(LFHS) 유형 시나리오[22)]

- 증권 거래소 네트워크 교란: 악의적 형태의 사이버 공격으로 인해 거래소 네트워크 교란이 발생함으로서 거래 청산이 정상적으로 이루어지지 않아 다수의 거래자들의 재정비용이 발생할 수 있다.
- 랜섬웨어로 인한 운영중단: 악의적 랜섬웨어 공격으로 인해 피해기업 내부망의 마비가 발생하여 사업의 지속성이 불가능한 상황이 도래하는 경우이다. 2020년 11월 이랜드의 경우 랜섬웨어 공격으로 인해 일부 점포의 휴점이 발생하였고, 이로 인한 사업휴지(business interruption) 비용이 상당할 것으로 추정된다.
- 클라우드 공급자 실패 또는 사용자 실패: 디지털 전환을 통한 수집 데이터 양이 급격히 증가하면서 외부 클라우드 시스템을 통한 데이터 관리 수요가 높아지고 있다. 클라우드 시스템의 서버 설정 오류와 같은 공급자의 실패가 발생하거나, 고객의 계정관리 실패

22) 이하 저빈도-고심도 및 고빈도-고심도 유형 시나리오는 Kaffenberger and Kopp(2019)를 참조함. 〈표 Ⅳ-1〉은 두 유형의 다양한 시나리오를 요약함

문제가 발생할 수 있는데, 일례로 2019년 7월 미국 대형 은행인 Capital One에서 외부 클라우드 서비스 AWS에 저장해놓은 약 1억 600만 명의 고객개인정보를 해킹당한 사례는 Captial One 담당자의 보안 설정 실수로 발생하였다.

- 주요 사회 기반 시설(critical infrastructure) 공격에 의한 공공서비스 장애: 국가 기반 시설 중 전력시설을 목표로 한 악의적 사이버 공격이 발생하면 해당 전력시설로부터 전력공급을 받는 기업의 운영 중단이 발생하여 거래중지 또는 기업휴지 비용이 발생할 수 있다. 일례로 2016년 12월 우크라이나 전력망을 겨냥한 악성 해킹으로 인해 1시간 가량 수도 키예프 지역 정전이 발생하였는데, 해당 공격과 같은 유형은 전기를 분배하는 변전소 내의 회로 차단기와 스위치를 원격 제어할 수 있어 신속한 수동 운영 전환 조치가 이루어지지 않는다면 정전사태가 장기화되어 더 큰 손실을 발생시킬 수 있는 잠재적 위험을 가지고 있다.

- 사이버 공격으로 촉발되는 물리적 무력충돌: 극단적인 형태의 시나리오로 분쟁 국가들 간 사이버 공격이 발생하여 물리적 충돌까지 이어지는 유형이 가능하다. 사이버 공격의 형태로는 국가기밀 반출 목적 해킹, 공공 클라우드 서비스 공격, 통신 기반 시설 마비, 에너지 공급 제어 시스템 공격 등이 있을 수 있으며, 국가 핵심시설에 대한 사이버 공격은 피해국가의 무력시위 등으로 이어져 긴장관계가 악화되고, 이는 각 국가의 금융시장에도 악영향을 미칠 수 있다.

나. 고빈도-고심도(HFHS) 유형 시나리오

- 데이터 유출 사고: 기업 신용평가 회사의 기업고객 신용 관련 데이터베이스로 해킹이 발생하여 다수 기업의 신용평가를 위한 내부 데이터가 공개되는 상황이 발생하면, 신용평가 회사의 평판뿐만 아니라 민감 정보가 유출된 기업고객의 평판까지 영향을 받을 수 있다. 데이터 유출 사고는 발생 유형이 관리자 소홀, 외부 악의적 해킹, 시스템 오류 등의 다양한 형태로 나타날 수 있고, 손실규모의 스펙트럼도 미약한 수준에서부터 기업 평판에 큰 영향을 끼칠 수 있는 수준까지 넓어서 높은 손실 빈도를 나타낼 수 있다.

- 거래시스템상 악성 소프트웨어 설치: 대형 증권사, 자산관리사의 내부 직원 컴퓨터에 악성 소프트웨어가 설치되어 내부망으로 악성 코드를 통해 자동화 거래 시스템(automated trading) 통제에 접근이 가능해지면, 동시다발적 대규모 거래를 통해 일시적 시장충격을

가지고 올 수 있다.

- 내부자를 통한 온라인 해외송금 사기: 악의적 목적으로 해외 외부자와의 결탁을 통해 금융사 내부 직원이 악성 소프트웨어를 내부망에 설치 시 해당 금융사 고객예금을 해외 외부자 계좌로 송금시킬 수 있는 시스템 통제가 발생할 수 있다.

〈표 Ⅳ-1〉 저빈도-고심도 및 고빈도-고심도 손실유형 시나리오

구분	저빈도-고심도 유형(LFHS)	고빈도-고심도 유형(HFHS)
가능 시나리오	• 거래소 네트워크 교란 • 랜섬웨어로 인한 운영중단 • 클라우드 공급자 실패 또는 사용자 실패 • 주요 사회 기반 시설 공격에 의한 공공 서비스 실패 • 사이버 공격으로 촉발되는 물리적 무력 충돌	• 데이터 유출 사고 • 거래시스템상 악성 소프트웨어 설치 • 내부자를 통한 온라인 해외송금 사기
피해범위	• 개별 기업 • 지자체/중앙정부	• 개별 기업
경감방안	• 개별 기업 리스크 통제계획 마련 및 투자 • 민관협력(public-private partnership) 프로그램	• 개별 기업 리스크 통제계획 마련 및 투자 • 민관협력(public-private partnership) 프로그램

자료: Kaffenberger and Kopp(2019)를 참조함

3. 디지털 리스크 관리방안에 관한 이론적 고찰

기업 입장에서 최소한의 자본을 활용하여 영업활동 중 발생 가능한 물리적 손실을 최대한으로 줄이고, 잠재적으로 발생 가능한 무형의 손실(예를 들면, 평판 하락 등)까지 방어하기 위한 최적 수단을 찾는 것은 중요하다. 따라서, 리스크 관리에 있어 효율적 전략을 탐색하는 것은 기업가치 극대화 목표를 달성하기 위해 필요하다. 특히, 최근 팬데믹, 자연재해 증가 등 기업의 영업환경에 심각한 영향을 끼칠 수 있는 위험상황 또는 사건이 빈번하게 발생하는 시기에는 전사적 관점에서 리스크 관리 전략의 중요성은 더 높아졌다고 볼 수 있다. 전반적인 기업활동에서 디지털 전환으로 인해 발생할 수 있는 리스크를 관리하

기 위한 전략 또한 효율적으로 설계되어야 한다. 이를 위해 리스크 관리방안에 대한 이론적 배경을 고찰하고, 가능한 전략에 대해서 논의하고자 한다.

가. 리스크 관리 전략

디지털 전환으로 인한 리스크는 동인에 따라 다양한 빈도와 심도를 발생시킬 수 있다. 이는 리스크 관리 전략을 설정하는 데 있어 상호 보완적 관점에서 다양한 수단을 적절하게 운용할 필요가 있음을 의미한다. 다만, 리스크 관리 전략을 설정할 때 디지털 리스크의 특성을 이해한 후 관리 수단을 선택해야 한다. Ⅳ장 2에서 소개했고, 〈그림 Ⅳ-1〉에서 볼 수 있듯이, 리스크는 손실의 빈도-심도 유형에 따라 크게 네 가지로 분류되는데, 최적 리스크 관리 전략은 각 유형에 따라 달라질 수 있다.[23)]

우선, 저빈도-저심도 유형(LFLS)은 손실사건의 발생 횟수가 상대적으로 높더라도 평균적인 손실크기가 높지 않으면 기업입장에서 해당 리스크를 보유하는 것이 비용-효율 측면에서 유리하다. 손실 심도가 매우 적은 경우 예상하지 못한 형태의 미미한 사건을 경험하여 의도치 않게 부담하는 리스크도 존재하는데 이를 소극적 리스크 보유라고 한다. 이러한 유형의 사건은 발생 가능한 손실 규모 만큼을 미리 준비금 또는 충당금으로 설정해 두고, 실제 손실사건이 발생하게 되면 설정된 금액으로부터 지불하는 방법이 가능하다. 자가보험(self-insurance)을 활용하여 보유 리스크를 대비할 수도 있는데, 이 경우 세금 공제 측면에서 준비금 적립에 비해 유리할 수 있다. 자가보험 형태로 대표적인 것은 캡티브(captive)로서, 내부 계열사로서 보험사를 직접 운영함으로써 기업 운영에서 발생하는 손실사건들을 재정적으로 처리하는 방식이다.

고빈도-저심도 유형(HFLS)은 손실통제(loss control) 또는 리스크 통제(risk control) 방식을 활용하여 관리하는 것이 효율적이다. 손실통제 기법은 기본적으로 손실의 발생 빈도와 심도를 줄이려는 방법, 도구 또는 전략을 포괄하는데, 발생 빈도를 줄이는 방법을 손실예방(loss prevention), 발생심도를 줄이는 방법을 손실감소(loss reduction)라고 한다. 리스크 보유 전략과는 다르게 손실사건 발생 이전에 이를 억제, 예방 및 축소하기 위한 방안을 전제로 한다. 손실예방 전략으로 대표적인 것은 자가보호(self-protection)가 있으며, 손실감소 전략으로는 앞에서 언급한 것과 같이 자가보험(self-insurance) 수단이 있다. 여기서 자가보호와 자가보

23) 이하 최적 리스크 관리 전략은 보험경영연구회(2019)를 참조함

험의 개념은 최초 Ehrlich and Becker(1972)가 제안하였는데, 두 개념의 현실적인 구분은 엄격하지 않고 수단에 따라 두 가지 효과를 모두 가지고 있는 경우도 있다.[24]

〈그림 Ⅳ-1〉 손실 빈도 및 심도에 따른 리스크 관리 최적 전략

	저빈도 (Low frequency)	고빈도 (High frequency)
저심도 (Low severity)	리스크 보유 (Risk retain)	리스크 보유 및 손실통제 전략 (Retain and implement loss control)
고심도 (High severity)	리스크 전가 (Risk transfer)	리스크 회피 (Risk avoidance)

저빈도-고심도 유형(LFHS)의 경우 이론적으로 리스크 전가 방법을 통해 관리하는 것이 기업 재무적 측면에서 효율적이다. 저빈도-고심도 유형의 리스크를 회피하려는 성향(risk averse)을 가진 보유자가 리스크 중립적 성향(risk neutral)을 가진 인수자에게 해당 리스크를 전가할 수 있는 리스크 거래 시장의 균형점이 존재할 수 있다. 보험시장이 리스크 전가가 이루어지는 대표적인 시장으로서 저빈도-고심도 운영리스크를 기업이 보험사에게 전가함으로써 기업은 보험료만큼의 비용만 감수하면 되고, 보험사는 대수의 법칙(law of large number)을 통해 적정 보험료 산출 및 수익성을 가질 수 있게 된다.

이와 연결하여 고빈도-고심도 유형(HFHS)의 경우에도 리스크 전가 방식을 통해 관리 전략을 취할 수 있으나, 이 경우 보험사 입장에서 부보 가능성이 낮은 리스크를 인수하게 되어 단수 보험사가 감당하기 어려운 상황이 발생할 수 있다. 이러한 유형을 시장을 통해 해결하기 위해서는 재보험을 활용하거나 공동보험 등의 형태로 다수 보험사들이 리스크를 분담하는 형태가 되어야 한다. 또는 공공영역이 시장에 개입하여 지원 프로그램을 운영하

24) 예를 들어, 화재경보시스템과 스프링클러 간의 차이를 두 개념에 비추어 판단하면, 화재경보시스템은 손실예방 수단으로서 실제 화재가 발생하기 전에 차단할 수 있는 환경을 제공하지만, 스프링클러는 실제 화재 발생 후 이를 차단하기 위한 환경을 제공하기 때문에 구분이 상대적으로 명확함. 이와 비교하여, 홍수를 대비해서 건설한 댐의 경우 그 수위를 넘기기 전까지 손실예방의 효과를 제공하고, 수위를 넘겨 하류지역에 홍수가 발생하더라도 댐이 무너지지 않는 한 홍수의 규모 측면에서 다소 경감의 효과를 제공할 수도 있어 손실감소의 수단으로서도 기능할 수 있다고 판단 가능함

거나, 의무보험의 형태로 시장참여자가 되는 방법도 가능할 것이다.[25] 리스크를 관리해야 하는 기업은 전가의 방식으로 해결되지 않는 고빈도-고심도 유형에 대해 리스크 회피(risk avoidance) 방식을 선택할 수도 있다.[26]

그렇다면 디지털/사이버 운영리스크를 효율적으로 관리하기 위한 수단으로 어떤 것을 선택하는 것이 기업 입장에서 최적의 결과를 도출할 수 있을까? 예를 들어, 앞서 설명한 디지털 전환에 따른 사업영역에서 시스템 및 프로세스 변화로부터 발생할 수 있는 디지털 리스크의 경우 자가보호 수단을 활용하여 발생확률을 줄이거나, 기업 내부적인 관리체계를 통해 손실의 크기를 줄일 수 있다. 네트워크상 외부자의 공격, 재해재난에 의한 디지털 자산의 손실 등은 손실통제 수단(loss control measure)을 통해서 빈도 및 심도를 줄일 수 있는 여지가 존재하나 이를 완벽하게 억제할 수 있는 전략을 세우는 것은 사실상 불가능하다.

〈그림 Ⅳ-2〉는 사이버 보안을 디지털 전환에 따른 리스크를 통제할 수 있는 일반적인 수단으로 보고, 위험수준과의 관계성을 살펴본 것이다. 사이버 보안수준이 높아질수록 기업이 노출되는 디지털/사이버 리스크는 점차 낮아지게 되어 일정 수준까지 수렴이 가능하다. 하지만 아웃소싱 클라우드 서비스, 상업 보안 소프트웨어, 외부 공급업체를 통한 핀테크 기술 협업 등은 기업이 자체적인 리스크 통제수단(사이버 보안 노력)을 사용하더라도 제거할 수 없는 잔존 리스크(residual risk) 또는 체계적 리스크(systematic risk)를 보유할 수 밖에 없다. 이러한 체계적 리스크는 상호 연결된 네트워크 속에서 이루어지는 디지털화된 사업환경이 만들어낸 피할 수 없는 리스크를 의미한다.[27]

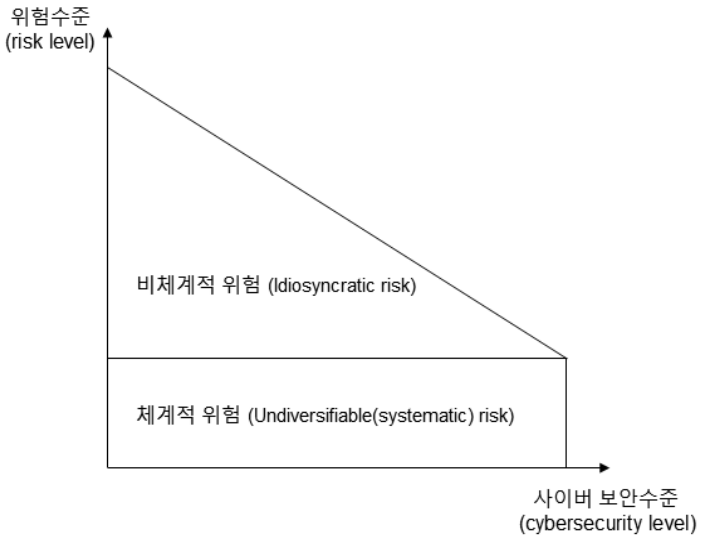
---

25) Ⅵ-2장에서 극단적 형태의 디지털/사이버 리스크를 관리하기 위한 민관협력방안에 대해 논의함

26) 예를 들면, 매년 발생하는 허리케인으로 인해 발생할 수 있는 손실을 회피하기 위해 미국 동남부 지역이 아닌 지역을 대상으로만 생산시설 확충 등의 의사결정을 고려하는 경우가 있음

27) Muermann and Kunreuther(2008)는 상호 연결 또는 상호 의존 리스크(interconnected/interdependent risk)에 노출되어 있는 경제주체(economic agents)의 자기보호 수단에 대한 최적 투자의사결정 문제를 논의하였음. 이들은 전통적인 기대효용이론을 활용하여 내쉬균형(Nash Equilibrium)하에서 긍정적인 외부효과(positive externality)가 자기보호에 대한 과소투자를 유도함을 증명하였으며, 여기서 긍정적인 외부효과는 상호 연결된 주체의 자기보호 투자 증가에 따라 리스크 수준이 하락하는 효과를 의미함. 이를 디지털/사이버 리스크 관점에 대입하면, 기업은 기본적으로 외부 사이버 위험으로부터 스스로를 방어하기 위해 자기보호 수단(즉, 보안체계 강화)에 투자를 하지만, 상호 연결된 산업 주체의 보안 취약성 증가로 인해 체계적 위험의 수준이 증가할 수 있다고 판단 가능함

〈그림 Ⅳ-2〉 사이버 보안과 위험의 다각화



자료: Kaffenberger and Kopp(2019)의 〈Figure 1〉을 재구성함

문제는 기업이 잠재적으로 노출된 체계적 디지털/사이버 리스크로부터 극단적 형태의 손실사건이 발생할 수 있는 가능성을 안고 있다는 점이다. 특히, 상호 연결된 산업주체의 보안 취약성 증가로 인해 체계적 위험 수준이 높아지게 되면 자연스럽게 Ⅳ장 2에서 소개한 사례들과 같이 극단적 손실을 유발할 수 있는 위험사건에 노출될 수 있다. 결국, 〈그림 Ⅳ-1〉과 같이 고심도의 특성을 가지는 손실사건을 관리하기 위한 방법으로서, 리스크 전가 및 회피의 수단을 병행하여 전략적인 관리가 필요하다.

하지만 현실적으로 사이버 공간에서 발생할 수 있는 손실사건을 회피할 수 있는 전략은 많지 않다. 극단적 형태의 물리적인 위험, 예를 들면 지진, 태풍, 해일 등으로 인한 사건의 경우 해당 위험요인이 발생할 가능성이 적은 지역에 사업계획을 수립하고 실행하는 전략이 가능하다. 즉, 계획 수립 시 이러한 위험요인에 노출될 가능성을 사전에 분석한 후 리스크 회피 전략이 비용적인 측면에서 효율적으로 작동할지 판단할 수 있다. 하지만 사이버 공간상 발생할 수 있는 위험사건은 공격자가 존재하는 경우가 대부분이고, 공격자의 전략 및 행위를 사전에 파악하기 어렵기 때문에 회피전략이 효율적으로 작동하기 어렵다. 따라서, 디지털/사이버 운영리스크에 의한 고심도 손실사건을 관리하기 위해서는 회피전략보다는 전가방법을 통해 관리하는 전략을 고려하는 것이 필요하다.

V 실증분석: 디지털 운영리스크 손실 빈도 및 심도 분포 추정

1. 개요

이 장에서는 앞서 분류한 디지털 운영리스크 체계를 기반으로 운영리스크 손실데이터상 심도 및 빈도의 통계적 분포를 추정하고, 잠재적 손실의 크기를 판단하고자 한다. 최적 리스크 관리 전략을 선택하기 위해서는 우선 정량적인 리스크 분석이 요구된다. 즉, 가용한 손실 데이터를 활용하여 분석하고자 하는 리스크의 통계적 속성을 파악하여 향후에 얼마나 자주, 어느정도의 크기로 발생 가능한지 예측하는 과정을 진행한다. 리스크의 통계적 속성은 기본적으로 해당 리스크로 인해 발생한 손실자료의 빈도 및 심도의 분포적 특성을 의미한다. 이를 파악하고 나면 앞서 논의한 리스크 관리 전략(〈그림 Ⅳ-1〉 참조) 중 최적의 방법을 선택하는 데 통계적 근거로서 활용할 수 있다.

2. 활용 데이터

운영리스크의 손실자료는 일반적으로 다른 형태의 리스크(예를 들면, 시장 또는 신용리스크) 관련 자료에 비해 상당히 부족하다. 기업 내부적으로 축적하고 있는 손실자료도 많지 않고, 축적된 데이터조차 충분하고 통계적으로 유의미한 결과를 도출하기 쉽지 않다.[28] 따라서, 기업 내부에서 축적한 데이터와 함께 외부 가용 데이터를 병합하여 손실자료의 크기를 충분히 확보할 필요가 있다. 외부 가용 데이터베이스와 관련하여 Wei, Li and Zhu(2018)는 66개의 운영리스크 관련 데이터베이스를 몇 가지 유형 및 가장 많이 활용되는 자료 위주로 분석하였다(〈표 V-1〉 참조).

28) Wei, Li and Zhu(2018)는 운영리스크 관련 301개의 학술논문과 66개의 관련 데이터베이스를 분석하였음. 해당 연구는 개별 은행이 축적하는 운영리스크 내부 손실자료의 문제점을 두 가지로 요약하였음. 첫 번째로 자료의 크기가 충분치 않아 의미있는 모델링을 진행하기 쉽지 않다는 점이고, 두 번째로 대부분의 손실이 고빈도-저심도(low frequency-high severity) 유형이기 때문에 미래 발생가능한 극단적 손실을 추정하는 데 제한이 있음을 밝혔음

〈표 Ⅴ-1〉 일반 운영리스크 및 디지털/사이버 운영리스크 관련 데이터베이스

〈일반 운영리스크 손실데이터베이스〉

유형		데이터베이스	출처	발행연도	최소손실	관측치수(개)
컨소시엄	은행	ORX-GBD	ORX	2002	€20,000	525,395 (2016 기준)
		DIPO	이탈리아 은행연합회	2003	€5,000	-
		DakOR	독일공공 은행연합회	2006	-	-
		DSGV	독일저축 은행연합회	-	-	-
		GOLD	영국은행 연합회	2000	-	-
		OLDSCD	미국은행 연합회	2003	-	-
		Cordex	인도은행 연합회	2008	-	-
		HunOR	헝가리 은행연합회	2007	HUF50,000	약 4,000 (2009 기준)
	보험	ORX-GID	ORX	2015	-	-
		ORIC	영국보험 연합회	2005	£10,000	약 2,000 (2009 기준)
상업용		Algo FIRST	IBM	1998	$1million	약 14,500 (2016 기준)
		Algo OpData	IBM	-	$1million	약 14,000 (2017 기준)
		SAS OpRisk	SAS	2005	$100,000	약 38,000 (2021 기준)
		WTW	Willis Towers Watson	-	-	-
		OpBase	Aon	-	-	-

〈디지털/사이버 운영리스크 손실데이터베이스〉

유형	데이터베이스	발행연도	최소손실	관측치수(개)
디지털/사이버 리스크 손실	Advisen	-	-	약 90,000
데이터 유출	Privacy Rights Clearinghouse	2005	-	약 9,000
디지털/사이버 리스크 손실	Cowbell Cyber	-	-	약 22,000

자료: Wei, Li and Zhu(2018)의 〈Table 2, 4〉를 포함하여 저자가 재구성함

본 보고서에서는 〈표 V-1〉에 나열된 데이터 중 디지털/사이버 운영리스크 손실에 초점을 맞춘 Cowbell Cyber 데이터를 수집하여 활용하였다. 해당 데이터는 미국 캘리포니아에 위치한 사이버 보험회사인 Cowbell Cyber Inc.에서 다수의 사이버 운영리스크 손실데이터베이스로부터 자료를 수집하여 자체 리스크 인수 평가를 위한 도구로 활용하고 있다. 본 데이터베이스는 미국 내 디지털 및 사이버 리스크 관련 손실정보를 제공하고 있으며, 따라서 이 장에서 제공하는 통계적 결과는 특정 회사 단위(firm-level)에 적용되지 않고, 미국 시장 단위에 적용되는 값임을 밝힌다.[29] 해당 데이터베이스는 각 손실사건에 대한 다수의 정보[30]를 포함하고 있는데, 본 보고서에서는 주요 손실변수인 Total loss amount의 월별 빈도 및 심도값을 가지고 일변량 분석(univariate analysis)을 진행하였다. 또한, 데이터상 금융 및 보험산업에 속하는 기업과 비금융권에 속하는 기업을 분류하여 추출하였으며, 두 산업유형 간 통계적 차이를 분석하였다.

3. 분석모형

본 연구에서는 운영리스크 데이터를 손실 빈도(loss frequency)와 심도(severity)로 구분하여 분석하였다. 운영리스크 손실 빈도 데이터는 이산분포(discrete distribution)을 따르며, 시간간격에 따라 다수의 0값을 포함하는 특성을 가진다. 특히, 일단위(daily) 데이터의 경우 이러한 특성이 두드러지는데, 분포 적합성 향상을 위해 본 분석에서는 손실자료를 월단위로 구분하여 분석을 진행하였다. 손실 심도의 경우 연속분포(continuous distribution)를 따르고 비음(non-negative)의 특성을 가지고 있으며, 빈도와 마찬가지로 다수의 0값(손실사건이 보고되었으나, 손실이 발생하지 않았거나 손실여부 확인이 되지 않

29) 즉, 손실 빈도의 경우 미국 시장 내 디지털 또는 사이버 리스크 손실 사건의 월별 발생 횟수를 의미하고, 손실 심도의 경우 사건별 발생 규모로 해석할 수 있음. 데이터베이스 측면에서의 한계점은 미국 시장 내 발생한 손실사건의 모집단을 나타내지 못한다는 점임. 이는 손실 사건 보고에 관한 규제가 주별로 존재하더라도 손실을 확인할 수 없는 매우 소규모 사건이거나, 손실 발생 여부를 인지하지 못한 외부 공격이 존재할 수 있기 때문에 데이터상의 편향(bias)이 존재함을 밝힘. 또한, 국내 디지털 및 사이버 환경을 정확하게 반영하지 못하는 한계점을 가지고 있고, 피해기업의 특성이나 규모 측면에서도 국내시장을 정확히 반영하지 못할 수 있음. 그럼에도 불구하고, 해당 데이터베이스는 디지털 또는 사이버 리스크와 관련하여 가장 큰 규모의 관측치 수를 보유한 데이터베이스들 중 하나이며, 실제 손실액 및 데이터 유출 건수 등의 정량변수들을 가지는 관측치 수가 다른 데이터베이스에 비해 많다는 점에서 의미 있는 결과를 도출함. 향후 국내시장에 대한 관련 데이터가 수집가능하다면 국내 금융시장 환경에 적합한 연구 결과를 도출할 수 있을 것으로 기대함

30) 데이터베이스가 포함하는 정보로는 피해기업 업종, 피해기업 위치(주단위), 데이터 유출 건수(데이터 유출 사건에 한함), 리스크 유형, 보안점수 등이 있음

은 경우)을 포함하고 있다. 따라서, 해당 손실자료는 전형적으로 보험 손실자료와 유사한 특성을 가지고 있다.

이 장에서는 운영리스크 손실 빈도 및 심도의 최적 분포를 통계적 검정을 통해 적합하고, 각각의 수준을 리스크 매트릭스(또는 리스크 맵)에 도식화하여 해당 리스크 유형을 판단할 수 있는 도구를 제안하고자 한다. 이 과정을 통해 분석하고자 하는 리스크 유형은 데이터의 특성상 크게 두 가지로 분류가 가능하다(〈표 V-2〉 참조).[31] 이와 같이 두가지 리스크 유형으로 분류한 이유는 유형별 충분한 분석자료 확보뿐만 아니라 다수의 기존 연구들과 미국 사이버보험 시장에서 크게 두 가지 유형에 따라 분석 및 보장영역을 규정하기 때문이다.[32]

손실 빈도와 심도분포를 추정하기 위한 통계적 분포는 다음과 같이 고려하였다. 손실 빈도의 경우 운영리스크 손실분포접근법(LDA) 및 보험 손실데이터 분석 시 많이 활용되는 포아송(Poisson), 음이항(negative binomial) 분포를 사용하였다.[33] 월단위 손실자료에 다수 관찰되는 0값(손실사건 미발생)의 적합성을 판단하기 위해 영과잉 포아송(zero-inflated Poission)분포 또한 사용하여 검정을 진행하였다. 손실 심도의 경우 기존 문헌에서 많이 활용한 감마(gamma), 로그정규(log-normal)분포 및 극단적 규모의 손실의 적합성을 판단하기 위한 임계치 초과극값(peaks-over-threshold; POT) 방법도 적용하였다.[34] POT 방법의 경우 로그정규분포와 일반화 파레토 분포(generalized Pareto distribution)의 합성분포를 활용하였다.[35]

31) 데이터가 제공하는 리스크 유형상 앞서 Ⅲ장에서 제안한 분류체계하 리스크 요인들을 고려하는 데 한계가 존재함. 더 구체적이고, 다양한 손실자료를 충분히 축적한다면 제안한 분류체계하에서 이질적 특성의 리스크 요인들을 통계적으로 분석함으로써 손실 예측력을 높일 수 있을 것으로 기대함

32) 기존 문헌은, 예를 들어, Edwards et al.(2016), Eling and Jung(2018)을 참조함. Romanosky et al.(2019)에서는 현재 미국 사이버보험 시장에서 거래되고 있는 100가지의 보험상품을 분석하여 크게 악의적 리스크를 보장하는 상품과 우연/실수에 의한 리스크를 보장하는 상품의 두 가지 형태가 존재함을 확인하였음. 특히, 악의적 리스크에 대해서 보장하는 상품의 수가 대다수를 차지하고 있음을 관찰하였으며, 악의적 리스크를 보장하는 상품들은 기존 손해보험의 특약 형태가 아닌 주로 단독형 상품(stand-alone)으로 개발되어 판매되고 있음을 발견하였음

33) Edwards et al.(2016), Eling and Jung(2018), Eling and Wirfs(2019)를 참조함

34) 일반 운영리스크 측면에서는 Moscadelli(2004), Shevchenko(2010)를, 디지털/사이버 운영리스크 측면에서는 Wheatley, Maillart and Sornette(2016), Eling and Wirfs(2019)를 참조함

35) 본 보고서에는 공간적 제한으로 인해 최적 분포에 관한 통계적 검정 결과만 제공함(〈표 V-5〉 및 〈표 V-6〉 참조)

〈표 V-2〉 실증분석을 위한 리스크 분류

악의적 리스크 유형 (Malicious risk)	기타 리스크 유형 (Non-malicious risk)
• 신원도용(identity theft) • 악의적 데이터유출(malicious data breach) • 피싱/위장/도용(phishing&spoofing) • 사적정보 침해(privacy breach) • 신용카드 정보도용(skimming) • 데이터 탈취(stolen data) • 사이버상 탈취(cyber extortion)	• 네트워크 교란(network disruption) • 환경설정/프로세싱 오류 (configuration/processing errors) • 의도치 않은 데이터 유출 (unintended data breach)

4. 분석결과

〈표 V-3〉과 〈표 V-4〉는 각각 금융기업 및 비금융기업의 월단위 손실 빈도 및 심도의 기초통계량을 보여준다. 금융 및 비금융기업 모두 악의적 리스크에 의한 손실사건이 비악의적 리스크에 의한 손실사건에 비해 평균적으로 월 7배 이상 더 많이 발생한다는 것을 확인할 수 있으며, 손실의 규모 측면에서는 평균적으로 금융기업이 10배, 비금융기업이 5배 가량 차이가 나타남을 알 수 있다. 또한, 비금융권에 속한 기업들이 금융권에 속한 기업들보다 더 자주 손실을 경험하며, 더 큰 피해에 노출되어 있음을 확인할 수 있다.

〈표 V-3〉 월별 손실 빈도 및 심도의 기초통계량(금융기업 데이터)

구분	악의적 리스크 (malicious risk)		비악의적 리스크 (non-malicious risk)	
	손실 빈도	손실 심도	손실 빈도	손실 심도
Mean	21.68	7.25	3.13	0.71
Std	28.09	33.88	3.43	4.64
Max	181.00	393.50	14.00	46.50
median	12.00	0.00	2.00	0.00
min	0.00	0.00	0.00	0.00

주: 손실 빈도는 횟수를 나타내고, 손실 심도의 단위는 $million임

〈표 V-4〉 월별 손실 빈도 및 심도의 기초통계량(비금융기업 데이터)

구분	악의적 리스크 (malicious risk)		비악의적 리스크 (non-malicious risk)	
	손실 빈도	손실 심도	손실 빈도	손실 심도
Mean	55.26	23.24	7.31	4.78
Std	63.86	139.64	7.38	34.16
Max	355.00	2,000.43	31.00	400.00
median	35.00	6.33	5.00	0.00
min	0.00	0.00	0.00	0.00

주: 손실 빈도는 횟수를 나타내고, 손실 심도의 단위는 $million임

적합성 검정은 로그가능도(Log-likelihood), 정보통계량(Akaike Information Criteria; AIC) 및 분포 적합성 테스트 결과(빈도는 Chi-square test, 심도는 Kolmogorov-Smirnov test)를 기반으로 진행하였다.[36] 최소 AIC를 기준으로 월별 손실 빈도와 심도에 관한 분포 적합성 검정 결과, 손실 빈도의 경우 금융, 비금융산업 및 두 가지 리스크 유형 모두 음이항 분포를 따르며, 손실 심도의 경우 로그정규분포가 더 나은 결과를 나타냄을 확인하였다(적합성 검정 결과는 〈표 V-5〉, 〈표 V-6〉 참조). 적합성 검정의 시각화된 결과는 〈부록 그림 Ⅱ-1~4〉의 진단 그래프(빈도그래프, Q-Q plot, P-P plot, CDF plot)를 통해 재확인할 수 있다.

월별 손실 빈도 및 심도의 통계적 적합성 검정 결과를 바탕으로 〈그림 V-1〉에서는 금융기관의 손실 빈도 및 심도의 리스크 맵을, 〈그림 V-2〉에서는 비금융기관의 손실 빈도 및 심도의 리스크 맵을 도식화하였다. 각 리스크 맵은 다섯단계의 수준(Extreme-Large-Medium-Small-Negligible)으로 구분되며, 단계를 구분하는 기준점은 빈도에 대해서는 적합된 분포의 분위수(2%-10%-50%- 80%)를 사용하였고 심도에 대해서는 적합된 분포의 분위수(25%-50%-70%-90%)를 사용하였다.[37]

36) 연속분포(continuous distribution)에 대한 적합성 검정으로서 일반적으로 Kolmogorov-Smirnov(K-S)가 널리 사용되지만, Anderson-Darling(A-D) 검정 또한 특정 상황(예를 들어, 분포 꼬리부분의 적합성 검정 등) 및 여러 측면에서 장점을 가지고 있음이 알려져 있음(Evans, Drew and Leemis 2008). 그럼에도 불구하고, 본 보고서에서는 결과가 명확히 도출되고 대표성을 가지는 K-S 적합성 검정 결과를 근거로 제시함

37) 해당 기준점은 0값의 밀도를 고려하여 선정하였으며, 특히 빈도에 관한 기준점의 경우 Louisot and Ketcham (2014)의 Ch.9을 참조하였음. 구체적으로 해당 기준점을 적용한 각 단계에서의 손실 빈도는 Extreme(월 45회 이상), Large(월 17~44회), Medium(월 2~16회), Small(월 1회), Negligible(월 0회)이고, 손실 심도는 Extreme

〈표 V-5〉 월별 손실 빈도 적합성 검정 결과(음이항 분포)

구분		악의적 리스크 (malicious risk)	비악의적 리스크 (non-malicious risk)
금융권	LogLik	-974.40	-549.37
	AIC	1,952.80	1,102.75
	Chi-sqr	29.91	28.89
비금융권	LogLik	-1,200.70	-734.88
	AIC	2,405.41	1,473.76
	Chi-sqr	28.07	16.96

주: Chi-sqr는 Chi-squared 검정의 통계량(statistics)을 의미함

〈표 V-6〉 월별 손실 심도 적합성 검정 결과(로그정규분포)

구분		악의적 리스크 (malicious risk)	비악의적 리스크 (non-malicious risk)
금융권	LogLik	-1,876.07	-326.21
	AIC	3,756.15	656.43
	K-S	0.08	0.15
비금융권	LogLik	-2,870.58	-946.77
	AIC	5,745.15	1,897.55
	K-S	0.07	0.06

주: K-S는 Kolmogorov-Smirnov 검정의 통계량(statistics)을 의미함

각 리스크 맵에서는 손실 빈도 및 심도 수준을 적합분포에 따른 확률값에 따라 세 가지 유형으로 평가하였다. 즉, 검정색은 해당 수준의 손실 횟수(예를 들면, 손실 빈도의 Extreme 수준은 월 45회 이상)가 발생할 확률이 40% 이상, 회색은 15%~40%, 흰색은 15% 이하를

(월 $10.26million 이상), Large(월 $0.597million~10.26million), Medium(월 $3,350~0.597million), Small (월 $1~3,350), Negligible(월 $1 이하)임. 매트릭스 구성을 위한 기준점 선정은 기업의 손실 빈도 및 심도 분포에 따라 특이점 또는 구조적 변화(structural break)를 보이는 분위 수를 도출하여 적용이 가능하며, 참조점으로 활용할 수 있는 동종업계, 유사규모의 타 기업 사례 등을 통해 벤치마킹도 가능함

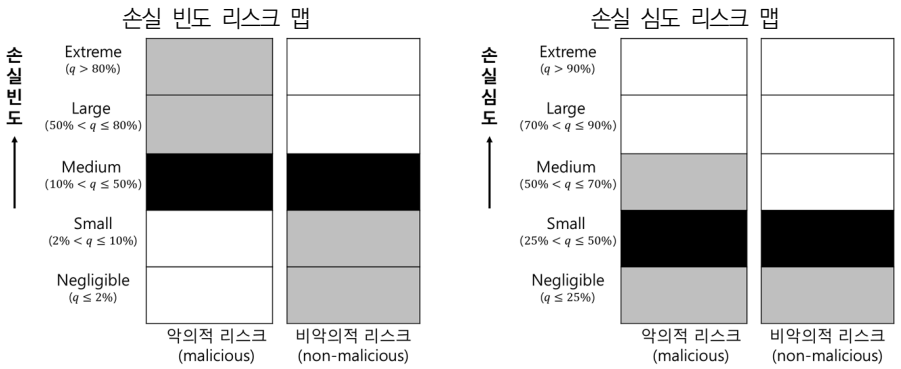
의미한다.[38] 이러한 평가를 바탕으로 도식화된 손실 빈도의 경우, 금융 및 비금융기관 모두 악의적 리스크에 의한 사건이 발생할 횟수가 월 2~16회 이하 범위 안에 들어갈 확률이 가장 높으며, 비악의적 리스크의 경우도 마찬가지로 월 2~16회 이하 범위 안에 들어갈 확률이 가장 높게 나타났다. 하지만, 악의적 리스크의 경우 금융 및 비금융기관 모두에서 'Large' 레벨 이상 손실 빈도 수준이 유의함을 확인하였으며, 비악의적 리스크의 경우 상대적으로 적은 빈도수준('Small' 이하)의 유의성이 나타났다. 이는 금융기업이든, 비금융기업이든 보안수준 향상 및 내부 보안교육 강화 등의 노력 증진 등을 통해 악의적 디지털 및 사이버 리스크에 의한 손실사건 빈도를 줄여야 함을 시사한다.

손실 심도의 경우, 금융기업에서 악의적 리스크에 의한 손실규모가 비악의적 리스크에 의한 영향보다 상대적으로 더 크게 나타난다. 비금융기관의 경우 상대적으로 비악의적 리스크의 매우 적은 수준의 손실 심도 사건이 발생할 가능성이 높게 나타났으며, 결국 금융 및 비금융기관의 도식화된 리스크 수준은 공통적으로 악의적 리스크의 심도수준이 더 우려스러운 상황임을 가리킨다. 따라서, 악의적 리스크는 고빈도-고심도 손실 유형을 유발할 수 있는 잠재성을 가지고 있다고 평가할 수 있는 반면, 비악의적 리스크는 저빈도-저심도 또는 고빈도-저심도 유형의 손실사건을 유발할 수 있다고 판단할 수 있다.

앞서 이론적 관점에서의 리스크 관리 전략에 따르면, 악의적 디지털 및 사이버 리스크의 경우 리스크 전가 또는 회피 방법을 활용하는 것이 효과적이며, 비악의적 리스크의 경우 기업 자체적인 리스크 보유 및 통제 전략을 세우는 것이 효과적이다. 효과적 리스크 전가 방법에 관해서는 다음 장에서 심도있게 다룰 것이나, 비악의적 리스크를 관리하기 위한 리스크 보유 및 통제 전략은 정확한 손실평가 모형 개발 및 사이버 보안 시스템 투자 확대, 전사적 디지털 리스크 관리체계 확립을 위한 경영진의 적극적 의사결정 등이 뒷받침되어야 한다. 이러한 노력이 이루어지지 않는다면, 단순히 소규모 사건들에 의한 비용 증가뿐만 아니라, 디지털 리스크 관리 전략 부재로 인한 시장 내 기업의 명성 하락 등의 간접적 비용 증가 또한 문제가 될 수 있음을 금융 및 비금융기업 모두 인식해야 한다.

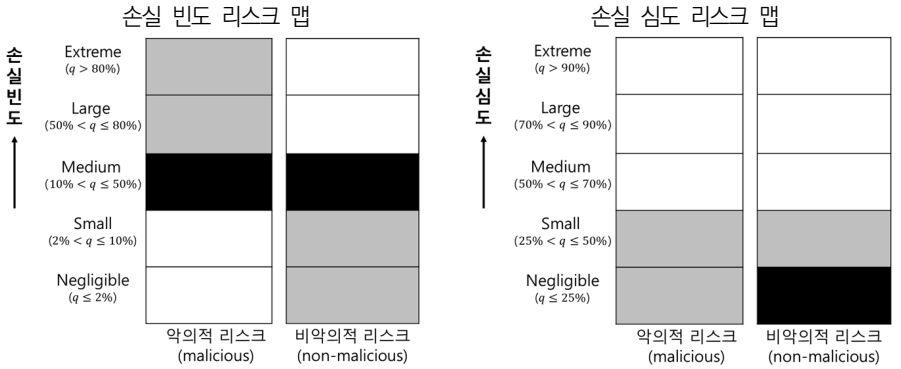
38) 유형을 분류하는 확률 기준에 관한 이론적 또는 관습적 근거는 명확하지 않기 때문에, 기준을 선정하는 것은 개별 기업의 과거 자료 및 시나리오 분석을 바탕으로 위험의 수준을 자체 평가할 필요가 있음. 본 보고서의 경우 다수의 산업 보고서를 참고하여 기업들의 위험에 대한 수준을 경험적 방식으로 판단하여 기준을 설정하였음

〈그림 Ⅴ-1〉 금융기관 리스크 맵



주: 손실 빈도의 다섯단계 수준(Extreme-Large-Medium-Small-Negligible)은 적합분포의 분위수(2%-10%-50%-80%)를 기준으로 구분하였으며, 검정색은 해당 수준의 손실횟수가 발생할 확률이 40% 이상, 회색은 15~40%, 흰색은 15% 이하를 의미함. 각 수준에 해당하는 발생 횟수는 Extreme(월 45회 이상), Large(월 17~44회), Medium(월 2~16회), Small(월 1회), Negligible(월 0회)임. 손실 심도의 다섯 단계 수준(Extreme-Large-Medium-Small-Negligible)은 적합분포의 분위수(25%-50%-70%-90%)를 기준으로 구분하였으며, 검정색은 해당 수준의 손실규모가 발생할 확률이 40% 이상, 회색은 15~40%, 흰색은 15% 이하를 의미함. 각 수준에 해당하는 발생규모는 Extreme(월 $10.26million 이상), Large(월 $0.597million~10.26million), Medium(월 $3,350~0.597million), Small(월 $1~3,350), Negligible(월 $1 이하)임

〈그림 Ⅴ-2〉 비금융기관 리스크 맵



주: 손실 빈도의 다섯단계 수준(Extreme-Large-Medium-Small-Negligible)은 적합분포의 분위수(2%-10%-50%-80%)를 기준으로 구분하였으며, 검정색은 해당 수준의 손실횟수가 발생할 확률이 40% 이상, 회색은 15~40%, 흰색은 15%이하를 의미함. 각 수준에 해당하는 발생 횟수는 Extreme(월 45회 이상), Large(월 17~44회), Medium(월 2~16회), Small(월 1회), Negligible(월 0회)임. 손실 심도의 다섯 단계 수준(Extreme-Large-Medium-Small-Negligible)은 적합분포의 분위수(25%-50%-70%-90%)를 기준으로 구분하였으며, 검정색은 해당 수준의 손실규모가 발생할 확률이 40% 이상, 회색은 15~40%, 흰색은 15% 이하를 의미함. 각 수준에 해당하는 발생규모는 Extreme(월 $10.26million이상), Large(월 $0.597million~10.26million), Medium(월 $3,350~0.597million), Small(월 $1~3,350), Negligible(월 $1 이하)임

Ⅵ 리스크 관리 시사점 및 결론

1. 최적 디지털 리스크 관리 전략: 리스크 전가

금융산업 내 전면적이고, 급격한 디지털 전환은 분명 사업 운영 측면에서 불확실성을 가져온다. 즉, 금융산업이 직면하는 운영리스크는 이미 시장, 신용리스크에 비해 더 복잡하고 다양하다는 점이 알려져 있지만, 디지털 전환으로 인한 금융산업의 비즈니스 프로세스 및 가치사슬(value chain)의 변화는 그 복잡성과 다양성을 한층 심화시켰다고 할 수 있다. 금융기업 입장에서는 디지털/사이버 운영리스크의 선제적 관리체계 구축뿐만 아니라 이러한 불확실성의 증가와 함께 잠재적으로 발생할 수 있는 손실을 관리하기 위한 효율적인 전략을 고민해야 한다. 특히, 앞 장에서 실증자료를 기반으로 확인된 악의적 리스크에 의한 고심도 손실사건을 관리하기 위한 전략이 필요한데, 이론적으로 가장 효율적 전략은 리스크 전가방법이다.

리스크 전가방법으로 가장 대표적인 것은 보험이다. 시장을 통해서 리스크를 거래함으로써 미래 잠재적 손실사건 발생 후 겪을 수 있는 재정적 어려움을 상당부분 해결 가능하다. 전통적 형태의 리스크(예를 들면, 화재, 자동차사고, 상해 등)들은 기본적으로 시장성을 확보할 수 있는 특성들을 가지고 있다. 보험의 기본원리인 대수의 법칙(law of large number)하에서 리스크 간 독립성이 보장되고, 동일 분포를 따른다는 가정이 성립하기 때문에 보험회사 관점에서는 해당 리스크들에 관한 불확실성을 감소시킬 수 있다.

반면, 디지털/사이버 운영리스크의 경우 리스크 간 상관 위험이 높고, 가용 데이터가 많지 않아 분포적 특징을 판단하기 어렵다. 또한, 위험의 양상(risk landscape)이 빠르게 변화한다는 특징을 가지는데, 이는 네트워크 환경에서 노출되는 범위(또는 노드)의 증가 및 정보기술 발전에 의한 공격자의 전략 및 기술 변화 등을 예측하기 힘들다는 것으로 대표될 수 있다. 그렇다면 저빈도-고심도 손실 유형을 효과적으로 관리하기 위한 방법으로서 디지털/사이버 위험에 관한 보험상품의 시장성은 충분한가?

리스크의 시장성을 평가하는 방법으로 Berliner(1985)가 제안한 부보 가능성(insurability)

평가 방법을 활용할 수 있다. Berliner(1985)는 리스크의 부보 가능성을 평가하기 위한 9가지 요인을 제안하였다(〈표 Ⅳ-2〉 참조). 일반적으로 시장에서 거래되는 리스크들은 이 9가지 요인을 만족하지만, Biener, Eling and Wirfs(2015)는 디지털 운영리스크에 속하는 사이버 리스크의 경우 현 시점에서 만족하지 못하는 요인들이 다수임을 밝혀냈다. 〈표 Ⅵ-1〉은 Biener, Eling and Wirfs(2015)의 사이버 리스크에 관한 부보 가능성 평가결과를 요약하고 있는데, 해당 리스크의 시장성을 저해하는 가장 큰 요인으로 리스크 간 상관위험, 정보비대칭 문제, 제한적인 보장범위 등을 들 수 있다.

리스크 간 상관위험이 큰 경우 리스크 풀(risk pool) 안에서의 다각화(diversification)를 통한 리스크 감소효과가 작동하지 않아 대수의 법칙이 효과를 내지 못한다.[39] 특히, 리스크의 속성, 양상 등이 빠르게 변화하기 때문에 리스크 간 상관위험의 정도를 판단하는 것이 어렵다. 따라서, 특정 손실사건이 단독으로 무작위하게 발생하기보다 여러 사건들이 연속적으로 발생하거나, 외부로부터 발생하는 단일 공격이 여러 손실사건들을 동시적으로 유발할 수 있다.[40]

두 번째 문제로 정보 비대칭 상황이 존재하는데, 개별 기업의 보안 수준을 보험사에서 정확하게 파악하는 것이 쉽지 않다는 점이 핵심이다. 보험사 입장에서는 디지털/사이버 보안 수준을 파악하기 위한 환경을 갖추지 못한 상태에서 외부 보안업체 등을 통해 인수과정의 도움을 받아야 하고 이는 추가적인 비용이 발생함을 의미한다. 따라서, 인수과정에서의 비용을 효율적으로 관리하기 위해 보안수준에 대한 평가를 최대한 단순하고, 표준화할 수밖에 없고, 이는 리스크 평가의 정확도를 낮추는 결과를 가져올 수 있다. 또한 보안수준 파악의 어려움은 피보험자가 보험 가입 후 보안시스템에 대한 투자를 줄임으로써 손실사건 발생확률을 높일 수 있다는 점에서 도덕적 해이(moral hazard) 문제도 유발될 수 있다.

---

39) 석승훈(2020)은 보험의 기제인 대수의 법칙이 작동하는 원리에 대해서 설명함. 대수의 법칙에서는 기본적으로 각 리스크 간 독립성을 전제로 하기 때문에 상호 의존적 리스크가 존재하는 리스크 풀의 경우 그 크기가 증가하더라도 단위당 위험이 사라지지 않게 됨. 결국 〈그림 Ⅳ-2〉의 비체계적 위험이 기대처럼 감소하지 않고 일정 수준 이상을 유지하는 경우로 수렴하게 됨

40) 단일 공격으로 인해 동시다발적인 손실사건이 유발될 수 있다는 점에서 디지털/사이버 리스크는 시스템 리스크(systemic risk) 성격을 가지고 있음. 이러한 동시다발적 손실사건들이 극단적 손실규모를 유발한다는 점에서 보험사 입장에서는 시장성이 떨어지는 리스크로 판단할 수밖에 없고, 특히 다수의 손실사건이 하나의 보험상품에만 영향을 끼치는 것이 아닌, 서로 다른 보험상품의 보장영역에 속함으로써 예상보다 큰 보장금액이 발생할 가능성이 존재함. Cartagena et al.(2020)은 이러한 리스크를 묵시적 사이버 리스크(silent cyber risk)라고 정의하였음

〈표 Ⅵ-1〉 디지털/사이버 운영리스크의 부보 가능성 평가

평가요인	내용	평가
손실 발생의 무작위성	• 리스크 간 상관위험(correlation risk) 존재 • 리스크 풀(risk pool) 내 다각화 어려움 • 사이버 위험의 빠른 변화양상 및 속도	○
최대가능손실	• 일반적 형태의 운영리스크에 비해 최대가능손실 규모는 더 낮다고 추정 • 보험사 입장에서 낮은 최대보장수준을 통해 최대가능손실 방어 가능	×
사건당 평균손실	• 일반적 형태의 운영리스크에 비해 평균 손실 규모는 더 낮다고 추정 • 피해기업규모, 자기보호수준 등에 따라 차이	×
손실 익스포져	• 디지털/사이버 손실사건 빈도의 증가 • 리스크 유형에 따라 차이	×
정보비대칭	• 보안수준 및 침투기술 등에 대한 정보 차이 • 사이버보험 가입 후 보안투자 감소 등의 도덕적 해이(moral hazard) 발생 가능	○
보험료	• 높은 불확실성으로 인한 높은 사업비 • 지리적, 산업별 큰 차이	△
최대보장수준	• 낮은 보장수준으로 인한 수요 저하 • 보장범위의 제한 및 간접손실/비용 제외	○
공공정책	• 리스크 간 높은 상호 연결 위험 • 사건발생의 탐지 어려움 등으로 보험사기 가능성 높음	△
법적 제한사항	• 위험환경 변화를 법적/제도적 장치가 따라가기 어려운 상황 • 데이터 유출에 대한 피해보상액 확정의 불확실성 존재	△

주: 평가부분에서 ○는 부보 가능성을 저해함을, △는 부보 가능성을 저해할 수 있음을, ×는 부보 가능성을 만족함을 의미함

자료: Eling and Wirfs(2016)의 〈Table 9〉을 재구성함

제한적인 보장수준(특히, 낮은 수준의 최대보장금액) 또한 디지털/사이버 리스크의 시장성을 저해하는 요인이다. Romanosky et al.(2019)은 분석시점 기준으로 현재 미국 사이버보험 시장에서 거래되고 있는 100가지 보험상품에 대한 보장수준을 평가하였다. 해당 연구는 실제 보험상품들이 테러와 관련된 리스크 및 부주의 등에 의한 리스크 등을 보장범위에서 제외하고 있음을 밝혀냈다. 보장범위에 있어 상당히 보수적인 시각이 반영된 점은 최대보장금액을 설정하는 측면에서도 적용되고 있다. Romanosky et al.(2019)에서 밝힌 미국

시장에서의 최대보장금액은 일반적으로 $10million~25million 수준인데 이는 현재 밝혀진 극단적 형태의 디지털/사이버 리스크 사건들의 손실규모와 비교하면 매우 적다.[41]

요약하면, 현재 상황에서 디지털/사이버 운영리스크의 부보 가능성은 여전히 다른 리스크 유형에 비교하여 낮은 편이라고 판단할 수 있다. 앞서 정리한 몇 가지 제한사항은 시장 내에서 자체적으로 해결하기에 아직 부족하다. 더 풍부하고, 자세한 정보를 포함하는 데이터가 축적되어야 하고, 이를 통해 리스크에 대한 이해가 높아짐으로써 시장 참여자가 증가하고, 보장범위에 대한 기업 수요를 만족시킬 만한 공급도 늘어날 수 있다.

2. 리스크 전가 기제의 실효성 향상 방안

그렇다면 부보 가능성을 저해하는 요인들을 어떻게 해결할 수 있고, 극단적 형태의 손실사건을 대비할 현실적인 대안에는 무엇이 있을까? Eling and Wirfs(2016)에서는 디지털/사이버 리스크의 부보 가능성을 향상시키기 위해 5가지 방법을 다음과 같이 제안하였다.

1. 데이터 풀(pool)을 확장하도록 장려할 필요가 있다. 디지털/사이버 운영리스크를 정확히 이해하기 위해서는 이러한 리스크에 의해서 발생한 손실데이터가 충분히 축적되어 통계적 분석이 의미를 가져야 한다. 하지만 현재 세계 어떤 곳에서도 공공 또는 민간 주도의 디지털/사이버 리스크 데이터 풀을 구성하고자 하는 실질적 노력이 관찰되지 않고 있다. 공공 주도로 디지털/사이버 리스크 관련 손실데이터를 공동 축적할 수 있는 제도적 여건이 마련된다면 좀 더 정확한 손실 추정치 및 손실사건들의 특성을 파악할 수 있다.
2. 리스크 경감(risk mitigation) 노력에 대한 최소 조건이 필요하다. 리스크 경감 노력은 대표적으로 보안시스템, 체계에 대한 투자를 통해 손실 발생 확률을 줄일 수 있는 자기보호(self-protection) 기제가 있다. 이러한 리스크 경감 최소 조건 부과 효과는 몇가지 측면에서 부보 가능성을 향상시키는 결과로 이어진다. 먼저 최소 보안수준을 만족해야

41) 예를 들어, 미국의 대표적인 신용보고기관인 Equifax는 2017년 약 1억 5천만 명의 개인정보 유출사건을 경험하였는데, 이에 대한 벌금 및 보상금으로 약 $750million을 지급하기로 2019년 결정되었음. 결정된 보상금의 크기는 Romanosky et al.(2019)에서 분석한 현 사이버보험 상품의 최대보장금액 수준의 30배에서 75배 정도의 차이를 보여줌

하기 때문에 보험상품 구매 후 보안 투자를 줄이는 도덕적 해이를 어느정도 제거할 수 있다. 두 번째로, 개별 기업이 부과된 최소 보안 조건을 만족한다면 사회 전체적으로 디지털/사이버 리스크 사건 발생확률을 낮출 수 있는 공공의 이익(publich good) 향상 효과로 이어질 수 있기 때문에 공공정책 측면에서도 효과가 있다.

3. 데이터 유출 또는 다른 형태의 사이버 공격이 발생했을 시 이를 정부 당국 및 피해자들에게 반드시 보고할 책임을 제도화할 필요가 있다. 손실사건의 보고절차 확립은 데이터 풀을 확장시키고 개별 손실사건의 세부 정보를 파악하는 데 도움이 된다. 현재까지 미국 사이버보험 시장이 유럽의 사이버보험 시장에 비해 압도적으로 큰 규모를 보여주는 이유 중 하나는 미국의 대부분 주들이 사이버 리스크 사건의 보고를 규제화하였기 때문이다.[42] 이렇게 제도화된 절차를 통해 더 구체적이고 광범위한 디지털/사이버 리스크 관련 데이터들이 축적될 수 있다.

4. 전통적 방식의 리스크 전가 기제들을 활용 및 장려할 필요가 있다. 개별 보험사가 디지털/사이버 리스크 인수에 어려움을 겪을 수 있다면 정부 당국의 중재를 통해 다수의 보험사가 풀(pool)을 구성하여 공동보험 형태로 시장 내 해결책을 제공할 수도 있을 것이다. 전통적 방식의 리스크 전가로 보험상품이 대표적이지만, 보험으로 해결할 수 없는 문제를 효율적으로 관리하기 위해서 자본시장 등을 활용할 수도 있다. 예를 들면, 재해재난 리스크를 관리하기 위해 개발된 대재해 채권을 사이버 테러 또는 공격에 의한 손실 방어 기제로서 고려해볼 수 있다.[43] 또한, 재보험사들의 적극적인 위험 인수를 장려하기 위한 공공정책 등을 고민해볼 수 있는데, 예를 들면, 사이버 테러와 관련한 위험 인수 시 보조금 지원 및 절세혜택 부여 등이 있을 수 있다.

5. 마지막으로 정부차원의 극단적 시나리오 설계 및 시뮬레이션 분석, 지원 방안 등을 강구하여 대비할 필요가 있다. 앞서 리스크 분류체계 중 외부사건-제3자 리스크-사회인프라 실패 유형은 공공인프라를 통한 극단적, 시스템 리스크를 유발할 수 있는 손실사건을 포함한다. 이러한 유형의 사건이 발생하게 되면 민간영역 안에서 충분한 대비, 관리, 회복이 이루어지기 쉽지 않기 때문에 공공영역과의 협력이 필수적이다. 정부는 이

42) 유럽의 경우 2018년 5월부터 일반 데이터 보호 규칙(General Data Protection Regulation; GDPR)이 시행되어 데이터 유출 관련 사고 발생 시 반드시 보고해야 하는 규정을 제도화하였음. 이에 따라 유럽 내 발생하는 디지털/사이버 리스크 관련 손실자료들이 과거에 비해 크게 확장될 것으로 기대하고 있음

43) 〈표 Ⅲ-7〉에서 확인할 수 있듯이, 대재해 손실자료의 통계적 특성이 사이버 공격에 의한 손실 자료의 통계적 특성과 동질적이지 않을 수 있으므로 대재해 채권의 구조를 사이버 공격을 기초자산으로 한 채권 구조로 최적화하여 설계하는 것이 필요함

러한 극단적 사건 발생에 대한 시나리오를 설계하고, 스트레스 테스트(stress test)를 통해 피해범위, 영향, 기간 등을 파악하여 사전에 공공/민간 영역 모두에서 대비가 가능하도록 지원해야 한다.

부보 가능성을 향상시키는 데 효과적으로 작동할 수 있는 기제들을 어떻게 효과적으로 개발하고, 시행하여 사회 전반에 큰 영향을 끼칠 수 있는 극단적 사건들을 대비할지는 민간 영역 내 협업 프로그램 또는 공공-민간 협력(Public-Private Partnership; PPP)을 통해 고찰할 필요가 있다.[44] 극단적 형태의 디지털/사이버 리스크 관련 손실사건은 대체적으로 악의적 의도를 가진 대규모 해킹 또는 대형 테러 유형일 가능성이 높다. 정교하고 발전된 해킹 기술을 보유한 해커집단(또는 특정 국가의 훈련된 테러조직)에 의해 발생하는 이러한 유형은 큰 규모의 개별 기업이나 동종 업계(특히, 금융산업) 다수 기업들을 목표로 이루어지는 경향이 있다.

이러한 다수 기업들을 목표로 하여 발생하는 공격으로부터 귀결되는 손실규모는 단일 보험사 입장에서 보장하기 어려운 수준이다. 예를 들어, 2017년에 발생한 Wannacry 랜섬웨어 공격의 경우 약 40억 달러의 손실을 야기한 것으로 평가되고 있으며, Lloyd's(2017)가 추정한 극단적 형태의 사이버 공격에 의한 손실액은 약 1,200억 달러 수준이다. 원수보험료 기준으로 미국 내 가장 큰 손해보험사인 State Farm의 2020년 총 원수보험료 660억 달러[45]와 비교하면 약 2배가량의 손실액이 단일 공격에 의해 발생 가능하다고 산술적인 판단이 가능하다.

단일 보험사가 보장하기 어려운 극단적 디지털/사이버 운영리스크 손실사건을 관리하기 위한 방법으로 자연재난 또는 테러리스크를 관리하는 방법을 참조할 수 있다. 〈표 Ⅵ-2〉는 극단적 형태의 자연재난 또는 테러리스크를 관리하는 방법을 민간 협력 및 공공영역의 개입 등으로 세분화하여 사례와 함께 보여준다. 우선, 민간영역에서의 협력 방안으로 자발적인 리스크 풀(risk pool) 구성과 공동보험 프로그램을 생각해볼 수 있다. 독일의 Friendsurance나 멕시코의 농업공동보험기구(f armer mutual insurance funds; Fondos) 등이 자발적인 리스크 풀의 사례로 볼 수 있는데, 해당 프로그램은 리스크 보유자(risk owners)들이 상호 합의하에 보험기능의 기금을 마련하여 잠재적 손실사건을 방어하는 기

44) 이 장의 내용은 Eling and Wirfs(2016)의 사이버 리스크 전가 방법 및 Jung(2021)에서 논의한 PPP를 통한 극단적 디지털/사이버 리스크 관리를 기초로 작성되었음

45) National Association of Insurance Commissioners(NAIC)의 데이터를 참조함

제이다. 산업전반에 걸친 리스크 풀(industry-wide risk pool) 구성도 하나의 대안이 될 수 있다. 이는 자발적인 리스크 풀에 비해 더 많은 수의 동질적 리스크 보유자들을 참여시켜 대수의 법칙이 기능할 수 있는 환경이 가능하다는 점에서 유리하다. 다만, 이러한 민간영역에서의 리스크 보유자들 간 협력관계는 극단적 형태의 사건이 발생했을 시 다수의 참여자가 피해에 노출될 가능성이 있고, 제도나 중재자가 없기 때문에 도덕적 해이, 정보 비대칭성 등의 시장실패 문제가 대두될 수 있다.

사이버보험을 판매하는 원수보험사들 간 공동보험이나 재보험사들 간의 공동재보험도 활용가능한 관리방안이다. 공동보험 또는 공동재보험 프로그램은 기본적으로 프로그램 참여자들이 공동으로 리스크를 인수하고 관리하는 방식이다(European Commission 2014). 참여자들은 어떤 리스크를 인수할지와 어떤 방식으로 인수할지에 대해서 우선 결정하는데, 주도적인 입장의 보험사가 특정 비율만큼을 인수하고 나머지 부분에 대해서 참여보험사들이 적정비율로 인수하는 형태가 일반적이다. 공동 (재)보험은 (재)보험사들 입장에서 상대적으로 적은 보험료 수입이 발생하지만, 극단적 형태의 손실을 경험할 경우 잠재적인 피해액이 분산되는 효과를 기대할 수 있다. 디지털/사이버 운영리스크와 같이 리스크의 불확실성이 크고, 데이터의 수가 적은 경우 공동 (재)보험은 단순히 리스크의 공동인수를 넘어서서 기술적 측면에서도 상호 도움이 될 수 있다. 다만, 디지털/사이버 리스크와 같이 보험상품의 표준약관 등이 가용하지 않고, 모호성이 많은 경우 얼마나 많은 참여자를 프로그램으로 유도할 수 있을지에 대한 의문이 남아있다.

마지막으로 국가가 직접 개입함으로써 극단적 형태의 리스크 사건을 관리할 수 있는 프로그램을 지원하는 방법이다. 먼저, 국가가 직접 시장에 세제 지원 및 제도적 차원에서의 지원을 제공하는 방법이 있다. 이 방법의 경우 디지털/사이버 리스크를 전가할 수 있는 보험시장을 성장시키기 위한 목적으로 시행된다. 다른 유형으로는 정부가 직접 원수보험사 또는 재보험사로서 시장에 참여하는 방법이다. 의무보험 형태로 보장을 제공할 수도 있고, 극단적 형태의 손실인 경우 일정 수준(임계점) 이상의 손실에 대해서 인수하는 방법이 될 수 있다.

자연재난 또는 테러리스크의 경우 전 세계에서 다양한 국가 프로그램 사례를 관찰할 수 있다. 대표적으로, 미국 연방재난관리청(Federal Emergency Management Agency; FEMA)에서 제공하는 국가홍수보험제도(National Flood Insurance Program; NFIP)가 있다. 이 프로그램은 허리케인이나 수해가 잦은 지역 중심으로 일반적인 주택보험(Homeowners

insurance)이 보장하지 못하는 피해를 줄이려는 목적으로 설계되어 저렴한 보험료를 통해 극단적 재정피해를 만회할 수 있는 기제를 제공한다. 테러리스크의 경우 다양한 국가에서 국가보험 형태로 보장이 제공되는데, 예를 들면, 영국의 Pool RE, 미국의 TRIA, 벨기에의 TRIP와 네덜란드의 NHT 등이 있다. 국가(재)보험 프로그램은 시장과의 협력을 통해 잠재적 시장실패를 국가가 직접 개입하여 피해를 최소화하는 기능을 제공한다는 점에서 공공-민간 협력(PPP)의 대표적인 기제가 될 수 있다.

〈표 Ⅵ-2〉 극단적 형태의 리스크 관리 대안

유형	내용	사례
자발적 리스크 풀 (Private risk pool)	• 동질적인 리스크에 노출된 기업들이 자발적으로 공동 리스크 풀을 구성하여 운영 • 산업전반 리스크 풀도 가능(industry-wide risk pool)	• Friendsurance(독일) • Fondos(멕시코)
공동(재)보험 (Co-(re)insurance)	• 공동으로 리스크를 인수하고 관리하는 프로그램 • 극단적 리스크 사건을 관리하는 데 도움 • 공동 인수 이외 기술적 측면에서의 협업 가능 • 모호성이 많은 리스크의 경우 참여자 유도 어려움	• VOV 공동보험(독일) • Swiss Natural Perils Pool(스위스) • GAREAT(프랑스) • Pool Inquinamento(이탈리아)
국가보험(의무보험)/ 국가재보험 (National program)	• 직접지원의 경우, 보험시장 발전을 위한 세제혜택 또는 제도적 지원 가능 • 간접지원의 경우, 의무보험 제공 또는 최후보루로서 임계점 초과 손실 인수자 역할 등이 가능	• National Flood Insurance Program(NFIP; 미국) • Pool RE(영국) • Terrorism Risk Insurance Act(TRIA; 미국) • Terrorism Reinsurance & Insurance Pool(TRIP; 벨기에) • Dutch Terrorism Reinsurance Pool(NHT; 네덜란드)

자료: European Commission(2014), Eling and Wirfs(2016), Jung(2021)을 참조함

3. 결언

본 보고서는 금융산업(은행 및 보험업)이 경험하고 있는 디지털 전환의 양상을 살펴보고, 디지털/사이버 환경에서의 운영리스크 형태와 분류체계를 연구하였다. 디지털 리스크 또는 사이버 리스크는 운영리스크의 유형으로서 해당 리스크에 노출된 기업 입장에서는 이에 대한 이해가 충분히 이루어져야 함에도 불구하고, 기업뿐만 아니라 해당 리스크를 인수하고자 하는 보험사들 입장에서도 해당 리스크의 불확실성과 모호성으로 인해 관리체계 확립에 어려움을 겪고 있다. 특히, 금융산업의 경우 돈과 신뢰를 바탕으로 하는 사업모델하에서 디지털/사이버 리스크에 상대적으로 더 많이 노출되어 있을 뿐만 아니라, 대규모 손실사건 발생 시 입게 될 잠재적 피해규모가 상당할 것으로 예상된다.

본 보고서는 디지털/사이버 환경에서의 운영리스크에 관한 이해를 높이고, 대응 방안을 제시하고자 구체적인 분류체계 연구와 더불어 리스크 관리체계에 대한 이론적 고찰과 최신 데이터를 활용한 실증분석을 진행하였다. 특히, 은행 및 보험회사가 적용 및 운영하고 있는 디지털 전환 사례들을 종합하였고, 해외 디지털 또는 사이버 보안 리스크 분류체계 관련 문헌들을 참고하여 대분류-소분류-요인으로 체계화된 리스크 환경(risk landscape)을 제시하였다. 디지털/사이버 리스크로 인한 손실자료를 활용하여 리스크 유형별 빈도/심도 수준을 평가하는 리스크 매트릭스(risk matrix/risk map)를 제안하였다. 이러한 데이터 기반(data-driven) 리스크 평가모델은 기존의 시나리오 기반 정성 모델(scenario-based qualitative model)을 보완하고, 머신러닝 및 딥러닝 기반 모델이 적용된 정량적 리스크 평가의 가능성을 보여준다는 점에서 시사하는 바가 크다. 이는 기존의 전사적 리스크 관리(Enterprise risk management) 체계가 빅데이터, AI 기술이 접목된 목적지향 리스크 관리(targeted risk management)로 향상될 수 있는 가능성을 의미한다.

서론에서 언급했듯이, 금융기업들은 현 기술발전의 속도와 산업으로의 적용 과정 속에서 역동적인 리스크 환경(risk dynamics)을 직면하고 있고, 경쟁에서 살아남기 위해 리스크 환경을 감내해야 하는 상황 속에 놓여있다. 이러한 상황에서 누가 앞서 기술한 효과적인 리스크 관리체계를 발전·적용시킬 수 있는지, 이를 통해 비용을 감소시키고, 궁극적으로 기업가치 제고를 성취하여 시장에서 선도적 역할을 할지는 의사결정자들의 전향적 인식 전환에 달려있다고 할 수 있다. 전사적 디지털 리스크 관리체계 확립을 위한 최고 리스크 관리책임자(Chief Risk Officer; CRO)의 권한을 늘리고, 실시간 리스크 감지체계를 통해 의사결정자들에게 주기적인 보고가 이루어지도록 효율적 리스크 의사소통 시스템을 갖출

필요가 있다. 기업 입장에서 충분한 재정적 지원을 제공하여 이러한 관리체계가 올바르게 확립된다면 장기적인 관점에서 극단적 형태의 손실 영향을 줄이고, 비용을 줄이는 효과를 얻을 수 있다고 기대한다.

참고문헌

금융보안원(2017), 「국내·외 금융권 머신러닝 도입 현황」

김규동·김윤진(2021), 「보험산업의 디지털 전환 현황과 과제」, 『KIRI 리포트』, 보험연구원

김덕수·이석우(2016), 『인크립션』

김은석·김영준(2019), 「인슈어테크 디지털 보험플랫폼서비스의 사용자 수용의도에 관한 연구」, 『경영학연구』, 48호

김학용(2021), 「크로스 플랫폼이 주도하는 플랫폼 경제」, 소프트웨어정책연구소

김회민(2018), 「KB 지식 비타민: VR/AR 기술을 활용한 차세대 금융서비스 사례」, KB금융지주 경영연구소

문장원·윤형진·선미란(2019), 「해외 디지털 헬스케어 규제개선 동향」, 『이슈리포트』, 37호, 정보통신산업진흥원

박소정·박지윤(2017), 「인슈어테크: 현황 점검 및 과제 고찰」, 『KIRI 리포트』, 보험연구원

보험개발원(2017), 「금융회사 가치와 자본관리」

보험경영연구회(2019), 『리스크와 보험』, 보험경영연구회

석승훈(2020), 「위험한 위험: 위험학으로의 초대」

선우석호·전은영(2006), 「운영리스크 추정과 손실분포 적합성 검증」, 한국금융연구원

설태현·강대승(2020), 「금융권의 디지털 전환 가속화 대비하기」, DB금융투자

윤혜영(2018), 「증강현실 콘텐츠의 유형 연구」, 『인문콘텐츠』, 49호, 인문콘텐츠학회

이재원·오상진(2020), 「인공지능 기술 기반 인슈어테크와 디지털보험플랫폼 성공사례 분석: 중국 평안보험그룹은 중심으로」, 『지능정보연구』, 26호

이혁성(2019), 「양자컴퓨터 기술 동향 및 산업 응용」, 『한국콘텐츠학회지』, 17호

이효섭(2019), 『디지털 혁신을 위한 한국 금융투자업계의 과제』, 자본시장연구원

장효미(2019), 「국내외 인슈어테크 시장 현황 및 시사점」, 『자본시장포커스』, 20호, 자본시장연구원

정민기·김중한(2020), 『소프트뱅크가 투자한 인슈어테크 유망주』, 삼성증권

조영현·이혜은(2018), 「주요 인슈어테크 기업 사례와 시사점」, 『KIRI 리포트』, 보험연구원

최창희·이규성·한성원(2017), 「중국 중안보험 인슈테크 사례의 시사점」, 『KIRI 리포트』, 보험연구원

한상열(2021), 「메타버스 플랫폼 현황과 전망」, 『미래연구 포커스』, 49호, 과학기술정책연구원

KPMG(2019), 「글로벌 증권산업의 디지털 혁신 동향과 국내 시사점」, 『Issue Monitor』, 101호, KPMG

_____(2021), 「은행산업에 펼쳐지는 디지털 혁명과 금융패권의 미래」, 『Samjong Insight』, 73호, KPMG

Aldasoro, I., Gambacorta, L., Giudici, P., and Leach, T.(2020), Operational and Cyber risks in the Financial Sector, Bank For International Settlements, Working paper, No. 840

Berliner, B.(1985), "Limits of insurability of risks", *The Geneva Papers on Risk and Insurance*, 10(37), pp. 313~329

Bharadwaj, A., Keil, M., and Mähring, M.(2009), "Effects of information technology failures on the market value of firms", *The Journal of Strategic Information Systems*, 18(2), pp. 66~79

Biener, C., Eling, M., and Wirfs, J. H.(2015), "Insurability of Cyber Risk: An Empirical Analysis", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), pp. 131~158

Bishop, T., and Karne, R.(2003), *A survey of middleware, Computers and Their Applications*, pp. 254~258

Böhme, R., Laube, S., and Riek, M.(2019), "A fundamental approach to cyber risk analysis", *Variance*, 12(2), pp. 161~185

Braun, A., and Schreiber, F.(2017), The Current InsurTech Landscape: Business Models and Disruptive Potential(No. 62), Institute of Insurance Economics, University of St. Gallen

Cartagena, S., Gosrani, V., Grewal, J., and Pikinska, J.(2020), "Silent Cyber Assessment Framework", *British Actuarial Journal*, 25, pp. 1~19

Cebula, J. J., and Young L. R.(2014), *A Taxonomy of Operational Cyber Security Risks Version 2,* Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst

De Mauro, A., Greco, M., and Grimaldi, M.(2016), "A formal definition of Big Data based on its essential features", *Library Review*

Delfs, H., and Knebl, H.(2015), Symmetric-key cryptography, In Introduction to Cryptography, Springer: Heidelberg, pp. 11~48

Dionne, G.(2019), *Corporate risk management: Theories and applications,* John Wiley & Sons: New Jersey

Edwards, B., Hofmeyr, S., and Forrest, S.(2016), "Hype and Heavy tails: A Closer Look at data breaches", *Journal of Cybersecurity*, 2(1), pp. 3~14

Ehrlich, I., and Becker, G. S.(1972), "Market insurance, self-insurance, and self-protection", *Journal of political Economy*, 80(4), pp. 623~648

Eisenbach, T. M., Konver, A., and Lee, M. J.(2020), "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis", *FRB of New York Staff Report*

Eling, M., and Jung, K.(2018), "Copula approaches for modeling cross-sectional dependence of data breach losses", *Insurance: Mathematics and Economics*, 82, pp. 167~180

Eling, M. and Wirfs, J. H.(2016), Cyber Risks: Too Big to Insure? Risk transfer options for a mercurial risk class(No. 59), Institute of Insurance Economics, University of St. Gallen

_____(2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, 272(3), pp. 1109~1119

European Commission.(2014), Study on co(re)insurance pools and on ad-hoc co(re)insurance agreements on the subscription market, European Commission: Luxembourg

Evans, D. L., Drew, J. H., and Leemis, L. M.(2008), "The distribution of the Kolmogorov–Smirnov, Cramer–von Mises, and Anderson–Darling test statistics for exponential populations with estimated parameters", *Communications in Statistics-Simulation and Computation*, 37(7), pp. 1396~1421

Financial Stability Board.(2017), *Financial Stability Implications from Fintech*, Financial Stability Board

Flage, R., and Aven, T.(2015), "Emerging Risk-Conceptual Definition and a Relation to Black Swan Type of Events", *Reliability Engineering & System Safety*, 144, pp. 61~67

GhasemiGol, M., Ghaemi-Bafghi, A., and Takabi, H.(2016), "A comprehensive approach for network attack forecasting", *Computers & Security*, 58, pp. 83~105

Gordon, L. A., and Loeb, M. P.(2002), "The Economics of Information Security Investment", *ACM Transactions on Information and System Security(TISSEC)*, 5(4), pp. 438~457

Hahn, A., Ashok, A., Sridhar, S., and Govindarasu, M.(2013), "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid", *IEEE Transactions on Smart Grid*, 4(2), pp. 847~855

Hall, S., Hobson, D., Lowe, A., and Willis, P.(2003), Culture, media, language: working papers in cultural studies, pp. 1972~1979, Routledge

Heckerman, D.(2008), "A tutorial on learning with bayesian networks", *Innovations in Bayesian Networks*, pp. 33~82

Hull, J. C.(2020), *Machine Learning in business: An introduction to the world of data science*, Amazon Distribution

Humayed, A., Lin, J., Li, F., and Luo, B.(2017), "Cyber-physical systems security-A survey", *IEEE Internet of Things Journal*, 4(6), pp. 1802~1831

Hurst, D.(2021. 9. 14), "'Significant threat': cyber attacks increasingly targeting Australia's critical infrastructure", The Guardian, Retreived from https://www.

theguardian.com/technology/2021/sep/15/significant-threat-cyber-attacks-increasingly-targeting-australias-critical-infrastructure

Hwang, T.(2018), Computational power and the social impact of artificial intelligence, Working paper

International Monetary Fund.(2017), *Fintech and financial services: Initial considerations*, International Monetary Fund

International Risk Governance Council.(2011), "Improving the Management of Emerging Risks: Risks from New Technologies, System Interactions, and Unforeseen or Changing Circumstances", International Risk Governance Council: Geneva

Jung, K.(2021), "Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk", *North American Actuarial Journal*, pp. 1~24

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., and Stulz, R. M.(2021), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of Financial Economics*, 139(3), pp. 719~749

Kaffenberger, L., and Kopp, E.(2019), "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment", Carnegie Endowment for International Peace

Koh, T. K., and Fichman, M.(2014), "Multihoming users' preferences for two-sided exchange networks", *MIS Quarterly*, 38(4), pp. 977~996

KPMG(2017), "2017 Fintech 100: Leading global fintech innovators", KPMG

Lloyd's.(2017), "Counting the cost: Cyber exposure decoded", Lloyd's: London

Lloyd's.(2018), "Cloud down: Impacts on the US economy", Lloyd's: London

Louisot, J. P., and Ketcham, C. H.(2014), *ERM-enterprise risk management: issues and cases*, John Wiley & Sons: New Jersey

McKinsey(2020), "McKinsey on Risk: New Risk Challenges and Enduring Themes for the Return", McKinsey

Moscadelli, M.(2004), The modelling of operational risk: experience with the analysis of the data collected by the Basel Committee, Working paper

Muermann, A., and Kunreuther, H.(2008), "Self-protection and insurance with interdependencies", *Journal of Risk and Uncertainty*, 36(2), pp. 103~123

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K.(2013), "Cyber-risk decision models: To insure IT or not?", *Decision Support Systems*, 56, pp. 11~26

Murray, W. H.(1995), "Modern cryptography", *Information Systems Security*, 3(4), pp. 30~33

Paté-Cornell, M. E., Kuypers, M., Smith, M., and Keller, P.(2018), "Cyber risk management for critical infrastructure: a risk analysis model and three case studies", *Risk Analysis*, 38(2), pp. 226~241

Pinckney, N., Harris, D. M., Jiang, N., Kelley, K., Antao, S., and Sousa, L.(2017), "Public key cryptography", *In Circuits and Systems for Security and Privacy*

Qiu, D., Li, B., and Leung, H.(2016), "Understanding the API usage in Java", *Information and software technology*, 73, pp. 81~100

Romanosky, S., Ablon, L., Kuehn, A., and Jones, T.(2019), "Content analysis of cyber insurance policies: How do carriers price cyber risk?", *Journal of Cybersecurity*, 5(1), pp. 1~19

Schroeder, B., and Gibson, G. A.(2009), "A large-scale study of failures in high-performance computing systems", *IEEE Transactions on Dependable and Secure Computing*, 7(4), pp. 337~350

Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., and Njilla, L. L.(2018), "Reducing informational disadvantages to improve cyber risk management", *The Geneva Papers on Risk and Insurance-Issues and Practice*, 43(2), pp. 224~238

Shevchenko, P. V.(2010), "Implementing loss distribution approach for operational

risk", *Applied Stochastic Models in Business and Industry*, 26(3), pp. 277~307

Sitaram, D., and Manjunath, G.(2011), *Moving to the cloud: Developing apps in the new world of cloud computing*, Elsevier: Waltham

Stulz, R. M.(2019), "Fintech, bigtech, and the future of banks", *Journal of Applied Corporate Finance*, 31(4), pp. 86~97

Wei, L., Li, J., and Zhu, X.(2018), "Operational loss data collection: A literature review", *Annals of Data Science*, 5(3), pp. 313~337

Wheatley, S., Maillart, T., and Sornette, D.(2016), "The extreme risk of personal data breaches and the erosion of privacy", *The European Physical Journal B*, 89(1), pp. 1~12

부록 Ⅰ

디지털 전환 사례와 리스크 분류체계 매핑

〈부록 표 Ⅰ-1〉 은행 프론트 오피스 디지털 전환 사례와 리스크 분류

구분	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
	소분류	리스크 동인	손실유형	하위유형
고객 금융데이터 기반 맞춤형 서비스	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
머신러닝 기반 ETF	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 처리절차 실패 • 의견 불일치 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
오픈 API 플랫폼 기반 금융 서비스	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 상호운용성 결여 • 처리절차 실패 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
분류총계	5가지 유형	13가지 요인	3가지 유형	4가지 요인

〈부록 표 Ⅰ-2〉 은행 미들 오피스 디지털 전환 사례와 리스크 분류

구분	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
	소분류	리스크 동인	손실유형	하위유형
초부유층 투자자 대상 통합 플랫폼	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 보안 취약성 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 의견 불일치 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
인공지능 기반 금융분석 서비스	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 호환성 문제 • 환경설정 문제 • 보안 취약성 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 시스템 복잡성 • 처리절차 실패 • 소통 실패 • 의견 불일치 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
AI 및 빅데이터 기반 약관 심사 솔루션	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 법적 리스크 • 경영 리스크	• 호환성 문제 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 시스템 복잡성 • 처리절차 실패 • 검토의 부적절성 • 주기적 검토 실패 • 규정 위반 • 신규 법률 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
분류총계	6가지 유형	18가지 요인	3가지 유형	5가지 요인

〈부록 표 Ⅰ-3〉 보험 가치사슬별 디지털 전환 사례와 리스크 분류(진단, 상품기획/설계)

보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
보험진단/분석	보험 내용 비교 및 필요상품 추천	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 방해/교란 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱 • 거래상대방
상품기획/설계	사물인터넷, 빅데이터 기반 운전자 운선 습관에 따른 보험료 책정	• 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 수행능력 결여 • 관리 부족 • 수명초과 • 호환성 문제 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 시스템 복잡성 • 처리절차 실패 • 설명 부족 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
	AI 및 빅데이터 기반 보험 오퍼레이션 모델	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 법적 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 처리절차 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 신규 법률 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱

〈부록 표 Ⅰ-3〉 계속

보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
상품기획/설계	사물인터넷 기반 건강관리 서비스	• 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 법적 리스크 • 경영 리스크	• 수행능력 결여 • 관리 부족 • 수명초과 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 시스템 복잡성 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 규정 위반 • 신규 법률 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
	빅데이터 기반 생명보험료 산출	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 법적 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 문제 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 처리절차 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 규정 위반 • 신규 법률 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
분류총계		9가지 유형	25가지 요인	4가지 유형	7가지 요인

〈부록 표 Ⅰ-4〉 은행 백 오피스 디지털 전환 사례와 리스크 분류

구분	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
	소분류	리스크 동인	손실유형	하위유형
머신러닝 기반 자금세탁 및 테러자금 감지 및 예방 솔루션	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 시스템 복잡성 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
AI 기반 직원 모니터링	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 처리절차 실패 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
블록체인 기반 청산결제 서비스	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 법적 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 처리절차 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 신규 법률 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
분류총계	6가지 유형	14가지 요인	3가지 유형	4가지 요인

〈부록 표 Ⅰ-5〉 보험 가치사슬별 디지털 전환 사례와 리스크 분류(상품 조회/가입)

보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
상품 조회/가입	디지털 플랫폼 기반 보험상품 비교 서비스	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 방해/교란 • 호환성 문제 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱 • 거래상대방
	인공지능 기반 역경매형 보험상품 비교 서비스	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 방해/교란 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱 • 거래상대방
	인공지능 기반 챗봇 서비스	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱

〈부록 표 Ⅰ-5〉 계속

보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
상품 조회/가입	이통사 및 카카오톡 간편 결제 서비스	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 절도/파손 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 외부사취 • 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 외부 절도 및 사기 • 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
	카카오톡 메신저 기반 간편인증	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크	• 사기/기만 • 절도/파손 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패	• 외부사취 • 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 외부 절도 및 사기 • 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 모니터링과 보고
	지문인증 기술 기반 전자서명 시스템	• 악의 리스크 • 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 절도/파손 • 수행능력 결여 • 관리 부족 • 수명초과 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 외부사취 • 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 외부 절도 및 사기 • 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱 • 거래상대방
분류총계		7가지 유형	21가지 요인	5가지 유형	9가지 요인

〈부록 표 Ⅰ-6〉 보험 가치사슬별 디지털 전환 사례와 리스크 분류(보상청구, 대출)

보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
보상청구	스마트폰 앱 기반 실손보험 청구대행	• 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 수행능력 결여 • 관리 부족 • 수명초과 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여 • 거래상대방 실패	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱 • 거래상대방
	AI 기반 지급보험금 결정 및 청구 시스템	• 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
	빅데이터 및 사물인터넷 기반 보험 신청 및 청구 절차 간소화	• 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 수행능력 결여 • 관리 부족 • 수명초과 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱

〈부록 표 Ⅰ-6〉 계속

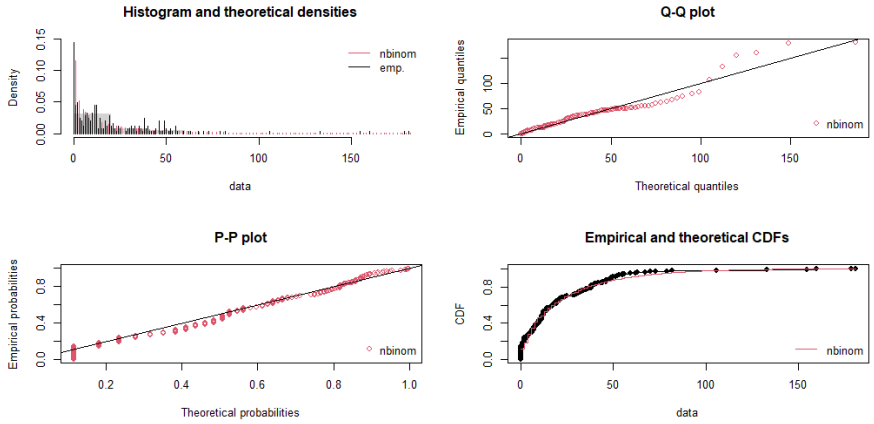
보험 가치사슬	예시	디지털 운영리스크 분류기준		바젤 운영리스크 분류기준	
		소분류	리스크 동인	손실유형	하위유형
보상청구	인공지능 기반 자동차 사고 수리비 자동견적 시스템	• 악의 리스크 • 하드웨어 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 절도/파손 • 수행능력 결여 • 관리 부족 • 수명 초과 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 외부사취 • 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 외부 절도 및 사기 • 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
대출	빅데이터 기반 대출 신용평가 점수모델링	• 악의 리스크 • 소프트웨어 리스크 • 시스템 오류 리스크 • 프로세스 설계 리스크 • 프로세스 통제 리스크 • 경영 리스크	• 사기/기만 • 방해/교란 • 절도/파손 • 환경설정 문제 • 프로그래밍 설계 • 테스트 문제 • 시스템 부적합성 • 개발소통 부족 • 상호운용성 결여 • 처리절차 실패 • 소통 실패 • 검토의 부적절성 • 측정 오류 • 주기적 검토 실패 • 공급자 실패 • 시장 경쟁력 결여	• 내부사취 • 영업중단 및 시스템 장애 • 고객, 상품 및 영업관행 • 집행, 전달 및 절차의 관리	• 내부 절도 및 사기 • 권한없는 행위 • 시스템 장애 • 적합성, 공시 및 신의 성실 의무 • 상품 결함 • 모니터링과 보고 • 공급업체와 아웃소싱
분류총계		7가지 유형	22가지 요인	5가지 유형	9가지 요인

부록 Ⅱ

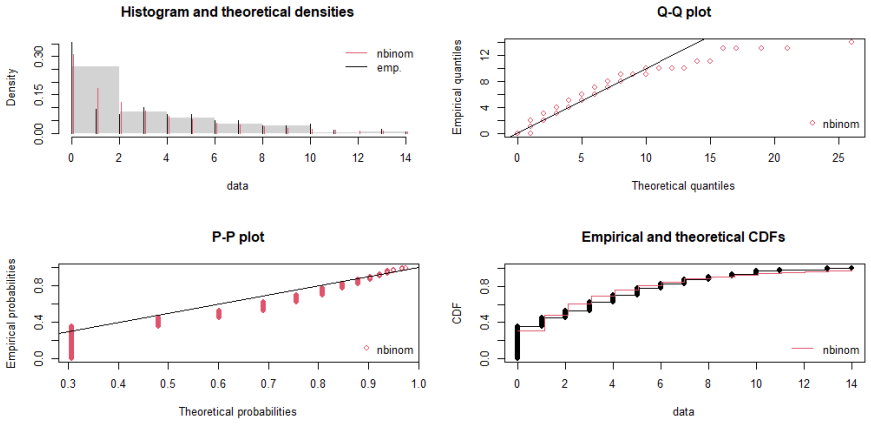
손실분포 적합성 검정 결과

〈부록 그림 Ⅱ-1〉 손실 빈도 분포 적합성 그래프 진단(금융기업)

〈악의적 리스크 손실 빈도 그래프 진단〉



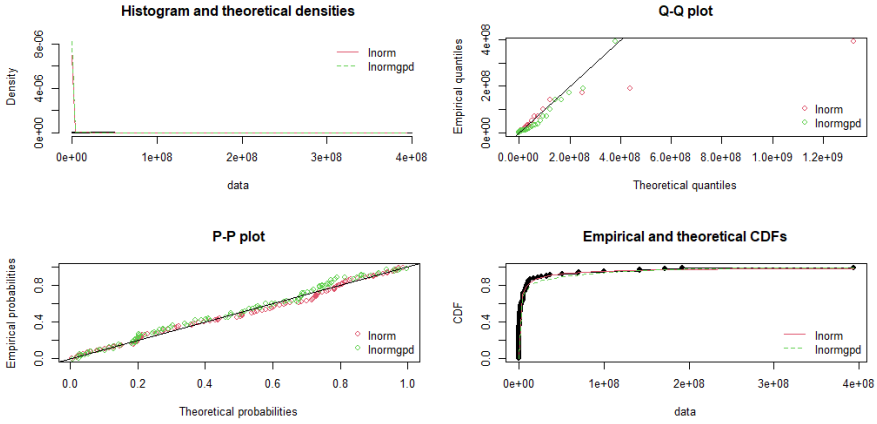
〈비악의적 리스크 손실 빈도 그래프 진단〉



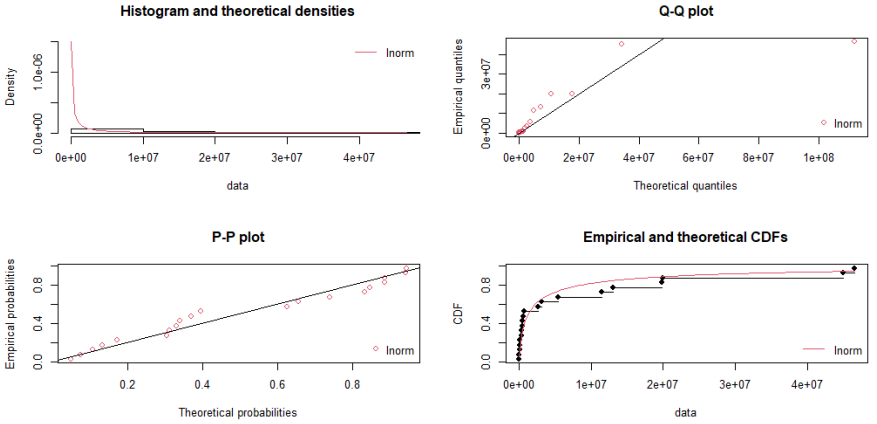
주: 〈표 Ⅴ-5〉의 적합분포(음이항분포)에 관하여 빈도그래프(좌측 상단), Q-Q plot(우측 상단), P-P plot(좌측 하단), CDF plot(우측 하단)을 통해 진행함

〈부록 그림 Ⅱ-2〉 손실 심도 분포 적합성 그래프 진단(금융기업)

〈악의적 리스크 손실 심도 그래프 진단〉



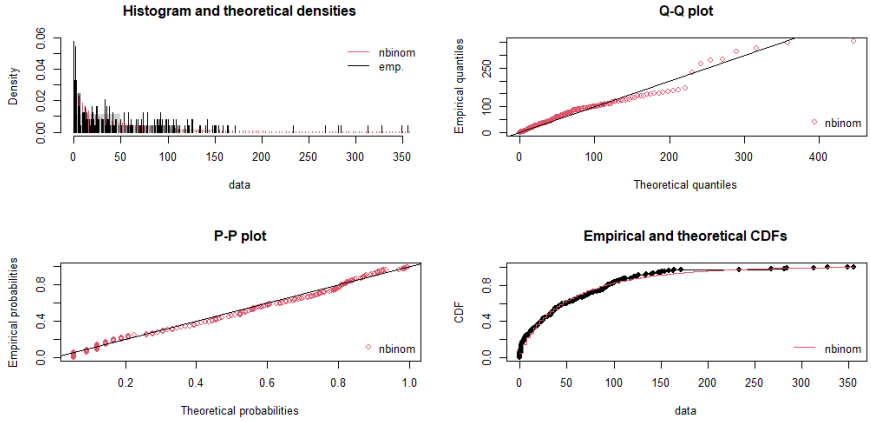
〈비악의적 리스크 손실 심도 그래프 진단〉



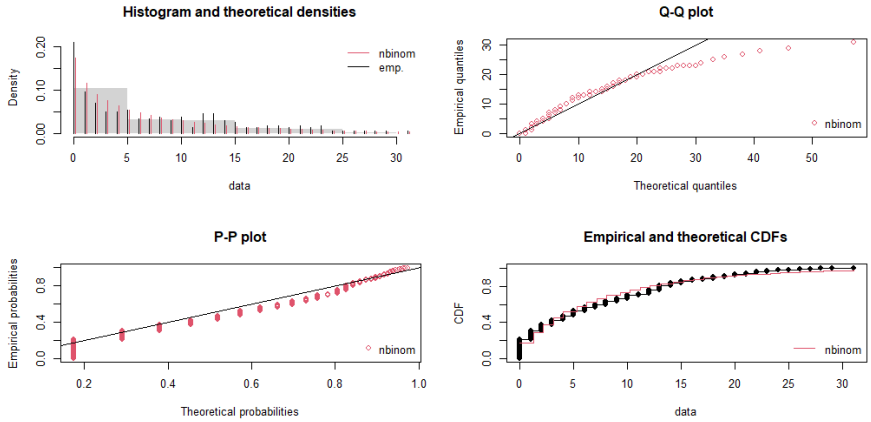
주: 〈표 Ⅴ-6〉의 적합분포(로그정규분포)에 관하여 빈도그래프(좌측 상단), Q-Q plot(우측 상단), P-P plot(좌측 하단), CDF plot(우측 하단)을 통해 진행함. 악의적 리스크의 경우 POT 방법에 의한 그래프도 도식함

〈부록 그림 Ⅱ-3〉 손실 빈도 분포 적합성 그래프 진단(비금융기업)

〈악의적 리스크 손실 빈도 그래프 진단〉



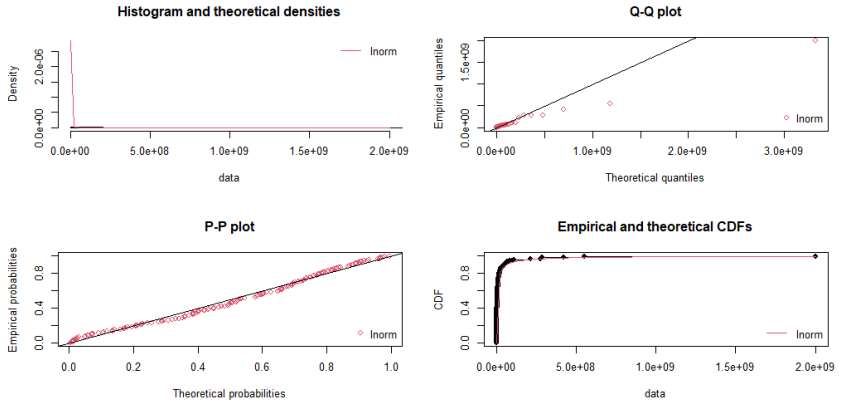
〈비악의적 리스크 손실 빈도 그래프 진단〉



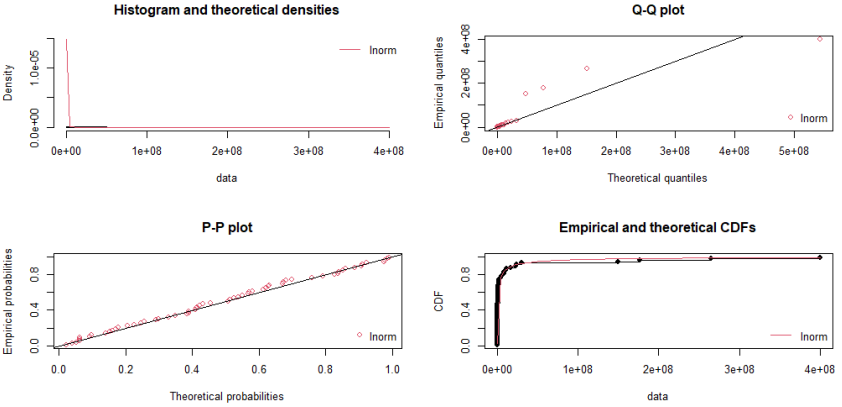
주: 〈표 Ⅴ-5〉의 적합분포(로그정규분포)에 관하여 빈도그래프(좌측 상단), Q-Q plot(우측 상단), P-P plot(좌측 하단), CDF plot(우측 하단)을 통해 진행함. 악의적 리스크의 경우 POT 방법에 의한 그래프도 도식함

〈부록 그림 Ⅱ-4〉 손실 심도 분포 적합성 그래프 진단(비금융기업)

〈악의적 리스크 손실 심도 그래프 진단〉



〈비악의적 리스크 손실 심도 그래프 진단〉



주: 〈표 Ⅴ-6〉의 적합분포(로그정규분포)에 관하여 빈도그래프(좌측 상단), Q-Q plot(우측 상단), P-P plot(좌측 하단), CDF plot(우측 하단)을 통해 진행함. 악의적 리스크의 경우 POT 방법에 의한 그래프도 도식함

도서회원 가입안내

회원	연회비	제공자료	
법인 회원	₩300,000원	- 연구보고서 - 기타보고서 - 연속간행물 · 보험금융연구 · 보험동향 · 해외 보험동향 · KOREA INSURANCE INDUSTRY	영문 연차보고서 추가 제공
특별 회원	₩150,000원		
개인 회원	₩150,000원		

* 특별회원 가입대상 : 도서관 및 독서진흥법에 의하여 설립된 공공도서관 및 대학도서관

가입 문의

보험연구원 도서회원 담당
전화 : (02)3775-9113 | 팩스 : (02)3775-9102

회비 납입 방법

무통장입금
- 계좌번호 : 국민은행 (400401-01-125198) | 예금주: 보험연구원

자료 구입처

서울 : 보험연구원 자료실(02-3775-9113 | lsy@kiri.or.kr)

저자약력

정광민 University of St. Gallen 금융학 박사 (리스크 관리 및 보험 전공) /
포항공과대학교 산업경영공학과 조교수
E-mail : kwjung@postech.ac.kr

연구보고서 2021-07

금융산업의 디지털 전환과 운영리스크
-은행과 보험산업 중심으로-

발 행 일 2021년 11월
발 행 인 안 철 경
발 행 처 보험연구원
주 소 서울특별시 영등포구 국제금융로 6길 38 화재보험협회빌딩
인 쇄 소 고려씨엔피

ISBN 979-11-89741-59-4 (정가 10,000원)
979-11-85691-50-3(세트)