

최근 금융회사 보안사고 주요 이슈와 보험산업 과제

요 약

최근 국내 금융권 보안사고는 외부자의 금융회사 외부 노출 시스템 및 제3자 연결 접점 침투가 주된 원인으로 지목되고 있음. 공격 측의 AI 활용이 현실화되는 가운데 보험산업도 전 밸류체인에서 AI 전환(AX)을 추진하면서 외부 연계와 공통 인프라 의존이 커지고 있으며, 이러한 특성은 제3자 위험과 공통 인프라 집중위험으로 심화될 수 있음. 따라서 보험산업은 보안 위험관리의 범위를 '개별회사 차원에서의 보안 통제'에서 '업권 차원의 공통 의존 관리'와 사고 발생 시에도 핵심업무를 이어가는 서비스 지속성 관리'까지 확장할 필요가 있음

1. 최근 금융회사 보안사고의 주요 이슈

○ 최근 국내 금융권 보안사고는 ① 사고를 일으킨 주체, ② 접근 방식, ③ 피해 확산 속도와 피해 회사 범위 측면에서 전통적인 금융권 보안사고와 다른 특징을 보임

- 전통적인 금융권 보안사고는 외주·파견 인력과 모집인 연계를 포함한 내부자가 업무용 권한을 남용해 업무 시스템에서 고객정보를 조회하고, 수개월에서 수년간 드러나지 않게 반출(USB, 출력, 화면 촬영 등)하는 등의 유형이 대표적이며 이러한 유형은 최근까지도 이어지고 있음
- 반면 최근 보안사고는 금전 목적의 범죄조직을 포함한 외부 공격자가 VPN, 결제 서버, 조회 서비스 등 관리가 상대적으로 취약한 외부 노출 접점이나 인증 허점을 통해 침투하며, 짧은 기간에 여러 기관에서 피해가 동시다발적으로 확산되는 특징을 보임

○ 특히 최근 외부 침투는 크게 외부 노출 시스템과 제3자 연결 접점의 두 경로로 나타남

- 패치가 누락된 결제 서버(롯데카드), 원격 접속용 VPN 장비(SGI서울보증) 등 인증과 접근 통제가 상대적으로 미흡했던 외부 인터넷 노출 시스템이 공격받음
- 대출모집인 전용 간편조회 서비스(신한은행), 영업지원 IT 협력업체에서 유출된 관리자 계정(GA 14개사), 가맹점 연동키(토스페이먼츠) 등 제3자 연결 접점이 외부 공격자의 표적이 됨

- 즉, 금융권 보안사고의 주된 원인이 ‘내부자의 권한 남용’에서 ‘외부 공격자의 노출 시스템 및 제3자 연결 점점 침투’까지 넓어짐

〈표 1〉 금융권 보안사고의 유형 변화

구분	전통적 유형(2011년~현재 지속)	최근 유형
사고 주체	내부자 중심 (외주·파견 인력, 모집인 연계 포함)	외부 공격자 중심
접근 방식	업무용 정상 권한으로 업무 시스템에서 고객정보를 조화하여 USB, 출력, 화면 촬영, 수기 기록 등으로 반출	관리가 취약한 노출 접점(VPN, 결제 서버, 조회 서비스 등)의 미패치 취약점, 인증 허점에 접근
피해 확산 속도 및 사고기관 범위	한 기관에서 수개월~수년간 조용히 진행 장기간 미인지	짧은 시간에 동시다발적으로 발생
대표 사례	시티은행, SC은행(2013), KB국민카드, 롯데카드, NH농협카드(2014), 우리카드(2022~2024), 신한카드(2022~2025)	GA 14개사(2025), SGI서울보증(2025), 롯데카드(2025), 코앰페이먼츠·토스페이먼츠(2026), 금융권 연쇄 해킹 16개사(2026)

자료: 각 사고 관련 기사를 참고함

- 더불어 전통 금융권 사고와 함께 이커머스, 결제 플랫폼 사고가 잇따르면서 서로 다른 곳에서 유출된 금융 정보와 생활 정보가 결합돼 개인별 맞춤형 피싱이나 사회공학적인 공격에 악용될 수 있다는 우려도 제기됨

- 이커머스, 결제 플랫폼 내 보안사고는 공동현관 번호, 구매 이력, 가족·지인 주소 등 금융거래 밖의 생활, 물리적 정보까지 유출 범위를 넓힘
- 유출 정보 자체를 결합해 악용한 피해는 아직 공식 확인되지 않았으나, 유출 정보가 축적·결합될 경우 전화·문자·SNS·이메일을 아우르는 정교한 맞춤형 공격에 활용될 가능성은 존재함

2. 보험산업 과제

- 최근 금융 보안사고에서 주목해야 할 점은 피해의 시작점이 핵심 금융거래 시스템뿐만 아니라 민감정보를 처리하는 주변 시스템이 될 수 있다는 사실임
- 보험회사 내부 시스템뿐만 아니라 고객정보를 처리하는 GA, 손해사정사, 콜센터, 전산 사업자와의 연결 관계까지 외부 공격의 표적이 될 수 있음

- 특히 보험회사는 건강·사고·가족관계 등 민감정보를 다수 보유해, 유출 시 협박이나 맞춤형 사기에 악용될 위험이 더 클 수 있음

○ 공격 측의 AI 활용이 현실화되는 가운데 보험산업도 전 밸류체인에서 AI 전환을 추진하고 있어, 이러한 금융 보안사고의 새로운 특성은 제3자 위험과 공통 인프라의 집중위험으로 심화될 수 있음

- AI는 공격에 필요한 시간과 전문 인력의 부담을 낮춰, 그동안 공격의 경제성이 낮았던 주변 시스템과 외부 접점이 표적이 될 가능성을 높임
 - 2026년 9~10월 금융권 연쇄 보안사고에서도 AI 침투테스트 도구가 활용된 정황이 보도되었으나 금융당국은 현재 AI 활용 여부를 조사 중임
- 특히 Agentic AI는 취약점 탐색과 공격 설계를 자동화해, 짧은 시간에 다수의 보험회사를 동시에 공격해 피해의 범위를 넓히고 확산 속도를 앞당길 수 있음
- 보험산업의 AX 과정에서 외부 AI 모델, 클라우드, 데이터 제휴, API 연계가 늘어나면 공격자가 노릴 수 있는 제3자 연결 접점도 함께 늘어남
- 여러 보험회사나 GA가 같은 전산 사업자, 영업지원 솔루션, 클라우드에 의존하게 되면, 공급자 한곳의 사고가 다수 회사로 동시에 번질 수 있음

○ 이에 국내에서도 외부 접점과 제3자 위험에 대한 대응이 진행되고 있음

- 금융보안원은 외부 노출 자산과 취약점을 지속적으로 식별하는 공격표면관리 서비스(Atlas ASM)를 제공하고, 2026년 8월 보험회사-GA 정보보안 협의체를 발족하는 등 제3자 보안 강화를 지원하고 있음
- 다만, 이는 외부 노출 자산의 취약점 식별과 제3자의 보안 수준 향상에 초점을 두고 있어, 여기서 확보한 정보가 업권 전체의 공통 의존관계와 핵심 기능 중단 위험관리로 이어지고 있는지는 점검할 필요가 있음

○ 따라서 보험산업은 보안 위험관리의 범위를 개별회사 차원에서의 보안 통제(자산관리, 수탁자 위험관리)에서 ① 업권 차원의 공통 의존관계 관리와 ② 사고 발생 시에도 핵심업무를 이어가는 서비스 지속성 관리까지 확장할 필요가 있음

- 개별 보험회사는 계약 시점의 위탁관리를 넘어 재수탁자(영업지원 IT업체 등)까지 포함한 제3자 의존관계를 파악하고 이들이 지원하는 보험 핵심 기능, 처리하는 데이터의 민감도, 대체 가능성을 기준으로 주요 제3자를 선별해 관리할 필요가 있음
- 업권 차원에서는 각 사의 주요 제3자 현황을 집계해 다수의 보험회사가 공통으로 의존하는 제3자를 파

악하고 집중위험을 관리할 필요가 있음

- 주요 제3자의 장애가 발생해도 사고 접수, 보험금·연금 지급 등 핵심업무를 이어갈 수 있도록, 업무별 중단 허용 한도와 회복에 필요한 시간과 비용을 파악하고 대체 수단을 마련할 필요가 있음
- 아울러 보험회사와 주요 제3자가 함께 참여하는 공동 장애 훈련을 통해, 실제 장애 발생 시 고객 피해와 서비스 중단을 허용 한도 안에서 막을 수 있는지 점검할 필요가 있음

손재희 연구위원
jaehee.son@kiri.or.kr



Recent Cybersecurity Incidents at Financial Institutions: Implications for the Insurance Industry

ABSTRACT

Recent cybersecurity incidents in Korea's financial sector have frequently involved external attackers exploiting vulnerabilities in financial institutions' internet-facing systems and third-party connections. As AI increasingly changes the cybersecurity threat landscape, the insurers are pursuing AI transformation (AX) across their value chain, potentially increasing their reliance on third-party services and shared infrastructure. These developments may heighten third-party risk and concentration risk arising from shared infrastructure. The insurance industry therefore needs to extend its risk management beyond individual insurers' security controls to address sector-wide common dependencies and maintain critical insurance services during cyber incidents.

1. Key Issues in Recent Cybersecurity Incidents at Financial Institutions

Recent cybersecurity incidents in Korea's financial sector exhibit different characteristics from traditional incidents in terms of (i) the perpetrators, (ii) the methods of intrusion, and (iii) the speed and scope of their impact across financial institutions. Traditional incidents have typically involved the misuse of legitimate access privileges by insiders and affiliated personnel, including outsourced staff, temporary workers, and individuals involved in insurance solicitation. Such incidents continue to occur. By contrast, recent incidents have involved external attackers, including financially motivated criminal groups, exploiting poorly protected internet-facing systems or authentication weaknesses in VPNs, payment

servers, inquiry services, and similar systems. Such incidents may affect multiple institutions within a short period.

Recent external intrusions have followed two main routes: internet-facing systems and third-party connection points. Examples include an unpatched payment server at Lotte Card and remote-access VPN equipment at SGI Seoul Guarantee Insurance, illustrating vulnerabilities in internet-facing systems and access controls; the latter include a simplified inquiry service for loan solicitors at Shinhan Bank, administrator accounts leaked from an IT vendor providing sales support to 14 general agencies (GAs), and merchant integration keys at Toss Payments. Cybersecurity incidents in the financial sector now arise not only from insiders' abuse of access privileges but also from external intrusions through internet-facing systems and third-party connection points.

〈Table 1〉 Changes in Types of Cybersecurity Incidents in the Financial Sector

Category	Traditional Patterns (2011–Present)	Recent Patterns
Perpetrators	Primarily insiders, including outsourced or dispatched personnel and insurance solicitors and affiliated personnel	Primarily external attackers
Access methods	Customer information accessed through legitimate business privileges and exfiltrated via USB drives, printouts, screenshots, handwritten notes, and similar means	Exploitation of unpatched vulnerabilities and authentication weaknesses at poorly managed exposed endpoints, including VPNs, payment servers, and inquiry services
Speed and scope of impact	Incidents proceed quietly within a single institution over months or years and remain undetected for long periods	Incidents occur simultaneously across multiple institutions within a short period
Representative cases	Citibank and Standard Chartered Bank Korea (2013); KB Kookmin Card, Lotte Card, and NH Nonghyup Card (2014); Woori Card (2022–2024); Shinhan Card (2022–2025)	14 GAs (2025); SGI Seoul Guarantee Insurance (2025); Lotte Card (2025); Coam Payments and Toss Payments (2026); a series of cyberattacks affecting 16 financial firms (2026)

Source: Compiled from news reports on the respective incidents.

At the same time, a series of incidents at e-commerce and payment platforms, alongside incidents in the traditional financial sector, has raised concerns that financial information and lifestyle data leaked from different sources could be combined and exploited in personalized phishing or social engineering attacks. Security incidents at e-commerce and payment platforms have exposed information beyond financial transaction data, including building entrance codes, purchase histories, and addresses of family members and acquaintances. No cases of misuse involving the combination of data leaked from different sources have been officially confirmed. However, the accumulation and combination of leaked information could enable more sophisticated, targeted social engineering attacks through phone calls, text messages, social media, and email.

2. Challenges for the Insurance Industry

One key lesson from recent financial-sector cybersecurity incidents is that incidents may begin not only in core financial transaction systems but also in peripheral systems that handle sensitive information. Connections with insurance general agencies (GAs), loss adjusters, call centers, and IT service providers that process customer information can also become targets of external attacks. Insurers in particular hold large volumes of sensitive information on health, accidents, and family relationships. If disclosed through a data breach, such information could be exploited for extortion or targeted fraud.

As the use of AI in cyberattacks becomes increasingly feasible and the insurance industry pursues AI transformation (AX) across its value chain, these new characteristics of financial-sector cybersecurity incidents may heighten third-party risk and concentration risk arising from shared infrastructure. AI reduces the time and technical expertise required to carry out cyberattacks, making peripheral systems and external interfaces that were previously less attractive targets more susceptible to attack.

Agentic AI, in particular, can automate vulnerability discovery and attack planning, potentially enabling attackers to target multiple insurers in rapid succession and increasing the speed and scale of potential attacks.

As the insurance industry's AX efforts increase the use of external AI models, cloud services, data partnerships, and API connections, the number of third-party connection points that attackers can target will also grow. If multiple insurers or GAs rely on the same IT service provider, sales-support solution, or cloud service, an incident at a single provider could simultaneously affect multiple firms.

Measures to address external connection points and third-party risk are also being introduced in Korea. The Financial Security Institute provides Atlas ASM, an attack surface management service that continuously identifies externally exposed assets and vulnerabilities. It also launched an information security council for insurers and GAs in August 2026, supporting efforts to strengthen third-party security. However, these measures focus primarily on identifying vulnerabilities in externally exposed assets and improving third-party security. It is therefore necessary to assess whether the information gathered through these measures is being used to manage common dependencies across the insurance sector and the risk of disruption to critical functions.

The insurance industry should therefore extend its cybersecurity risk management beyond individual insurers' security controls, including IT asset management and third-party risk management, to (i) address sector-wide common dependencies and (ii) maintain the continuity of critical insurance services during disruptions. Individual insurers should extend their oversight of outsourced service providers beyond the initial contracting stage and map their third-party dependencies, including subcontractors such as IT vendors providing sales-support services. They should identify and manage key third parties based on the critical insurance services they support, the sensitivity of the data they handle, and the availability of substitutes. At the sector level, information on each insurer's key third parties should be aggregated to identify providers on which multiple insurers depend and to manage concentration risk.

To maintain critical insurance services such as claims intake, claims payments, and annuity payments during disruptions affecting key third parties, insurers should define impact tolerances for important business services for each service, assess recovery time and cost, and establish alternative arrangements. Insurers and key third parties should also conduct joint disruption scenario exercises to test whether they can keep customer harm and service interruptions within the defined tolerances.

Jaehee Son, Research Fellow
jaehee.son@kiri.or.kr