참고 8.

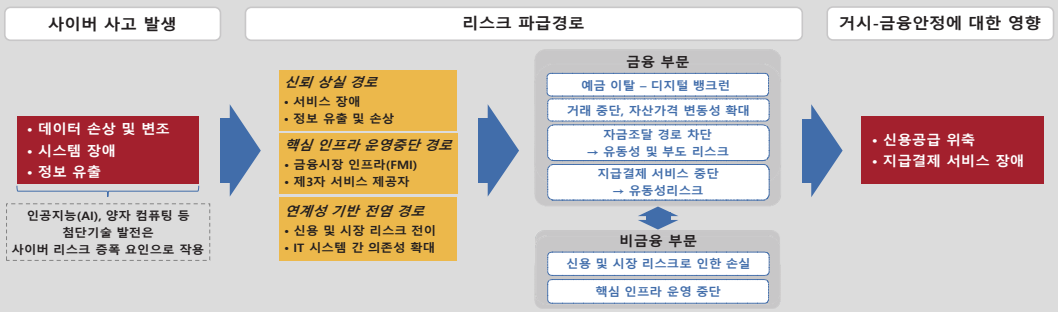
사이버 리스크가 금융안정에 미치는 영향 및 주요국 대응방향[223]

최근 국내 통신사의 유심(USIM) 서버 해킹, 미국 가상자산 거래소의 내부자 연루 해킹 등 사이버 공격이 연이어 발생하면서 사이버 리스크에 대한 우려가 높아지고 있다.[224] 동 사건들은 사이버 리스크가 기술적·인적 취약점을 통해 개인정보 유출, 자산 탈취 등 다양한 방식으로 현실화될 수 있음을 보여준다. 아직까지 금융시스템 안정성이 실질적으로 훼손된 사례는 드물지만 사이버 리스크가 금융안정에 중대한 영향을 미칠 수 있다는 인식이 국내외 금융권 전반으로 확산되고 있다. 이에 본고에서는 사이버 리스크가 금융안정에 미치는 영향과 주요국의 대응방향을 살펴보고 정책적 시사점을 도출하였다.

사이버 리스크가 금융안정에 미치는 영향

금융안정위원회(FSB)[225]는 사이버 리스크를 "정보시스템에서 처리·저장·전송되는 정보의 기밀성, 무결성, 가용성에 부정적 영향을 미치는 사이버 사고로 인해 금융기관에 운영리스크나 손실이 발생할 수 있는 위험"으로 정의한다. 최근 들어 사이버 리스크는 개별기관 차원의 위험을 넘어, 금융시스템 전반의 안정성을 위협할 수 있는 거시적 리스크로 부각되고 있다. 이에 IMF의 글로벌금융안정보고서(2024년 4월)에서는 사이버 리스크가 금융안정에 영향을 미치는 세 가지 주요 파급경로를 다음과 같이 제시하였다. 첫째, 대규모 데이터 유출 등으로 특정 금융기관에 대한 신뢰가 훼손될 경우 대규모 예금 이탈(디지털 뱅크런)이 발생할 수 있다. 둘째, 대체 불가능한 핵심 금융인프라에 장애가 발생할 경우, 금융시장 기능이 마비되면서 연쇄적 혼란이 초래될 수 있다. 셋째, 금융기관이 동일한 제3자 정보통신기술(ICT) 서비스를 이용[226]하거나 상호 연계된 금융거래 구조를 가질 경우, 한 기관의 사이버 사고가 금융시스템 전체로 확산될 수 있다(참고 8-1).

참고 8-1. 사이버 리스크 파급경로



자료: IMF 글로벌금융안정보고서(2024년 4월) <그림 3.4> 재인용

223) 본고는 편도훈·김우섭(안정분석팀)·안소희(글로벌금융규제팀)가 작성, 임광규(금융안정기획부장)·정연수(금융시스템분석부장)·문용필(안정분석팀장)·이정연(글로벌금융규제팀장)이 검토하였다.

224) 한편, 2023년 7월 클라우드 보안업체 CrowdStrike의 소프트웨어 오류로 전세계 윈도우 시스템에서 대규모 장애가 발생한 사례처럼 악의적인 공격 의도 없이 기술적 결함 및 인적 오류로 인해 발생하는 사고도 사이버 리스크의 범주에 포함되며, 이러한 비악의적 사고 또한 증가하는 추세이다.

225) 자세한 내용은 FSB(2023)의 「Cyber Lexicon – Updated in 2023」을 참고하기 바란다.

226) IMF는 구조적 연결성과 리스크 집중도를 분석하기 위한 감독수단으로 '사이버 매핑(Cyber Mapping)'을 제시하였으며, 이는 금융기관과 ICT 서비스 제공자 간의 연결구조를 시각화하여 시스템적 취약성을 구조적으로 분석하는 기법이다.

이처럼 사이버 리스크는 신뢰 상실 경로, 핵심 인프라 운영중단 경로 및 연계성 기반 전염 경로를 통해 금융 및 비금융[227] 부문 전반에 영향을 미치며, 그 결과 신용공급 위축, 지급결제 기능 장애 등 금융시스템 내 불안정성을 초래할 수 있다. 결국 사이버 리스크는 정보 유출이나 시스템 장애 등 직접적인 피해뿐 아니라, 시장심리 위축과 전염효과 등을 통해 금융안정을 위협하는 새로운 시스템 리스크 요인으로 작용할 수 있다.

금융부문의 주요 사이버 리스크 유형 및 특징

IMF에 따르면, 2023년 기준 사이버 공격 건수는 코로나19 이전인 2019년에 비해 약 2배 증가하였으며, 극단적 손실(tail risk) 발생 가능성도 높아진 것으로 나타났다.[228] 특히 2020년 이후 금융부문에서 발생한 사이버 사고로 인한 직접 손실 규모가 전세계적으로 약 25억달러에 이르는 등 사고 빈도와 피해 규모가 빠르게 증가하고 있으나, 기술 환경의 빠른 변화로 인해 이에 대한 이해와 대응체계는 여전히 제한적인 수준이다.

주요 사이버 사고 사례를 살펴보면, 사이버 리스크는 악성코드 및 랜섬웨어 공격, 사회공학 기반 공격[229], 데이터 유출, 분산서비스거부(DDoS) 공격, 제3자 리스크 및 비악의적 사고 등으로 유형화할 수 있다. 이러한 사이버 사고는 단순한 정보 유출이나 시스템 마비를 넘어 직접적인 금전 피해와 평판 훼손을 초래할 수 있으며, 나아가 탈취된 정보를 이용한 계좌 도용 등 2차 금융범죄로 이어질 가능성도 존재한다(참고 8-2). 특히 최근 딥페이크 및 생성형 AI 확산으로 공격 수법이 더욱 정교해지면서, 사이버 위협의 복잡성과 심각성이 한층 증대되고 있다.

참고 8-2. 주요 사이버 리스크 유형 및 특징

유형		주요 사례 및 특징
악성코드 및 랜섬웨어 공격	사례	- 2020년 외환 핀테크社 Travelex가 랜섬웨어 공격을 받아 온라인 서비스 일시 중단 - 2023년 중국공상은행(ICBC) 뉴욕 소재 자회사(ICBCFS)가 랜섬웨어 공격을 받아 미국 국채시장 거래 일시 지연
	특징	- 시스템 암호화를 통한 금전 요구와 함께 서비스 중단, 평판 훼손 등 피해 발생 - 핵심 시스템 마비 시 복구에 장기간 소요
사회공학 기반 공격	사례	- 2024년 글로벌 엔지니어링 기업 Arup이 딥페이크 기반 본사 임원 사칭 공격을 받아 금전적 피해 발생 - 다수의 금융기관 임직원 대상 피싱 공격
	특징	- 신뢰 관계를 가장하거나 영상·음성 등을 위조하는 고도화된 공격 기법 활용
데이터 유출	사례	- 2025년 SK텔레콤 유심 서버 해킹으로 약 2,695만 건의 유심 정보 유출 - 2025년 미국 가상자산 거래소 Coinbase의 계약직 직원을 매수하여 내부 시스템 접근권한 확보 및 고객정보 유출
	특징	- 악성코드 삽입, 내부자 연루 등을 통해 고객 식별정보, 금융거래정보 등을 탈취 - 금융사기, 신용도 저하, 법적 분쟁 등 유발
DDoS 공격	사례	- 2020년 뉴질랜드 증권거래소가 DDoS 공격을 받아 4일 연속 서비스 중단 - 2024년 일본 일부 대형 은행이 DDoS 공격을 받아 인터넷뱅킹 등에 일시적 장애 발생
	특징	- 대량 트래픽을 유발하여 금융기관의 온라인 서비스, 지급결제 시스템 등 마비 - 서비스 중단으로 고객 불편, 신뢰도 하락, 거래·결제 차질 등 피해 발생
제3자 리스크 및 비악의적 사고	사례	- 2023년 금융소프트웨어기업 ION이 서버 공격을 받아 유럽·미국 은행, 헤지펀드 등 42개社 거래 및 청산시스템 사용 불가 - 2024년 CrowdStrike社의 보안 소프트웨어 업데이트 오류로 금융기관을 포함한 글로벌 주요 기관의 윈도우 시스템이 대규모로 마비 - 2024년 Google Cloud社의 코드 오류로 인해 약 3시간 동안 금융기관 애플리케이션 장애
	특징	- 동일한 제3자 서비스 제공자가 인프라를 제공하는 경우, 복수 금융기관에 동시다발적 대규모 피해 유발 - 내부자 실수, 소프트웨어 결함 등 우발적 요인으로 발생하여 예방 및 방어가 어려움

자료: 한국은행(국제기구, 주요국 중앙은행 및 연구기관 자료 발췌·정리)

227) IMF는 통신·에너지 등 비금융부문에서 발생한 사이버 사고도 금융기관의 운영에 영향을 미칠 수 있다고 언급하였는데, 이는 사이버 리스크가 부문 간 경계를 넘어 시스템 리스크로 확대될 가능성을 보여준다.

228) 자세한 내용은 IMF 글로벌금융안정보고서(GFSR) (2024년 4월) 제3장 「Cyber Risk: a Growing Concern for Macrofinancial Stability」를 참고하기 바란다.

229) 사회공학(social engineering) 기반 공격은 정보시스템의 기술적 취약점이 아닌 사용자의 심리적·행동적 약점을 악용하여 정보를 탈취하는 방식으로, 사용자가 악성 링크를 클릭하거나 민감정보를 자발적으로 제공하도록 유도함으로써 보안정책을 우회한다.

국제기구 및 주요국 정책당국 대응방향

국제기구와 주요국 정책당국은 금융시스템 전반의 사이버 복원력[230] 강화를 위해 다양한 전략과 정책수단을 마련하고 있다. FSB는 2020년 금융기관 「사이버 사고 대응 및 복구 모범관행(Effective Practices for Cyber Incident Response and Recovery)」을 통해, 지배구조, 계획·준비, 분석, 완화조치, 복원·복구, 협업·소통, 개선 등 7대 영역에서 49개 지침을 제시하였다.[231] 이는 금융기관이 사이버 사고 발생 시 피해를 최소화하고 핵심 서비스를 신속히 정상화하며, 관련 정보를 공유함으로써 시스템 리스크 확산을 방지하기 위한 방안을 제시한 것으로, 다수 국가의 감독체계에 반영되고 있다. 나아가 2023년에는 「제3자 리스크 관리 및 감독 강화를 위한 정책수단(Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities)」을 통해 ICT 기반 클라우드 및 외부 위탁 서비스에 대한 금융기관의 의존도 확대에 대응하여 금융기관의 제3자 리스크 관리를 위한 정책수단(참고 8-3)과 감독당국의 관리·감독 강화를 위한 지침을 종합적으로 제시하였다.

유럽시스템리스크위원회(ESRB)[232]는 2024년 「사이버 복원력 강화를 위한 거시건전성 정책수단의 발전 – 운영지속성 정책수단(Advancing macroprudential tools for cyber resilience – Operational policy tools)」 보고서를 통해 완충자본·유동성 지원 등 전통적 금융안정 정책만으로는 사이버 복원력 확보에 한계가 있으므로 정보관리 체계, 감독당국·금융기관 간 위기관리 및 협력 메커니즘, 비상 대응체계 및 백업 시스템 등 금융시스템의 지속성 및 복원력 확보를 위한 보완적 거시건전성 정책수단의 필요성을 강조하였다.

참고 8-3. 금융기관의 제3자 리스크 관리 수단

단계	구분	세부 내용
계약 이전 단계	중요 서비스 식별	- 운영 및 전략적 중요성, 장애 발생 시 영향 정도, 대체 가능성 등을 기준으로 중요 서비스 여부를 판단
	실사	- 사이버 보안·데이터 보호·재위탁업체 리스크 관리 체계 등을 점검하여 규제 준수 역량 평가 - 사고 발생 시 적시에 통지할 의무를 계약 조건에 포함
운영 단계	모니터링 및 리스크 점검	- 사고 보고 체계와 정보 접근 권한이 계약에 따라 이행되고 있는지 점검 - 금융기관의 감사 수행 가능여부 및 재위탁 제한 조건의 준수 여부 점검 - 계약조건 변경 시, 리스크 및 서비스 중요도를 재평가하고 변경사항 문서화
	사고 대응	- 사고 발생 시, 유형 및 중대성 기준에 따른 적시 보고 요구 - 보고 대상, 기한, 절차, 후속보고 체계를 포함한 사고 대응 체계 마련
계약 종료 및 전환 단계	지속성 및 출구전략 확보	- 제3자 서비스 제공자의 업무지속 계획(business continuity plans) 검토 및 공동 테스트 실시 - 계약 종료 또는 비상 상황에 대비한 출구전략 수립

자료: FSB(2023) 인용

한편 영란은행은 2022년 금융시스템상 중요 기관을 대상으로 사이버 리스크 스트레스 테스트를 실시하여 사고 탐지 및 복구 능력, 금융시스템 참여자 간 협력 체계의 실효성을 점검하고 보완 과제를 도출하였다. ECB도 2024년 직접 감독 대상인 109개 은행을 대상으로 사이버 공격 발생 시 대응·복구계획 및 제3자 리스크 관리 능력을 평가하였다. 미국은 2024년 재무부 주도로 금융부문 대상 민관 합동 사이버 보안 협력체계인 '프로젝트 포트리스(Project Fortress)'를 출범시키고, 이를 통해 사이버 위협 정보의 공유, 자동화된 보안 취약점 진단 도구 제공, 사이버 공격자에 대한 제재 등 사후적 수단까지 포함한 통합적 보안 시스템을 구축하였다.

230) FSB는 사이버 복원력(cyber resilience)을 "금융기관이 사이버 사고에 선제적으로 대비하고, 사고 발생 시 영향을 최소화하며, 핵심 기능을 지속할 수 있도록 신속히 복구하는 능력"으로 정의한다.
231) 자세한 내용은 2020년 12월 금융안정보고서 <참고 7>「코로나19 이후 주요국 사이버 리스크 대응현황 및 시사점」을 참고하기 바란다.
232) ESRB(European Systemic Risk Board)는 금융시스템 안정성 감시, 시스템 리스크 예방·완화 등을 수행하는 유럽연합 내 기구이다.

우리나라 금융 분야의 사이버 보안 체계는 금융위원회와 금융감독원이 정책 수립 및 감독 기능을 수행하고, 한국은행 등 유관기관이 협력하여 대응체계를 운영하는 구조로 이루어져 있다. 2013년 발생한 대형 전산 장애 및 해킹 사고를 계기로 금융권에 망분리 의무화 조치가 도입되었으며[233], 이후 규칙(Rule) 기반의 규제 강화를 통해 보안 수준을 제고해 왔다. 그러나 디지털 전환의 가속화와 국제기준 변화, 클라우드·생성형 AI 등 신기술 확산에 따라 급변하는 리스크에 효과적으로 대응하기 위해, 최근에는 혁신과 보안 간 균형을 유지할 수 있도록 원칙(Principle) 기반의 유연한 규제 환경 조성으로 정책 기조가 전환되고 있다.[234] 또한 제3자 서비스의 중요도에 따른 차등적 보안통제 기준을 마련하고, 금융지주 계열사 합동 재해복구 훈련, 정례적인 모의해킹 실시 등 실전 대응 중심의 복원력 점검을 병행하고 있다. 아울러 한국은행은 지급결제시스템의 사이버 복원력 강화를 위해 상시 모니터링 및 현장 점검 체계를 운영[235]하는 한편, BIS 지급결제·시장인프라위원회(CPMI), 국제증권감독기구(IOSCO) 등과의 국제 협력 활동에도 적극 참여[236]하고 있다.

시사점

기술 혁신이 가속화되고 금융기관의 제3자 ICT서비스 의존이 심화되는 가운데, 사이버 리스크에 효과적으로 대응하기 위해서는 다음과 같은 추가적인 노력을 통해 금융부문의 사이버 보안 역량을 강화해 나가야 한다.

먼저, 정책당국은 금융회사의 개별 스트레스 테스트와 모의훈련에 더해 금융시스템 전반의 리스크를 체계적으로 파악·평가할 수 있도록 거시건전성 관점의 사이버 스트레스 테스트를 도입할 필요가 있다.[237] 아울러, 사이버 리스크의 국경 간 전이 가능성을 고려할 때, 주요국 정책당국과의 협력 강화, 국제 공조 및 정보 공유 체계 구축이 필수적이다.

한편, 금융기관은 사이버 리스크에 대한 인식을 조직 전반으로 확산시켜 이사회의 책임 강화, 임직원 대상 보안교육 확대 등 보안 거버넌스의 내재화를 추진하고, 사고 발생 시 금융서비스의 연속성과 이용자 신뢰를 유지할 수 있도록 복구 절차 및 커뮤니케이션 전략 등 대응체계를 사전에 정비해야 한다. 아울러, 감독당국은 업권 간 전이 가능성에 대비하여 금융기관들과 함께 공동 대응 매뉴얼을 마련함으로써, 전체 금융시스템의 복원력 제고를 도모할 필요가 있다.

궁극적으로 디지털 환경에서 금융시스템의 안정성과 신뢰성을 지속적으로 확보하기 위해서는, 사이버 사고를 예방하는 수준을 넘어 사고 발생 이후에도 핵심 금융서비스가 유지될 수 있도록 하는 '사이버 복원력' 중심의 대응체계를 금융시스템 전반에 구축해 나가는 것이 중요하다.[238]

---

233) 망분리 의무화는 2013년 대규모 사이버 공격으로 인한 금융사 등의 전산시스템 마비 이후 도입된 조치로, 업무망과 인터넷망을 물리적으로 분리하여 외부 침입을 차단하는 방식이다.

234) 금융위원회는 「금융분야 망분리 개선 로드맵」(24년 8월)을 통해 원칙(Principle) 기반 보안규제로의 전환을 제시하고, 「전자금융감독규정」을 개정(25년 2월)하여 행위규칙을 293개에서 166개로 축소하였다.

235) 한국은행은 2018년 1월 국내 금융시장인프라(FMI) 운영기관이 사이버 리스크 대응체계를 자가 진단할 수 있도록 국제기준을 기반으로 국내 상황에 맞게 59개 질문 항목으로 구성된 「사이버복원력 평가지침서」를 발간·배포하였다.

236) 한국은행이 참여하고 있는 BIS CPMI 산하 이행점검 상설그룹(IMSG)은 한은금융망을 포함한 28개국 37개 지급결제시스템을 대상으로 IT부문 운영리스크 관련 사이버 복원력에 대한 평가를 실시하였으며, 그 결과보고서를 2022년 11월 발표하였다.

237) Vermeulen et al.(2025년 3월, ECB Macroprudential Bulletin 27)은 사이버 사고가 금융시스템 전반에 미치는 영향을 체계적으로 평가하기 위해서는, 개별 금융기관이 사이버 사고 발생 시의 자체 대응 및 복구 능력을 평가하는 미시적 스트레스 테스트(상향식 접근)와 감독당국이 시스템 전체의 연계성, 2차 효과 등을 반영한 거시적 스트레스 테스트(하향식 접근)를 병행할 필요가 있다고 강조하였다.

238) IMF 글로벌금융안정보고서(2024년 4월), FSB(2023), ECB 금융안정보고서(2024년 5월) 등에서는 사이버 리스크와 관련한 정책대응 방향을 기존의 사고 예방(prevention) 중심에서 복원력(resilience) 제고 중심으로 전환할 것을 제안하였다.