

## 은행의 새로운 경쟁력, 사이버 보안

정 윤 영 수석연구원(yunyeong.j@hanafn.com)

디지털 금융 환경 변화로 사이버 리스크가 확대되면서 은행의 사이버 보안이 주요 쟁점으로 떠오르고 있다. 금융프로세스 전반에 걸친 사이버 리스크의 대응 및 관리 전략이 중요해지면서 글로벌 은행들은 지속적인 기술 투자로 보안 경쟁력을 강화하는 등 관련 인프라 구축에 적극적으로 임하고 있다. 사이버 공격이 빠르게 진화하는 가운데 은행의 사이버 리스크 대응 전략은 신뢰성과 연결되어 중요하다. 따라서 국내 은행들도 보안 경쟁력 강화를 위한 장기적인 전략을 마련할 필요가 있다.

### ■ 디지털 기술발전 가속화로 금융회사의 편의성은 향상되었지만 사이버 리스크는 중대<sup>[1]</sup>

- 코로나 19 이후 원격근무 확산, 핀테크 기업과의 디지털 경쟁 심화, 오픈뱅킹 도입 등의 영업환경 변화로 은행은 보안에 취약한 환경에 노출
  - 급속한 디지털 전환 시도로 발생하는 디지털 발전과 사이버 보안사이의 기술격차로 인해 은행은 민감한 데이터를 적절히 관리하지 못하는 상황에 노출
- 사이버 리스크는 온라인 사기부터 데이터 유출, 멀웨어 및 랜섬웨어, DDoS 등의 사이버 공격까지 다양하며 관련 범죄도 점증할 것으로 예상
  - Cybersecurity Ventures에 따르면 전 세계 사이버 범죄 규모는 2025년까지 연간 10조 5천억 달러에 이를 것으로 추정

### ■ 금융프로세스 전반에 걸친 사이버 리스크의 대응 및 관리가 중요해지면서 은행들은 다양한 방식으로 사이버 보안 인프라 구축 노력


- 은행의 사이버 보안 관리 영역은 하드웨어, 소프트웨어 및 서비스에 이르기까지 광범위하며, 시스템과 어플리케이션을 보호하기 위해서는 영역별 관리가 중요
- 은행들은 보안 프로그램 구매, 자체 보안 기술 개발, 관련 인력 충원 등의 방식으로 보안 시스템 구축에 임하고 있으며 관련 이슈에도 적극적으로 대응 중
  - 은행부문 사이버보안 관련 특허 증가(건): 4,892('14) → 16,228('21)
  - 은행부문 사이버보안 관련 일자리 수 증가(개): 2,578('20.1월) → 17,146('22.3월)
  - JP Morgan, BOA, Wells Fargo 등 시가총액 상위 10개 중 9개 은행은 별도의 CISO(Chief information security officers)를 고용

[1] "Cybersecurity in Banking", GlobalData, 2022.06.30

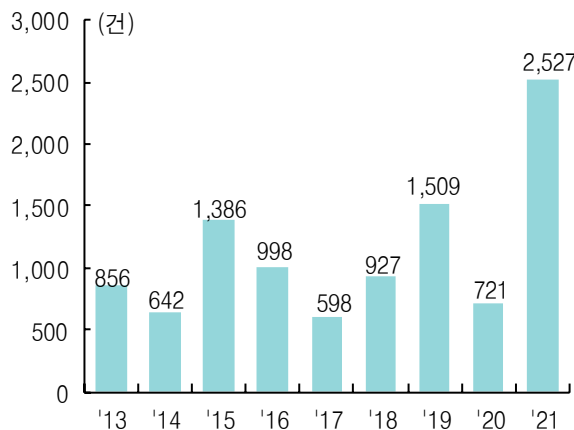
## ■ 주요 글로벌 은행들은 자체 보안 시스템 구축과 더불어 보안 기술 투자에도 적극적

- 글로벌 은행들은 과거 사이버 공격에 노출되었던 경험을 바탕으로 보안 인프라를 구축할 뿐 아니라 보안 관련 회사 및 기술에도 적극적으로 투자
  - (HSBC) '12년 멕시코 마약 카르텔의 돈세탁 혐의에 연루된 이후 고객과 회사간의 비정상 금융거래 탐지 솔루션 개발에 막대한 비용을 투자하였으며, '17년 HSBC Ventures를 통하여 사이버 보안 회사 Menlo Security에도 4천만 달러 투자
  - (JP Morgan) '14년 7600만 가구와 700만 중소기업의 계정 해킹 공격에 노출된 이후 사이버 보안 인식 및 사기 방지팀을 통해 다양한 교육 및 전문가 지원을 제공하며, '22년에는 사이버 보안을 포함한 기술영역에 120억 달러 투자 발표
  - (Goldman Sachs) 실제 보안 설계 솔루션 구현을 담당하는 전문가 및 엔지니어를 포함한 모니터링 팀을 구성하여 보안 위협을 분석하며, '19년 Immersive Labs의 사이버 보안 기술 플랫폼에 800만 달러 투자도 주선

## ■ 사이버 공격이 지속적으로 진화하는 가운데 은행의 사이버 리스크 대응은 신뢰성과 연결될 수 있어 중요하며, 국내 은행들도 사이버 보안 경쟁력을 강화하는 전략이 필요

- 오픈 API, 오픈뱅킹 등 금융산업 개방으로 국내 은행도 보안 위협에 지속적으로 노출되고 있으며 이에 보안 관련 국·내외 금융규제도 강화되는 추세
  - 금융보안원에 따르면 국내 소매금융 취급 은행 17곳이 '17~'21년 받은 사이버 공격은 109만1천606건으로 매일 598건의 사이버 공격이 발생
  - 국내 금융당국은 전자금융거래법 및 전자금융감독규정을 기반으로 사이버 보안에 대한 검사를 실시하고 있으며, 지급결제 기관에 대해서는 망분리 제도를 시행
- 디지털 금융의 기반에는 보안성이 전제되는 만큼 국내 은행도 단기적 대응뿐만 아니라 장기적 관점의 사이버 보안 전략 수립이 필요 

### ■ 전세계 금융산업 사이버 사고 건수 추이



자료 : Statista

### ■ 해외 은행들의 사이버 리스크 대응 현황

	사례
아부다비은행	<ul style="list-style-type: none"> <li>• Visa의 생체인식 솔루션을 소비자 인증 서비스에 활용함으로써, 간소화된 인증프로세스 제공</li> </ul>
HSBC	<ul style="list-style-type: none"> <li>• 음성기반 생체인식을 활용한 인증 방식 채택</li> <li>- 폰뱅킹 사기시 사람의 목소리는 모방할 수 없다는 점에서 착안한 인증방식(VoiceID)</li> <li>- 은행은 PIN번호 없이 고객의 신원을 확인할 수 있으며 사기성 뱅킹 활동도 방지 가능</li> </ul>
Danske은행	<ul style="list-style-type: none"> <li>• 기술지원 이니셔티브를 도입하여 상대적으로 보안이 취약한 중소기업의 사이버 보안 인프라를 서비스로 제공</li> <li>- 중소기업 전용 사이버 보안 솔루션을 출시하여 사이버 금융 범죄로부터 기업을 보호하도록 지원</li> </ul>
도이치뱅크	<ul style="list-style-type: none"> <li>• 연중무휴 글로벌 사이버 인텔리전스 및 대응센터를 운영(싱가포르, 독일, 미국)</li> </ul>

자료 : GlobalData