ZOOM
-IN

# 금융기관의 사이버보안 위험과 과제

□ 디지털 환경의 발달로 금융기관의 영업환경이 변화하며 편의성이 증대되었으나, 이에 따른 위험도 함께 증가

□ 금융 부문의 사이버보안 위험 사례가 증가하고 있는 가운데, 데이터 유출 및 시스템 공격, 피싱 등 다양한 형태의 사이버보안 위협 문제가 나타남

□ 이에 대비하여 규제 마련 및 금융기관의 사이버보안 강화 전략으로 대응하고 있으나 더욱 정교하고 복잡해진 기술로 인해 사이버보안 위험은 더욱 증가하는 상황

□ 금융기관은 민감한 정보 보호 및 금융시스템의 안정성, 그리고 금융 손실 예방 등을 위해 중요한 과제로서 지속적인 사이버보안 인프라 구축 노력이 필요

□ 국내에서도 규정 마련과 함께 금융기관의 사이버보안 강화 노력이 계속되고 있는 가운데, 급변하는 상황에 적합한 유연한 대응 능력이 중요

## □ 디지털 환경의 발달로 금융기관의 영업환경이 변화하며 편의성이 증대되었으나, 이에 따른 위험도 함께 증가

— 금융기관은 디지털 기술의 발달로 인터넷 및 모바일 뱅킹의 활용이 증가하면서 접근성이 향상되고 신속한 거래 및 비용 절감이 가능해짐에 따라 효율성이 증가

- 금융기관 입장에서는 인터넷 거래 시스템 활용으로 지점 운영 비용이 감소하여 보다 효율적인 운영이 가능하게 되고, 사용자 입장에서는 편리하고 즉각적으로 금융서비스를 이용할 수 있게 됨

— 이와 같은 디지털 금융의 발달은 금융기관의 업무 효율성 향상과 금융서비스의 편의성 증대를 이끌어냈지만, 그 이면에는 사이버보안 위험이 확대되는 문제도 발생

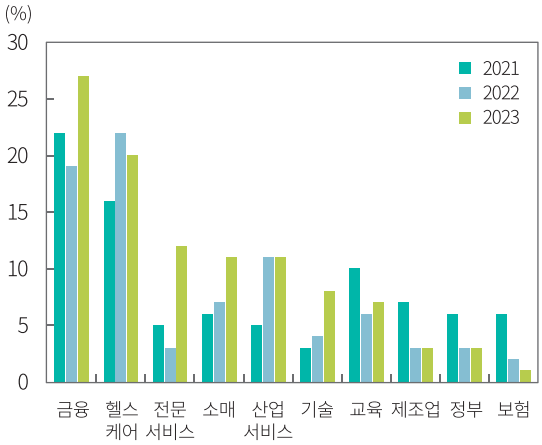
- 인공지능의 급속한 발전으로 인해 사이버보안 위험은 금융 부문의 가장 큰 체계적 위험 요소로 인식[1)]
- IMF 조사에 의하면 금융 부문은 사이버보안 위협에 가장 취약한 산업으로서 지난 20년 동안 사이버 사고의 20%가 금융 부문에서 발생했고 금융기관의 손실은 2004년 이후 총 120억 달러에 달했으며, 2020년 이후의 손실액만 25억달러 규모[2)]

1) Bank of England, 2023. 10, *Systemic Risk Survey Results - 2023 H2.*

2) IMF, 2024. 4, *The Last Mile: Financial Vulnerabilities and Risks.*

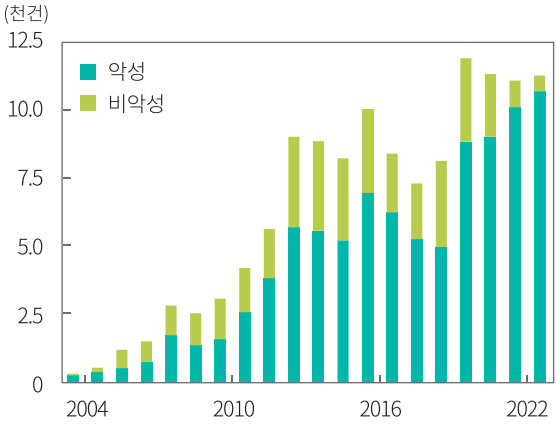
• 디지털 기반의 서비스가 점차 복잡해지고 다양화되면서 사이버 공격은 매년 증가하고 있으며, 특히 코로나 팬데믹을 겪은 2020년 이후 급격하게 증가한 디지털 활용으로 인해 사이버 공격이 크게 증가

**〈그림 1〉 데이터 침해가 발생한 산업별 비중**




자료: Kroll, 2024. 2. 7, Data breach outlook: Finance surpasses healthcare as most breached industry in 2023

**〈그림 2〉 사이버보안 사고 현황**




자료: IMF

□ **금융 부문의 사이버보안 위험 사례가 증가하고 있는 가운데, 데이터 유출 및 시스템 공격, 피싱 등 다양한 형태의 사이버보안 위협 문제가 나타남**

— 금융기관은 다른 부문에 비해 대규모의 민감한 데이터를 보유하고 있어 해커들의 주요 표적이 됨[3)]

• 대규모 유출 사례로서 2019년 First American Financial의 8억 8,500만명의 고객 정보가 유출된 사건이 있고, Equifax에서도 2017년 1억 6,000만명 이상의 민감한 정보가 유출됨

• 2024년 들어서도 푸르덴셜 보험이 사이버 공격을 당하면서 250만명의 고객이 피해를 입었고 LoanDepot에서도 1,600만명의 고객 데이터가 노출되는 등 계속적으로 중요한 정보에 대한 데이터 침해 사고가 이어지고 있음

— 분산 서비스 거부 공격인 디도스(DDoS)는 대량의 악성 트래픽을 순간적으로 일으켜 서버를 마비시키면서 사용자들의 접근 및 사용을 방해하는 것으로 금융권에서 빈번하게 발생

• 2023년 전체 DDos공격의 35%가 금융 부문을 표적으로 삼으며 피해가 발생했으며 EMEA (유럽, 중동 및 아프리카) 지역에서 금융 부문에 대한 DDos 공격이 66%, 북미에서는 28%를 차지[4)]

3) Financial Times, 2024. 1. 16, Cyber attacks reveal fragility of financial markets.

4) FS-ISAC, 2024. 3, *DDoS: Here to Stay.*

- JP 모건, 씨티은행 등 여러 은행이 DDoS 공격을 받아 온라인 서비스가 몇 시간 동안 중단되었고 뉴질랜드 증권거래소도 2020년 DDos 공격으로 인해 며칠에 걸쳐 거래 및 서비스 중단이 반복적으로 발생

— 기기 및 데이터에 접근하지 못하게 하고 이에 대한 금전을 요구하는 랜섬웨어 공격은 악성 광고 및 손상된 웹사이트, 이메일 첨부 파일을 통해 발생하며, 이로 인해 금융기관의 서비스 운영이 중단되고 거액을 요구하므로 큰 손실이 발생

- 2023년 11월에는 중국 공상은행 뉴욕 지점이 랜섬웨어 공격을 받아 거래 장애가 발생하면서 25조달러 규모의 미국 국채시장 거래가 중단
- Bank of America는 2024년 2월 랜섬웨어 공격으로 계좌 및 신용카드 번호와 같은 금융 데이터를 포함한 개인정보가 유출

— 직원의 부주의나 악의적인 행동으로 인해 중요한 데이터가 유출되거나 피싱 공격으로 이메일, 문자 메시지 또는 전화를 통해 직원을 속여 민감한 정보를 공개하는 사례도 발견

- 모건스탠리의 한 직원은 35만명의 개인정보를 유출했고, Capital One에서는 내부 클라우드 보안 설정 오류로 인해 사이버보안 사고가 발생
- 피싱은 이메일이나 휴대폰 문자 메시지 등을 통해 이루어지며, 2023년 평균 피싱 공격으로 인한 손실은 476만 달러의 규모[5)]

□ **이와 같은 사이버보안 위험에 대비하여 규제 마련 및 금융기관의 사이버보안 강화 전략으로 대응하고 있으나 더욱 정교하고 복잡해진 기술로 인해 사이버보안 위험은 더욱 증가하는 상황**

— 점차 증가하는 금융기관의 사이버보안 위협에 대해 해외 각국에서는 규제를 마련하여 대응

- 미국 SEC는 상장기업이 사이버 공격을 받은 경우 4일 이내에 공개하도록 요구함으로써 투자자 보호를 강화했고, 뉴욕주는 지난해 11월 금융기관 사이버보안규정(NYCRR part 500) 최종안을 발표하여 정교해진 사이버 공격에 대비한 사이버보안 프로그램의 개선과 감독을 강화
- 유럽의 경우 데이터 보호 규정(GDPR), EU 사이버보안법, 네트워크 및 정보시스템 지침(Network and Information Systems: NIS) 등을 통해 사이버보안을 강화하고 고객의 데이터 보호 및 금융시스템 안정성 유지를 위한 지침 제시
- 일본에서도 FSA는 금융기관 시스템에 대한 FISC(Financial Industry Information Systems) 보안 가이드라인을 개정하여 사이버보안을 더욱 강화할 것을 밝힘[6)]

— 국가 차원의 규제 및 가이드라인뿐 아니라 금융기관 자체에서도 사이버보안 위협을 방지하기 위해 보안 전략을 강화하며 대응

- 바클레이스는 고객정보보호와 거래 안전성 강화를 위해 사이버보안 및 회복성을 최우선 순위로 삼고 사이버보안 전략을 수립

5) IBM, 2024. 3. 17, What is phishing?

6) FSA, 2024. 3. 11, The dialogue between the Financial Services Agency(FSA) and the Center for Financial Industry Information Systems(FISC).

- JP모건 체이스는 고객 및 회사, 금융시스템 등을 사이버 위협으로부터 보호하기 위해 지속적으로 사이버보안 강화에 투자하고 있으며, 보안 기술력을 강화하는 데 중점을 두고 있고, 골드만삭스도 예상치 못한 사이버 위협에 대응하기 위해 전담팀을 운영하며 모의 해킹 및 보안에 대한 평가를 실시
- HSBC는 사이버보안에 대한 지속적인 모니터링을 실시하고 동향과 취약한 부분을 파악하기 위한 프로그램을 운영하여 사이버보안 위험에 대비

— 이와 같은 해외 각국의 규제 마련과 사이버보안 위험을 인식하고 해결하기 위한 노력이 진행되고 있으나 여전히 미흡한 상황

- 51개 국가를 대상으로 한 IMF 조사에 따르면 중앙은행이나 금융감독기관의 56%가 금융 부문에 대한 국가 사이버 전략이 미비하며, 금융기관 중 42%는 전담 사이버보안 또는 IT 위험 관리 규정이 없고 68%는 감독 부서 내에 전담 위험 담당 부서가 없다고 답했고, 64%는 사이버보안 테스트 및 실행을 의무화하지 않은 것으로 나타남[7)]
- 2023년 KPMG가 금융기관 CEO를 대상으로 실시한 설문조사에서 70% 이상이 사이버보안이 주요 우려 사항이라고 답했고, 사이버 위협에 대한 대비가 되어 있다고 답한 비율은 54%로 준비 부족의 이유로는 공격자의 정교함 증가, 전문인력의 부족, 사이버 방어에 대한 투자 부족 등을 꼽음[8)]

□ **금융기관은 민감한 정보 보호 및 금융시스템의 안정성, 그리고 금융 손실 예방 등을 위해 중요한 과제로서 지속적인 사이버보안 인프라 구축 노력이 필요**

— 금융기관은 민감한 고객 데이터를 보유하고 있고 시스템의 안정성 확보 및 규제 준수, 경제적 손실 예방 측면에서 매우 중요하므로 이러한 중요성을 인식하고 지속적으로 보안 체계를 강화하여 사이버보안 위협에 효과적으로 대응해야 함

- IMF는 금융 부문의 사이버 위험 노출로 인한 손실은 심각한 시장 혼란이 발생할 수 있다고 경고했고 특히 금융 부문은 민감한 데이터가 관련되어 있기 때문에 사이버 공격에 취약하다는 것을 강조
- 금융 부문의 보안 사고는 금융 시스템에 대한 신뢰를 약화시키고, 중요한 서비스를 방해하거나, 다른 기관에 파급효과를 일으킬 경우 금융 및 경제 안정성을 위협하며, 금전적인 손실뿐 아니라 평판 훼손과 같은 간접적인 손실도 상당히 높게 발생할 수 있음

— 금융기관도 사이버보안 전략 강화를 위한 적극적인 노력으로 보안 기술의 도입 및 직원 교육 등 자체적인 보안 역량을 갖추는 것이 중요[9)]

- 보안 모델 수립과 실시간 모니터링을 통한 침입감지 시스템, 데이터 암호화, 보안 교육 및 인식 제고, 백업 및 복구 계획 등을 고려

---

7) IMF, 2024. 4, *The Last Mile: Financial Vulnerabilities and Risks.*

8) KPMG, 2023, *KPMG 2023 Banking CEO Outlook.*

9) IMF, 2024. 4, *The Last Mile: Financial Vulnerabilities and Risks.*

- 사이버보안 환경을 주기적으로 평가하고 제3자 서비스 제공업체를 포함하여 상호 연결성과 집중으로 인한 잠재적인 체계적 위험을 식별

□ **국내에서도 규정 마련과 함께 금융기관의 사이버보안 강화 노력이 계속되고 있는 가운데, 급변하는 상황에 적합한 유연한 대응 능력이 중요**

— 국내 금융기관도 사이버보안 위협의 대상이 되고 있어 금융기관의 사이버보안 위험을 인식하고 규제가 마련되어 있으며, 금융기관 차원의 노력도 진행

- 국내 금융기관도 몇 년 동안 DDos, 랜섬웨어 공격을 받은 전례가 있고, 증권사의 개인정보를 유출하거나 국내 은행의 해외지점이 금전적인 피해를 입는 등 끊임없이 사이버 공격이 시도됨
- 국내에서는 사이버보안 위협에 대비하기 위해 대표적으로 전자금융거래법, 전자금융감독규정, 개인정보보호법 등의 법률이 마련되어 있음

— 금융당국은 사이버보안 위협에 선제적으로 대응이 필요함을 강조하며 고도화되는 사이버 위협에 효과적으로 대응하기 위해 전자금융감독규정 개정 예정

- 금융당국은 지난해 DDos 공격으로 인한 피해를 최소화하기 위한 사전 준비로 '금융전산 재난대응 안전한국훈련'을 실시
- 금융감독원은 금융 부문의 사이버보안 관리체계 및 우수사례 등을 공유하여 적극적인 디지털 금융 활용을 위해서는 금융 안정성이 담보되어야 함을 강조하며 사이버보안 대응 능력 향상을 도모[10)]
- 2024년 금융보안 규제를 규칙(rule) 중심에서 원칙(principle) 중심으로 개선하여 급변하는 디지털 환경에서 사이버보안 위험에 유연하게 대처할 수 있도록 자율보안 역량을 강화할 예정

— 이와 같이 금융 당국과 금융기관의 사이버보안 위험 대비를 위한 노력이 계속되고 있으나 신기술 발달로 인한 새로운 사이버 공격에 대응하기 위한 준비가 여전히 필요

- 금융기관은 상당한 자금을 투자하여 사이버보안 강화에 노력해 왔음에도 음성 분석 및 딥페이크 기술 등 공격 채널의 다양화로 사이버 공격의 가능성이 증가[11)]
- 따라서 금융기관은 지속적으로 사이버보안 강화와 함께 새로운 기술로 인한 위험 요소에 대비할 필요

선임연구원 홍지연

10) 금융위원회, 2024. 3. 21, 금융위·금감원, 정부부처 대상 「사이버보안 우수사례 설명회」 개최, 보도자료.

11) 금융보안원, 2023. 11. 2, 금융보안원이 전망하는 2024년 디지털금융 및 사이버보안이슈, 보도자료.