

2026.10.07.

AI 시대 금융회사의 사이버 리스크와 신용위험, 국내외 사례 및 신용평가 체계에 대한 함의

김정현 평가기준실 전문위원 김경무 평가기준실 실장
02.368.5347 02.368.5524
jhkim911@korearatings.com kmkim@korearatings.com

❖ Summary

최근 사이버 리스크는 정보보호 차원의 기술적 위험을 넘어 기업 및 금융회사의 신용위험과 금융시스템 안정성을 좌우할 수 있는 핵심 비재무 위험으로 변화하고 있다. 특히 생성형 AI와 프론티어(Frontier) AI, AI 에이전트(Agent)의 등장으로 공격자의 취약점 탐색 및 공격 자동화 능력이 크게 향상되면서 기존의 사이버 보안체계가 전제로 해온 공격 탐지 및 대응에 필요한 시간이 빠르게 단축되고 있다. IMF도 2026년 금융부문 사이버 리스크 보고서에서 AI의 핵심 위험은 반드시 새로운 공격 유형을 만들어낸다는 데 있는 것이 아니라 기존 공격의 속도·빈도·범위를 비선형적으로 확대한다는 데 있다고 평가했다.

금융부문은 특히 사이버 리스크에 취약하다. 금융회사는 대규모 개인정보와 신용정보를 보유하고 있으며, 동시에 결제·송금·증권 거래·보험금 지급 등 실시간 핵심 금융서비스를 운영한다. 따라서 사이버 공격이 개인정보 유출에 그치지 않고 거래 중단, 지급결제 장애, 유동성 충격, 고객 신뢰 하락으로 이어질 수 있다. 또한 금융업권은 공통 클라우드, 소프트웨어, 데이터센터, 외부 IT사업자 등에 대한 의존도가 높기 때문에 특정 취약점이 다수 금융회사에 동시에 영향을 미칠 수 있다. IMF와 ECB는 사이버 침해사고가 이러한 경로를 통해 금융시스템 전반으로 확산되면서 금융안정성을 위협하는 시스템 리스크(systemic risk)로 이어질 수 있다고 분석하고 있다.

국내에서도 이러한 위험이 현실화되고 있다. 2025년 카드사의 개인정보 유출과 보험사의 랜섬웨어 공격에 따른 전산시스템 마비 사태가 발생한 데 이어, 2026년 9월말~10월초에 걸쳐 은행, 저축은행, 캐피탈 등 7개 금융회사에서 외부 업무지원 시스템을 겨냥한 해킹과 정보 유출이 잇따라 확인되면서 금융업권 전체에 대한 사이버 리스크 전염(contagion) 우려가 크게 높아졌다. 공격 대상은 고객 거래 채널이 아니라 대출모집인용·직원용·영업지원용 등 상대적으로 통제가 약한 외부 접점이었으며, 일부 공격에서는 자동화된 AI 도구를 활용해 상대적으로 보안이 취약한 외부 접점과 연계 시스템을 집중적으로 타격한 것으로 추정되고 있다. 현재 공개된 정보만으로 각 사고의 AI 사용 여부와 기술적 공격 경로가 최종 확인된 것은 아니므로 이를 일률적으로 'AI 해킹'으로 규정하는 것은 신중할 필요가 있다. 다만 이러한 동시다발적 사고는 개별 금융회사의 보안 수준뿐 아니라 금융업권 전체가 유사한 소프트웨어, 외주업체, 인증 인프라를 공유함으로써 발생할 수 있는 '공통 취약성(common vulnerability)'의 문제를 보여주고 있는 것으로 판단된다.

사이버 리스크가 신용도에 미치는 영향은 사고 발생 자체보다 사고의 지속기간, 핵심 영업기능에 미치는 영향, 재무적 흡수 능력, 사고 이후 운영 복원력과 회복 속도, 반복적인 통제 실패 여부 등에 의해 결정된다. 한국기업평가는 금융회사 신용평가지 사이버 리스크를 사업항목 평가요소인 '경영 및 리스크 관리' 매핑 변경요인으로 반영하거나 ESG 위험요인 관련 기타평가요소로 고려하는 방식으로 신용등급에 반영하고 있다. 특히 사이버 침해사고 발생시에는 재무적 능력 대비 손실(비용) 규모, 핵심 영업기능의 중단 여부 및 운영 복원력, 평판 저하에 따른 고객 이탈 수준 및 회복 기간, 사고 이후 통제수준의 실질적 개선 여부, 사고의 반복성 등을 종합적으로 고려하여 신용등급에 반영한다. 예를 들어 2025년 8월 대규모 정보유출 사고가 발생한 롯데카드의 경우 2026년 3월 정기평가지 경영 및 리스크 관리 평가요소 매핑을 하향조정한 바 있다.

최근 국내 금융회사의 디지털 의존도가 높아지고 AI 기반 공격이 확산되면서 사이버 리스크 발생 빈도가 크게 증가하고 범위도 확대되고 있다. 한국기업평가는 사이버 리스크가 수익성, 현금흐름, 유동성, 자본적정성, 규제비용, 평판 및 자금조달비용을 동시에 악화시킬 수 있는 복합적인 신용위험 요인으로 진화하고 있으며 신용도에 미치는 중요도도 높아진 것으로 판단하고 있다. 이에 따라 중장기적으로 사이버 리스크를 정성적 평가항목으로 고려하는 것을 넘어 사이버 리스크 노출도에 대한 보다 객관적인 평가 지표 도입 방안을 검토할 예정이다.

CONTENTS

I. 사이버 리스크, 금융부문의 새로운 위협요인	3
II. 최근 국내 사례와 문제점	4
1. 국내 사이버 침해사고 증가	4
2. 주요 문제점과 구조적 취약성	6
3. AI 시대 사이버 리스크와 대응체계 구축	7
III. 신용평가 측면의 합의	8
1. 사이버 리스크의 신용위험 전환 경로	8
2. 금융회사 신용평가 측면의 고려 사항	9
3. 글로벌 신용평가사의 사이버 리스크 신용평가체계와 평가사례	10
4. KR의 사이버 리스크 신용평가체계와 개선 방향	12

I. 사이버 리스크, 금융부문의 새로운 위협요인

디지털 전환과 AI 도입 가속화로 사이버 리스크 확대

디지털 전환의 진전은 금융회사와 기업의 비용 효율성과 고객 편의성을 높여 왔지만 이와 동시에 IT 시스템과 데이터에 대한 의존도가 커지면서 사이버 침해사고 발생 시 피해범위도 확대되고 있다. 과거 사이버 침해 사고는 개별 서버나 PC의 악성코드 감염 등 비교적 국소적인 문제로 인식되었으나, 최근에는 클라우드, API, SaaS, 결제망, 인증시스템 및 외부 IT 사업자와 같은 공통 인프라가 공격 대상이 되면서 하나의 취약점이 다수 기업과 금융회사로 확산될 가능성이 높아졌다.

금융부문은 특히 취약하다. 금융회사는 대규모 개인정보와 신용정보를 보유하고 있으며, 동시에 결제·송금·증권거래·보험금 지급 등 실시간 핵심 금융서비스를 운영한다. 따라서 사이버 공격이 개인정보 유출에 그치지 않고 거래 중단, 지급결제 장애, 유동성 충격, 고객 신뢰 하락으로 이어질 수 있다. 또한 금융업권은 공통 클라우드, 소프트웨어, 데이터센터, 외부 IT 사업자 등에 대한 의존도가 높기 때문에 특정 취약점이 다수 금융회사에 동시에 영향을 미칠 수 있다. IMF와 ECB는 사이버 침해사고가 이러한 경로를 통해 금융시스템 전반으로 확산되면서 금융 안정성을 위협하는 시스템 리스크(systemic risk)로 이어질 수 있다고 분석하고 있다.

2026년 들어서는 AI의 발전이 위험을 한 단계 높이고 있다. BIS는 Frontier AI 모델이 취약점을 자동으로 탐색하고 취약점 악용 코드(exploit)를 개발하거나 복잡한 다단계 공격을 수행하는 능력을 확대하여 공격자의 전문성·시간·비용 장벽을 낮출 수 있다고 평가하였다. 따라서 향후 사이버 리스크 분석은 ‘해킹을 당할 가능성이 높은가’에 그치지 않고 ‘얼마나 빨리 공격이 이루어질 수 있는가’, ‘얼마나 넓게 확산될 수 있는가’, ‘공격 이후 얼마나 빨리 핵심업무를 복구할 수 있는가’에 초점을 맞출 필요가 있다.

금융산업의 사이버 리스크는 금융시스템 차원의 위협요인으로 진화

금융산업의 디지털 전환과 AI 기술의 급격한 도입은 금융 서비스의 편의성을 극대화하는 동시에 공격 표면(Attack surface)을 기하급수적으로 확장시키는 부작용을 초래했다. 최근의 사이버 위협은 과거의 단순 침입이나 악성코드 유포 방식을 넘어, AI 에이전트(Agent)를 활용한 지능형·자동화 공격으로 패러다임이 전환되었다. AI 기술을 악용한 공격자들은 대량의 유출된 크리덴셜을 지능적으로 대입하는 크리덴셜 스테핑(Credential Stuffing)을 자동화하고, 무작위 웹 크롤링 및 API 요청 변조 수법을 정밀화함으로써 기존의 방화벽과 완충지대(DMZ) 통제망을 효과적으로 우회하고 있다.

금융업권은 높은 자산집중도와 기관 간 연계성으로 인해 단일 기관의 사이버 침해사고가 전체 금융시스템의 신뢰성 마비와 연쇄적인 유동성 충격으로 전이될 가능성이 매우 높다. 이러한 환경 변화는 금융회사의 신용도를 평가하는 관점에도 근본적인 변화를 요구한다. 과거 사이버 리스크가 일회성 우발채무나 일시적 경비 증가를 초래하는 요인으로 취급되었다면, 현재 신용평가체계에서는 기업의 지속가능성과 직결된 지배구조(Governance), 운영 리스크, 그리고 재무적 충격 흡수력을 결정짓는 핵심 위협 요인으로 다루어질 필요가 있다.

II. 최근 국내 사례와 문제점

1. 국내 사이버 침해사고 증가

2025년 이후 사이버
위생 실패, 내부자
정보유출, 랜섬웨어
공격 등으로 사이버
침해사고 크게 증가

2025년 8월 롯데카드 해킹사고는 국내 금융업권 사이버 리스크의 대표적인 사례이다. 약 297만명의 회원정보가 유출되었고 이 중 약 28만명은 카드번호·CVC 등 부정사용이 가능한 정보까지 유출되었다. 금융감독원 검사 결과 온라인 결제서버에서 정보처리시스템 보정(patch) 작업 미실시, 침입차단·침입탐지시스템 미설치, 개인정보 암호화 미이행, 백신 소프트웨어 미설치 등 기본적인 보안통제 미비가 확인되었다. 금융위원회는 2026년 7월말 정례회의에서 업무정지 1.5개월과 50억원의 과징금을 부과하였다. 이 사고는 고도화된 공격기법 자체뿐 아니라 중요 보안패치, 침입차단·탐지 등 기본적인 보안통제가 충분히 작동하지 않은 상황에서 대규모 정보유출로 이어졌다는 점에서 사이버 위생(Cyber hygiene; 개인이나 조직이 사이버 공격과 정보보안 사고를 예방하기 위해 일상적으로 수행해야 하는 기본적인 보안 관리·보호 활동과 그 수준)의 중요성을 보여준다.

신한카드는 동년 12월 외부 해킹과 달리 내부 직원에 의한 수년간의 정보유출이 확인되었다. 내부직원이 신규 카드 모집을 위해 확보한 약 19.2만건의 가맹점 대표자 개인정보(대부분 휴대폰번호)를 외부로 반출한 것으로 확인되었으며, 금융당국은 카드업권 전반으로 점검을 확대하고 제재 절차를 진행 중이다. 이는 사이버 리스크가 기술적 방어만의 문제가 아니라 임직원 행동, 권한관리, 내부통제, 데이터 접근 권한 등의 문제라는 점을 보여주었다.

정보유출 외에 랜섬웨어로 핵심 업무가 멈추는 사례도 나타났다. 2025년 7월 서울보증보험은 랜섬웨어 공격으로 전산시스템이 마비된 바 있으며, 이로 인해 시중은행 신규 전세대출에 필요한 보증서 발급을 비롯해 약 40개 보증상품의 업무가 핵심 시스템이 복구될 때까지 약 3일간 중단되었다. 보증서가 없으면 대출이 실행되지 않는 구조여서 피해는 서울보증에 그치지 않고 은행의 전세대출, 협력업체의 이행보증 가입 등 연계 금융거래 전반으로 번졌다. 회사는 피해 신고센터를 운영하며 피해 전액 보상 방침을 밝혔고, 금융감독원은 8월 20일 현장검사에 착수하였다. 고객 대면 시스템은 빠르게 복구되었지만 내부 업무지원 시스템 복구와 보안 강화까지 모두 마친 것은 사고 약 6개월 뒤인 2026년 1월 20일이었다. 이 사례는 사이버 침해사고가 정보유출 비용을 넘어 영업 중단, 연계 거래 차질, 장기 복구비용 발생으로 이어질 수 있음을 보여주며, 얼마나 빨리 핵심 업무를 복구할 수 있는지가 중요하다는 점을 확인시켜 주었다.

2025년 8월에는 웰컴금융그룹 계열 대부업체인 웰릭스에프앤아이대부가 랜섬웨어 공격을 받았다. 러시아 연계 해커조직은 다크웹에서 고객 성명, 생년월일, 주소, 계좌번호 등을 포함한 약 1TB의 데이터를 탈취했다고 주장했으며, 회사는 내부 문서 유출을 확인하고 고객정보 유출 여부를 조사하였다. 그룹의 핵심 계열사인 웰컴저축은행은 서버가 분리되어 있어 피해가 없었던 것으로 알려졌다. 이 사례는 금융그룹 안에서 상대적으로 보안 투자가 적은 계열사가 공

격 경로가 될 수 있다는 점을 보여주며, 반대로 계열사 간 시스템 분리가 피해 확산을 막는 장치로 작동할 수 있다는 점도 보여준다. 따라서 저축은행·캐피탈사 등 중소형 금융회사의 사이버 대응력을 평가할 때는 모회사·계열사 시스템 의존도와 그룹 내 망 분리 수준을 함께 살펴볼 필요가 있다.

한편 2025년 비금융 기업들의 대형 사이버 침해사고에 부과된 과징금 규모는 사고 발생에 따른 규제 비용이 상당한 부담이 될 수 있다는 점을 보여주었다. 개인정보보호위원회는 2025년 4월 유심 정보 해킹으로 약 2,324만명의 피해가 발생한 SK 텔레콤에 대해 2025년 8월 약 1,348억원의 과징금을 부과하였다. 2025년 9월 불법 소형기지국을 통한 무단 소액결제와 개인정보 유출이 발생한 KT 에는 2026년 7월 약 540억원의 과징금을 부과하였다. 2025년 11월 약 3,370만 계정의 정보가 노출된 쿠팡에는 2026년 6월 약 6,247억원을 부과했는데, 이는 역대 최대 규모이다. 이들 과징금은 모두 상한이 전체 매출액의 3%였던 개정 전 법률에 따라 부과되었으며, 2026년 9월 시행된 개정 개인정보보호법에서는 고의·중과실에 의한 반복·대규모 유출의 과징금 상한이 10%로 상향되었다.

**26년 9월말~10월초
금융업권 전반에 대한
해킹 공격으로 정보유출
발생 크게 증가**

최근 2026년 9월말~10월초에 걸쳐 은행, 저축은행, 캐피탈 등 7개 금융회사에서 외부 업무지원 시스템을 경유한 해킹과 정보 유출이 잇따라 확인되면서 국내 금융업권 전체에 대한 사이버 리스크 전염(contagion) 우려가 크게 높아졌다. 공격 대상은 고객 거래 채널이 아니라 대출모집인용·직원용·영업지원용 등 상대적으로 통제가 약한 외부 접점이었으며, 일부 공격에서는 자동화된 AI 도구를 활용해 상대적으로 보안이 취약한 외부 접점과 연계 시스템을 집중적으로 타격한 것으로 추정되고 있다.

신한은행의 경우 대출모집인 전용 서비스의 본인확인 절차를 우회한 외부 비인가자의 공격으로 약 2만 5천명의 고객정보가 유출됐다. 공격자는 다른 곳에서 유출된 계정정보로 로그인한 뒤 조회 요청값을 무작위로 변조한 것으로 알려졌다. 보안업계에서는 AI 자동침투 도구가 활용되었을 가능성을 제기하고 있다. 다만 구체적인 공격 경로와 AI 의 역할에 대해서는 추가적인 조사가 필요하다. 유출된 데이터는 단순 성명과 연락처에 그치지 않고, 고객의 연소득, 대출 산출한도 등 자산 및 신용 상태에 직결된 민감 금융정보가 포함되어 보이스피싱 등 2차 피해의 우려가 커진 상황이다.

국민은행에서는 직원용 모바일 업무 지원 시스템이 외부 침입을 당해 119명의 개인정보가 유출되었으며, 하나은행에서도 외부 해킹 세력의 영업지원시스템(ODS)에 대한 비정상 접근으로 89명의 고객 정보가 유출되었다. 부산은행은 외주 개발직원 11명의 개인정보 유출이 확인되었고, 우리은행과 농협은행 역시 외부 해킹 공격 시도가 포착되었으나 정보 유출은 없는 것으로 파악된다.

제2금융권의 경우에도 예가람저축은행이 외부 솔루션의 원격 취약점을 이용한 것으로 추정되는 해킹 공격으로 약 4만명의 고객 정보가 유출되었으며, 웰컴저축은행은 약 2,200건의 법인

고객 정보, 현대캐피탈은 146명의 주택대출 모집인 정보가 해킹 공격으로 유출된 것으로 파악된다. 해킹 공격 대상이 금융업권 전반으로 확산되면서 금융당국은 긴급 점검에 착수하고 위험정보 공유와 공동대응을 강화하는 등 대응방안을 모색하고 있는 상황이다.

현재 공개된 정보만으로 각 사고의 AI 사용 여부와 기술적 공격경로가 최종 확인된 것은 아니므로 이를 일률적으로 ‘AI 해킹’으로 규정하는 것은 신중할 필요가 있다. 다만 이러한 동시다발적 사고는 개별 금융회사의 보안 수준뿐 아니라 금융업권 전체가 유사한 소프트웨어, 외주업체, 인증 인프라(authentication infrastructure)를 공유함으로써 발생할 수 있는 ‘공통 취약성(common vulnerability)’의 문제를 보여주고 있는 것으로 판단된다.

[표 1] 2026년 9월말~10월초 국내 금융업권 정보유출 사고 발생

금융회사	정보 유출 규모 및 대상	주요 공격 수법 및 진입 경로	유출 정보의 민감도
신한은행	약 2만 5천명 (고객)	대출모집인 전용 서비스의 본인확인 절차를 우회한 외부 비인가자 공격	성명, 전화번호, 주민등록번호, CI(연계정보), 연소득, 대출 산출한도 등
국민은행	119명 (고객 및 임직원)	직원용 모바일 업무 지원 시스템 외부 침입	성명, 전화번호, 주소, 암호화된 주민등록번호 등
하나은행	89명 (고객)	외부 해킹 세력에 의한 영업지원시스템 비정상 접근	성명, 전화번호, 주민등록번호, 주소, 이메일, 직장명 등
부산은행	11명 (외주 개발직원)	외부 협력업체 및 외주 직원 정보 관리 접점 공격	성명, 전화번호, 이메일, 생년월일 등
예가람저축은행	약 4만명 (고객)	외부 솔루션 원격 취약점 이용으로 추정되는 해킹 (세부 경로 미공개)	성명, 생년월일, 전화번호 등
웰컴저축은행	약 2,200건 (법인 고객)	외부 접점 공격(세부 경로 미공개)	법인명, 담당자 성명, 이메일, 전화번호 등
현대캐피탈	146명 (주택대출 모집인)	주택대출 모집인 조회 페이지 해킹 공격	성명, 전화번호, 이메일, 주민등록번호 등

주) AI 도구 활용 여부와 구체적인 공격 방식, 유출 정보 범위 등은 조사 결과에 따라 달라질 수 있음.

자료) 업계 자료

2. 주요 문제점과 구조적 취약성

**경계 중심의 방어체계,
API 보안 공백,
제3자 위험관리 부실,
방어체계 속도 불균형
이 취약점으로 작용**

최근 국내 금융권의 연쇄 해킹 사태는 AI 기반의 공격 가능성이 제기되고 있어 개별 금융사의 일시적인 관리 실수보다 기술적·구조적 한계에서 비롯된 결과일 가능성이 높다. 공격자가 AI를 무기화하여 크리덴셜 스테핑과 API 변조를 자동화하고 자동화된 입력값 대입과 반복적인 정보 조회를 통해 대규모 데이터를 탐색하는 공격이 가능해지면서 기존의 수동적·정적 방어체계의 한계가 부각되고 있다.

첫째, 경계 중심 방어 체계의 한계와 API 보안 공백이 취약점으로 작용하고 있다. 국내 금융사들은 방화벽, DMZ 등 외곽 경계를 구축하고 내부 망을 분리하는 전통적 접근에 의존해 왔으나, AI 도구를 악용한 최근 공격은 정식 인증을 거친 정상적 API 요청으로 위장하거나 대출모집인 망 등 외곽 연결 접점의 파라미터를 변조하는 수법을 사용한다. 내부 시스템으로 진입한 이후

데이터 조회 단계에서 2차 검증 및 무단 크롤링 탐지 메커니즘이 부재한 경우, 민감 데이터가 아무런 제지 없이 빠져나가는 결과가 초래될 수 있다.

둘째, 공급망 및 제3자 리스크(Third-Party risk)에 대한 관리 부실이다. 금융 서비스가 모바일 앱, 대출 모집인 플랫폼, 외주 IT 개발사 등 외부 생태계와 복잡하게 연계되면서, 금융사 본체보다 보안이 상대적으로 취약한 제3자가 공격자의 주요 침투 경로로 악용되고 있다. 이번 사태에서도 시중은행의 모바일 업무 지원망과 외주 직원 관리 접점이 일차적인 공격대상이 되었으며 이는 제3자 위험 관리 체계의 실패를 보여준다.

셋째, 방어 체계의 속도 불균형이다. 공격자는 최신 AI 도구를 동원해 유출된 크리덴셜을 무작위로 대입하고 보안 허점을 24시간 실시간 탐색할 수 있는 반면, 금융사의 보안 시스템과 보안관제센터가 여전히 정적 룰(Rule) 기반 탐지나 사후 모니터링 방식에 머물러 있는 경우, 침입 탐지와 원인분석에 시간이 소요될 수 있으며 공격 자동화가 고도화될수록 탐지·대응시간의 단축이 매우 중요해진다.

3. AI 시대 사이버 리스크와 대응체계 구축

사이버 공격 속도
증가, AI 에이전트
권한 부여에 대응한
보안체계 강화 필요

AI 이전의 사이버 리스크는 상당부분이 공격자의 인력과 시간 제약이라는 한계를 가지고 있었다. 그러나 AI 도구가 공격 과정에 활용될 경우, 취약점 발견 → 공격경로 탐색 → 코드 생성 → 자격증명 획득 → 측면 이동(lateral movement) → 데이터 탐색 → 데이터 탈취(exfiltration)의 과정이 자동화될 가능성이 있다. 이 때문에 가장 중요한 변화는 공격의 정교함 뿐만 아니라 공격 속도의 증가이다. 기존 보안체계가 취약점 발견 후 보정(patch)을 적용할 수 있는 며칠 또는 몇 주의 기간을 전제로 한다면, AI 기반 공격은 취약점 발견과 취약점 공격(exploitation) 사이의 시간이 크게 단축되어 적시적 대응이 불가능할 수 있다. 따라서 이에 대응가능한 AI 기반 방어체계를 구축하는 새로운 보안 패러다임이 필요하다.

금융회사가 AI 를 업무에 활용하는 경우에는 별도의 위험이 발생한다. AI 에이전트에 고객정보 접근 권한, 내부 업무시스템 접근 권한 또는 거래 실행 권한이 부여되면 단순한 정보 유출을 넘어 AI 에이전트(Agent) 자체가 새로운 권한있는 사용자가 될 수 있기 때문이다. 따라서 AI 시대의 금융 보안에서는 AI 에이전트의 최소 권한 원칙, 고위험 행위에 대한 인간의 승인(Human approval), AI 에이전트의 모든 행동에 대한 실시간 추적, 모니터링과 보안 유지를 위한 차단 등의 대응체계를 마련하는 것이 필수적이다.

AI 시대 사이버
리스크에 적합한
대응체계 구축 필요

AI 시대 사이버 리스크 특성을 감안하여 국내 금융회사에 필요한 대응체계를 몇 가지 모색해보면 다음과 같다. 첫째, 사이버 위생(Cyber hygiene)을 강화하여 기본적인 보안통제의 실패를 없애는 것이 중요하다. 정보시스템·네트워크·데이터·사용자 계정 등에 존재하는 보안 취약점을 지속적으로 식별·관리하고, 기본적인 보안 통제를 일상적으로 적용함으로써 사이버 공격 및 정보보안 사고의 발생 가능성과 피해를 최소화해야 한다. 둘째, 고객정보를 보유하는 시스

템과 일반 업무시스템을 분리할 필요가 있으며, 내부 망이 안전하다는 기존의 경계 기반 보안 가정을 폐기하고 모든 API 요청과 내부 데이터 접근을 절대 신뢰하지 않고 항상 검증하는 제로 트러스트 아키텍처(Zero Trust Architecture) 구축이 필요하다.

셋째, AI 관련 시스템에 대해 공격자가 실제로 어떤 방식으로 시스템 경계를 우회할 수 있는지를 검증하는 AI red teaming을 정례화할 필요가 있다. 넷째, 기존 보안체계에서 강조되던 탐지와 차단보다 공격 이후 얼마나 빨리 정상적인 활동으로 복원될 수 있는지가 중요해졌기 때문에 핵심 시스템별로 백업 시스템이나 대체 프로세스 사이트 구축, 수동 처리 역량 등 복구를 위한 시스템을 구축하고 실제 상황에서 정기적으로 테스트해야 한다.

다섯째, 클라우드·SaaS·외주개발사·결제사업자·데이터센터·보안업체 등 제3자(Third-party)에 대한 의존도를 파악하고, 중요한 외부 업체의 사이버 실패(cyber failure)가 미칠 영향을 분석하여 관리할 필요가 있다. 외주 IT 업체, 대출 모집인, 협력사의 보안 수준을 주기적으로 평가하는 제3자 위험 관리(TPRM)를 제도화하고, 계약 조건에 보안기준 미달 시 즉시 접근 권한을 박탈하는 강제 조항을 명시해야 한다. 여섯째, 전통적인 재무 스트레스 테스트에 사이버 시나리오를 결합한 사이버 스트레스 테스트(Cyber stress test) 체계를 구축할 필요가 있다. 마지막으로 예측 불가능한 대규모 과징금 및 민사 소송 리스크에 대비하기 위해서는 적정 담보 한도를 갖춘 사이버 보험 가입을 확대하여 재무적 버퍼를 확보하는 위험 전가 전략이 병행되어야 한다.

III. 신용평가 측면의 합의

1. 사이버 리스크의 신용위험 전환 경로

직접적인 재무손실, 영업중단 영향, 규제 및 법률비용 증가, 평판위험 및 유동성 위험, 시스템적 전염 등

사이버 리스크가 금융회사의 신용위험으로 전환되는 경로를 살펴보면, 첫째는 직접적인 재무손실이다. 해킹 자체에 따른 자금 탈취, 랜섬웨어 유포, 포렌식 비용, 시스템 복구비용 등이 발생할 수 있다. 둘째, 영업중단에 따른 손실이다. 핵심 IT 시스템이 중단되면 거래량 감소와 매출 손실이 발생하며, 특히 금융회사에서는 모바일뱅킹, 결제승인, 대출심사, 증권거래, 보험금 지급 등이 중단되면서 정상적인 영업활동이 어려워지는 상황이 발생할 수 있다. 셋째, 규제 및 법률비용이 증가하게 된다. 개인정보보호 관련 과징금, 영업정지, 고객보상, 손해배상 소송, 규제 관련 시정 조치 비용이 발생한다. 특히 사고 발생 이후 보안시스템 전면 개편이 요구되는 경우 상당한 자본적 지출이 발생할 수 있다.

넷째, 평판 및 프랜차이즈 가치 손실이 나타날 수 있다. 금융회사에서 개인정보와 거래정보의 보호는 고객 신뢰의 핵심이며, 사고 이후 신규고객 유입 감소, 고객 이탈, 교차판매 감소 등 장기적인 영업수익성 훼손이 발생할 가능성이 높다. 다섯째, 유동성 위험 증가 가능성도 내재한다. 사이버 침해사고 자체가 곧바로 뱅크런(bank run)으로 연결되는 것은 아니지만, 핵심 결제

· 송금기능이 중단되거나 금융회사에 대한 신뢰가 급격히 저하될 경우 예금·자금조달 구조에 영향을 줄 수 있다. 특히 사고가 다른 금융기관이나 시장인프라와 동시에 발생할 경우 유동성 위험이 증폭될 수 있다.

여섯째, 시스템적 전염이다. 공유 클라우드 제공자, SaaS, 결제 인프라, 인증 제공자 등에서 발생한 하나의 사고가 여러 금융회사에 동시다발적으로 영향을 미칠 수 있다. FSB와 IMF는 최근 보고서에서 이와 같은 제3자 집중도(third-party concentration)를 사이버 리스크가 금융 안정 리스크로 전환되는 핵심 경로로 보고 있다.

2. 금융회사 신용평가 측면의 고려사항

신용평가 측면에서는
사이버 침해사고 발생
여부보다 사업위험 및
재무건전성에 미칠
영향을 반영

최근 AI 해킹에 따른 정보유출 사태 확산은 금융회사 신용평가지 사이버 리스크 반영의 중요성을 높이는 계기가 되고 있다. 다만 중요한 것은 사이버 침해사고 발생 여부 자체보다는 사고 발생이 사업위험 및 재무건전성에 미칠 영향을 반영하는 것이 될 것이다.

사이버 침해사고 발생은 금융회사의 재무제표에 직접적인 타격을 입히며, 신용평가 지표 중 수익성, 유동성, 자본적정성 지표를 직접적으로 악화시킬 수 있다. 2026년 9월 시행된 개인정보보호법 개정으로 고의·중과실에 의한 반복·대규모 유출 시 과징금 상한이 전체 매출액의 3%에서 10%로 상향되었으며, 금융회사는 신용정보법·전자금융거래법상 제재도 동시에 받을 수 있다. 이러한 과징금과 대규모 손해배상 소송에 따른 합의금·배상금은 일시에 큰 영업외비용을 발생시켜 당기순이익을 급감시킬 수 있다. 사후 수습을 위한 보안 인프라 전면 재구축, 외부 컨설팅, 고성능 보안 솔루션 도입 등은 막대한 자본적 지출을 수반할 가능성이 있다. 또한 시장 신뢰 저하로 인한 신용 스프레드 확대는 금융채 발행 금리를 상승시켜 자금조달 비용 부담을 늘리고 순이자마진(NIM)을 압박하는 요인으로 작용할 수 있다.

정성적 측면에서 사이버 침해사고는 사업항목 평가요소인 ‘경영 및 리스크 관리’ 매핑 변경 요인으로 반영될 수 있다. 초보적인 수법에 의해 침해를 당하거나 기본적 API 검증을 누락한 경우 해당 기업의 운영 리스크나 내부통제 역량에 대해 부정적인 평가가 불가피할 것이다. 이와 함께 금융업의 본질인 신뢰가 훼손됨에 따라 예금 고객 이탈, 마이데이터 및 대출 신규 고객 감소 등 사업기반이 유의미하게 약화될 가능성도 신용도에 부정적인 요인으로 반영될 수 있다.

AI 시대 사이버
리스크 대응력 평가
항목은 금융업권별로
다소 상이

AI 시대 도래와 함께 사이버 리스크 대응력의 중요성이 높아짐에 따라 사이버 리스크 노출도를 신용평가에 반영하는 방안도 검토될 수 있다. 중점적으로 고려할 항목은 금융업권별로 다소 상이하다. 은행의 경우 핵심계정 및 지급결제 시스템 의존도, 고객정보 규모, 디지털 채널 비중, IT 외주업체 집중도, 사고 발생 시 운영 복원력 및 유동성 영향 등이 주요 평가항목이 될 수 있다. 신용카드사는 결제·승인 시스템 문제 발생시 치명도(criticality), 고객정보 및 신용정보 규모, 피해규모(fraud loss), 개인정보보호 비용, 규제 집행 위험 등이 검토될 수 있다.

증권사의 경우 거래시스템의 가용성, 주문·결제·청산 시스템, 시장데이터 의존도, 고객계좌 및 자산 규모 등이 고려될 수 있으며, 보험사는 고객정보 규모, 보험금 지급시스템, 언더라이팅 데이터, 사이버 보험 언더라이팅 리스크 등이 주요 평가항목이 될 수 있다. 저축은행·캐피탈사의 경우 상대적으로 제한된 IT 및 보안 투자역량이 취약점으로 작용할 수 있으며, 외주업체나 클라우드 의존도, 조직규모 대비 보안인력 및 시스템 구축 수준, 모회사 또는 계열사 시스템 의존도 등이 사이버 리스크 대응력에 대한 주요 평가 항목이 될 것이다.

3. 글로벌 신용평가사의 사이버 리스크 신용평가체계와 평가 사례

사이버 리스크를
M&G, 사업 및 재무
위험 지표나 ESG 요
소에 통합하여 평가

글로벌 신용평가사들이 사이버 리스크를 신용등급에 반영하는 체계를 살펴보면, 3사 모두 공통적으로 사이버 리스크를 독립된 별도의 평가항목으로 다루기보다 기존의 사업 및 재무위험 틀이나 ESG 평가항목에 통합하여 신용도에 반영하고 있다. 또한 사고 발생 시 단순히 사이버 공격을 받았다는 사실 자체보다 실질적으로 중대한 재무적·운영적 영향이 발생하는지에 따라 신용등급(전망)의 조정 여부를 결정하는 것으로 파악된다.

S&P 는 사이버 위생·거버넌스·복원력을 포함한 사전적 위험관리를 강조하는 가운데 사이버 리스크 관리 체계를 경영진 및 지배구조 항목에 반영하는 정성적 평가 구조가 상대적으로 명확하다. Moody's 는 전문 사이버 평가기관과의 협업을 통해 섹터별 사이버 리스크 노출도를 분석하고, 실제 사이버 침해사고 발생 시 펀더멘탈 및 궁극적인 상환능력을 훼손하는지 여부를 평가하여 신용도에 반영한다. Fitch 또한 사이버 리스크를 Event Risk 성격으로 보아 사고 발생 시 현금흐름, 유동성, 손실 회복력 등 실질 재무 영향을 평가하여 신용등급(전망)에 반영하는 것으로 파악된다.

S&P 는 사이버 침해사고 발생 전의 대비 수준, 즉 사이버 위생과 리스크 관리 체계를 중시한다. ESG 원칙상 사이버 리스크를 지배구조(Governance)의 하위 평가 요소로 명시하고 있으며, 분석과정에서 미국 NIST 사이버보안 프레임워크의 기능(식별·보호·탐지·대응·복구)을 참고로 활용한다고 밝힌 바 있다. 평가방법론 상 일반기업은 경영 및 지배구조(M&G) 평가의 하위요인인 '리스크 관리 및 내부통제'에서 사이버 보안을 포함한 우발위험 관리 체계 평가를 조정요소(Modifier)로 반영할 수 있다. 금융회사는 사업기반(Business Position) 내 지배구조·경영·전략 평가와 위험관리(Risk Position) 내 운영리스크 평가에서 사이버 리스크를 반영하고 있다. 사이버 침해사고 발생 시에는 영업 중단, 고객 이탈, 벌금·복구비용, 유동성 부담 등 사업·재무 영향과 복원력을 함께 고려하며, 사고가 즉각적인 등급 하락으로 이어지지 않더라도 대응이 지연될 경우 하향 압력으로 작용할 수 있다.

Moody's 는 사이버보안 전문기업인 BitSight 와의 전략적 제휴를 바탕으로 섹터별 사이버 리스크 노출도와 대비 수준을 평가한 '사이버 리스크 Heatmap'을 발표하고 있다. 다만 신용평가 시에는 사이버 리스크를 별도 평가항목으로 두지 않고 자연재해와 유사한 이벤트 리스크로

보아, 사고 발생 시 운영중단의 정도와 기간, 데이터 피해, 매출·비용 영향, 유동성·자본에 미치는 영향 등을 종합적으로 평가하여 신용도에 반영하고 있다.

Fitch 또한 사이버 리스크를 별도 평가항목으로 두지 않고 기존 사업·재무위험 분석과 ESG 체계에 통합하여 반영한다. ESG 관련성 점수(ESG Relevance Score)에서 데이터 보안은 사회(Social) 요소의 하위 항목으로 평가되며, 리스크 관리 역량은 경영진과 이사회의 책임 측면에서 함께 고려된다. Fitch는 사이버 침해사고를 사전에 예측하기 어려운 Event risk로 보아, 사고 발생 시 직접비용, 영업중단, 현금흐름·유동성·자본여력 영향이 기존 등급에 내재된 위험수준을 얼마나 변화시키는지 평가하여 신용등급(전망)에 반영한다.

[표 2] 글로벌 신용평가사의 사이버 리스크 관련 신용평가 사례

신용평가사	회사명	업종	사이버 침해사고	사이버 리스크의 신용도 전이	Rating Action
S&P	Tata Motors / Jaguar Land Rover	자동차 제조	2025년 JLR 사이버 공격	생산중단 → 매출·EBITDA 감소 → 레버리지 상승	Outlook Negative
	Clorox	소비재	2023년 사이버 공격	시스템 중단 → 생산·유통 차질 → 매출/수익성 악화	Outlook Negative
	캐나다 Hamilton시	지방자치 단체	2024년 사이버 공격	데이터 복구 지연 → 재무보고 및 risk management 취약성	AAA → AA+
	Travelex	외환/결제 서비스	2019년 랜섬웨어 공격	약 1개월 디지털 영업 중단 (신용등급 하향의 복합요인)	B- → CCC
	Bank of Valletta	은행	2019년 사이버 공격	채널 셧다운 → 운영리스크·거버넌스 취약성	BBB → BBB-
Moody's	Tata Motors / Jaguar Land Rover	자동차 제조	2025년 JLR 사이버 공격	생산·판매 중단 → 이익 감소	Outlook Positive → Negative
	Mount Sinai	의료(병원)	2024년 Change Healthcare 사이버 공격	청구·현금회수 지연, 실적부진 → 유동성 악화	Baa1 → Baa3, Negative
	SolarWinds	IT 소프트웨어	2020년 사이버 공격	거버넌스, 법률 및 재무 영향 불확실성	Review for Downgrade
	Equifax	신용정보 서비스	2017년 사이버 공격	정보 유출 → 법률·IT 비용 부담 확대	Outlook Negative
Fitch	Frederick Health	의료(병원)	2025년 사이버 공격	회복 지연이 재무/평판에 미칠 영향 불확실	BBB+ → BBB(↓)
	Palomar Health	의료(병원)	2024년 사이버 공격	장기 운영중단·핵심 billing 기능 장애 → 재무 악화	BB+ → B → B-
	ACMC Healthcare	의료(병원)	2024년 Change Healthcare 사이버 공격	수익창출 사이클 훼손, 시설투자 조달 증가 → 현금흐름 악화	BBB+ → BBB
	Ascension Health	의료(병원)	2024년 랜섬웨어 공격	사고 직후 강한 유동성 완충으로 등급 유지 → 사이버 관련 손실로 수익성 회복 지연되어 하향	AA+ → AA

자료) 각 신용평가사 자료 참조

4. KR의 사이버 리스크 신용평가체계와 개선 방향

경영 및 리스크 관리 등 사업항목과 ESG 관련 기타평가요소에 사이버 리스크 반영

사이버 리스크가 신용도에 미치는 영향은 사고 발생 자체보다 사고의 지속기간, 핵심 영업기능에 대한 영향, 재무적 흡수 능력, 사고 이후 운영 복원력과 회복 속도, 반복적인 통제 실패 여부 등에 의해 결정된다. 사이버 침해사고 발생시 ‘해킹을 막았는가’도 중요하겠지만 ‘공격받았을 때 얼마나 빨리 피해를 제한하고 정상영업으로 복귀할 수 있는가’가 보다 중요하다. 따라서 신용평가 측면에서 AI 시대 사이버위험에 대한 대응력은 단순히 보안에 많은 돈을 지출하는 것이 아니라, 공격 가능성을 낮추고 → 공격을 초기에 탐지하고 → 피해 확산을 차단하고 → 핵심 서비스를 지속하며 → 신속히 복구하고 → 사고 이후 통제체계를 개선할 수 있는가에 초점을 두고 있다.

반복적인 사이버 침해사고 발생은 운영리스크 관리와 내부통제에 대한 부정적인 신호가 될 수 있다. 재무능력 대비 손실(비용) 규모의 경우 일반기업은 EBITDA·FCF 대비로, 금융회사는 총 전영업이익, 자기자본, 유동성 버퍼 대비로 상대적인 부담 수준을 평가할 수 있으며, 사이버 보험으로 손실을 보전할 수 있는지 여부도 검토되어야 한다. 핵심 영업기능의 중단 여부 및 기간의 경우, 일시적인 개인정보 유출인지 아니면 수일간 결제 또는 거래가 중단되는 사고인지에 따라 신용도에 미치는 영향 수준이 달라질 수 있다. 사고 이후 보안투자가 증가했는지, 외주구조가 개선되었는지, 취약점이 제거되었는지를 확인하여 통제수준이 실질적으로 개선되었는지 확인할 필요가 있다.

한국기업평가는 금융회사 신용평가지 사이버 리스크를 사업항목 평가요소인 ‘경영 및 리스크 관리’ 매핑 변경요인으로 반영하거나 ESG 위험요인 관련 기타평가요소로 고려하는 방식으로 반영하고 있다. 특히 사이버 침해사고 발생시에는 재무적 능력 대비 손실(비용) 규모, 핵심 영업기능의 중단 여부 및 운영 복원력, 평판 저하에 따른 고객 이탈 수준 및 회복 기간, 사고 이후 통제수준의 실질적 개선 여부, 사고의 반복성 등을 종합적으로 고려하여 신용등급에 반영한다. 예를 들어 2025년 8월 대규모 정보유출 사고가 발생한 롯데카드의 경우 2026년 3월 정기평가지 경영 및 리스크 관리 평가요소 매핑을 하향조정할 바 있다.

사이버 리스크 발생빈 도 및 중요도 증가, 중장기적으로 보다 객관적인 평가지표 도입 방안 검토 예정

최근 국내 금융회사의 디지털 의존도가 높아지고 AI 기반 공격이 확산되면서 사이버 리스크 발생 빈도가 크게 증가하고 범위가 확대됨에 따라, 사이버 리스크가 수익성, 현금흐름, 유동성, 자본적정성, 규제비용, 평판 및 자금조달비용을 동시에 악화시킬 수 있는 복합적인 신용위험요인으로 진화하고 있으며 신용도에 미치는 중요도도 높아진 것으로 판단하고 있다. 이에 따라 중장기적으로 사이버 리스크를 정성적 평가항목으로 고려하는 것을 넘어 사이버 리스크 노출도에 대한 보다 객관적인 평가지표 도입 방안을 검토할 예정이다.

[유의사항]

- (1) 한국기업평가(주)(이하 ‘당사’)가 제공하는 신용등급은 특정 금융상품, 금융계약, 발행자 등의 상대적인 신용위험에 관한 분석 시점에서의 당사의 의견입니다. 또한, 당사가 제공하는 보고서 등의 제반 연구자료(이하 ‘간행물’)는 상기 특정 금융상품, 금융계약, 발행자 등의 상대적인 신용위험에 관한 당사 또는 필자 개인의 견해를 포함할 수 있습니다. 신용등급 및 간행물은 특별한 언급이 없는 한 신용위험을 제외한 다른 위험(금리나 환율변동 등에 따른 시장가치 변동위험, 해당 증권이 유동성위험, 내부절차나 시스템으로 인해 발생하는 운영위험)에 대해서는 설명하지 않습니다. 또한 신용등급 및 간행물에 포함된 당사의 의견은 현재 또는 과거 사실에 관한 진술이 아니며, 당사 고유의 평가기준에 따라 평가대상의 미래 상환능력 등에 대해 예측한 독자적인 견해로서, 이러한 예측정보는 실제 결과치와 다를 수 있습니다. 신용등급 및 간행물은 환경변화 및 당사가 정한 기준에 따라 변경 또는 취소될 수 있습니다.
- (2) 신용등급 산출 및 간행물 발간(이하 ‘신용평가업무 등’)에 이용되는 모든 정보는 평가대상회사 또는 기관이 제출한 자료와 함께 각종 공시자료 등의 자료원으로부터 수집된 자료에 근거하고 있으며, 당사는 제3자 요청 신용평가 등 예외적인 경우를 제외하고는 신용등급 산출 시 제출자료에 거짓이 없고 중요사항이 누락되어 있지 않으며 중대한 오해를 불러일으키는 내용이 들어 있지 않다는 확인서를 평가대상회사 또는 기관으로부터 수령하고 있습니다. 당사는 평가대상회사 또는 기관 및 이들 대리인이 정확하고 완전한 정보를 적시에 제공한다는 전제 하에 신용평가업무 등을 수행하고 있으며, 신용평가업무 등 과정에서 이용하는 정보에 대해 별도의 실사나 감사를 실시하고 있지 않습니다. 따라서 제공된 정보의 오류 및 사기, 허위에 따른 결과에 대해 당사는 어떠한 책임도 부담하지 않습니다.
- (3) 당사는 신용평가업무 등 과정에서 이용되는 정보에 대해 별도의 검증절차를 거치지 않았고, 분석자·분석도구 또는 기타요인에 의한 오류 발생 가능성이 있기 때문에 당사는 신용등급 및 간행물의 정확성 및 완전성을 보증하거나 확약하지 않습니다. 당사 간행물의 모든 정보들은 신용평가업무 등에 필요한 주요한 판단 근거로서 제시된 것으로 평가대상에 대한 모든 정보가 나열된 것은 아니며, 법률에 의하여 인정되지 않는 이상 당사 신용등급 및 간행물 상의 정보이용으로 발생하는 어떠한 손해 및 결과에 대해서도 당사는 책임지지 않습니다.
- (4) 당사는 금융상품의 매매와 관련한 조언을 제공하거나 투자를 권유하지 않습니다. 당사의 신용등급 및 간행물은 특정 유가증권의 매수, 매도 혹은 보유를 권유하는 정보가 아니며 시장 가격의 적정성에 대한 정보도 아닙니다. 당사의 신용등급 및 간행물은 그 내용으로 이용자의 투자결정을 대신할 수 없고 금융상품의 투자 결과에 대한 법적 책임소재를 판단하기 위한 증빙자료로도 사용될 수 없습니다. 따라서 정보이용자들은 스스로 투자대상의 위험에 대해 분석하고 평가한 다음 그 결과에 따라 각자 투자에 대한 의사결정을 하여야만 합니다. 특히, 당사의 신용등급과 간행물은 시장 전문기관을 일차적인 이용대상으로 하고 기본적으로 개인 투자자에 의한 이용을 전제로 하고 있지 않아 이를 이용하여 개인투자자 스스로 투자의사결정을 내리는 것은 적절하지 않을 수 있으므로 사전에 반드시 외부전문기관의 도움을 구할 필요가 있습니다. 아울러, 공시되지 않은 신용등급이나 제3자 요청 신용평가에 따라 산출된 신용등급의 경우 신용평가 요청인 이외에는 해당 신용등급을 믿고 이용하여서는 안 된다는 점을 밝혀 둡니다.
- (5) 본 보고서의 내용은 필자의 개인의견으로 당사의 공식의견이 아닙니다.

Copyright 2026, Korea Ratings Corporation. All Rights Reserved. 서울특별시 영등포구 의사당대로 97 대표전화: 368-5500 FAX: 368-5353.

본 보고서에서 제공하는 모든 정보의 저작권은 한국기업평가(주)의 소유입니다. 따라서 어떠한 정보도 당사의 서면동의 없이 무단으로 전재되거나 복사, 인용(또는 재인용), 배포될 수 없습니다.