KiRi 리포트 2018.1.15.
글로벌 이슈

미국의 보험데이터보안모델법

박정희 선임연구원

요약

미국 보험감독자협의회는 18개월간의 심의과정을 거쳐 보험데이터보안모델법을 승인함. 동 법안에 따라 보험회사는 사전적인 자체 위험평가에 기반하여 데이터보안 중심(데이터유출 통제, 파기, 암호화 등)의 정보보안프로그램을 구축하고 실행 및 관리해야 함. 사후적으로는 비공개정보의 기밀성과 무결성을 저해하는 사이버보안 사건 발생 시 보험회사는 즉각 이를 조사하고 주(州)보험감독청장에게 관련 내용을 신고해야 하며, 해당 기록은 5년 이상 보관 · 유지해야 함

미국 보험감독자협의회(NAIC: National of Insurance Commssioners)는 18개월간의 심의과정을 거쳐 보험데이터보안모델법(이하 데이터보안법)을 승인함[1)]

- 데이터보안법은 데이터보안 표준 및 사이버보안 사건(Cybersecurity Event)[2)]에 대한 주(州)보험감독청장의 조사 · 신고 표준을 수립하기 위해 발효된 법안임
  - 사전적으로는 보험회사, 대리점 및 기타 단체[3)]의 주(州)보험감독청이 규제하는 데이터보안 중심의 정보보안프로그램[4)] 구축, 사후적으로는 사이버보안 사건 발생 시 조사, 신고 등을 규제함
- 이 법안은 2017년 3월 시행된 뉴욕금융서비스국(NYDFS)의 사이버보안규정[5)]인 위험평가 기반의 사이버보안 체계 구축 내용과 유사함

동 법안에 따라 보험회사는 사전적으로 자체 위험평가에 기반한 데이터보안 중심(데이터유출 통제, 파

1) NAIC(2017. 10. 24), "NAIC Passes Insurance Data Security Model Law", Cybersecurity model law creates information security standards for insurers
2) 정보시스템 또는 정보시스템에 저장된 정보에 무단으로 접촉하거나 중단 또는 오용을 유발하는 이벤트를 의미함
3) 비공개정보(nonpublic information)에 접근이 가능한 면허소지자 또는 해당 정보시스템에 접근이 가능하도록 허가 받은 자
4) 인가된 사용자가 비공개정보를 접근, 수집, 배포, 처리, 보호, 저장, 사용, 전송, 처분 등을 위해 사용하는 관리상, 기술상, 물리적 안전장치를 의미함
5) NY Comp. Codes R. & Regs. tit.23, § 500, Cybersecurity Requirements for Financial Services Companies는 뉴욕주의 모든 금융기관(은행, 보험, 금융서비스 기관 등)에 적용되는 금융서비스업 규제임

기, 암호화 등)의 정보보안프로그램을 구축하고, 실행 및 관리해야 함

- 정보보안프로그램은 비공개정보의 보안 및 암호화를 통한 보호조치, 정보시스템의 내·외부의 위협으로부터 소비자의 피해를 최소화하는 것임
  - 비공개정보라 함은 사업관련 정보(유출 시 사업, 운영, 보안 등에 악영향을 끼치는 정보), 개인식별정보(개인정보, 계좌 및 신용카드정보, 생체인식기록 등), 건강정보(의료제공자 또는 소비자에 의해 파생된 모든 헬스케어 관련 정보) 등을 포함
- 보험회사는 해당 정보시스템 내에서의 위협 가능성과 비공개정보의 손상으로 인한 잠재적 손실을 평가하기 위해 최소 1년마다 정보보안 위험평가를 수행해야 함
  - 이러한 위협을 관리할 수 있는 정책, 절차, 정보시스템 및 기타 안전장치 등이 충분한지(직원교육 및 관리, 네트워크 및 소프트웨어 설계, 정보 분류, 처리, 저장, 전송 및 파기, 시스템 오류 감지, 공격 방지 및 대응)를 평가
- 이런 위험평가를 효과적으로 관리하기 위해서는 보험회사가 정보시스템에 대한 접근을 인가된 사용자에 한해 가능하도록 통제하고 개별 접근 시 다중요소인증[6]절차 등을 거치도록 함
  - 또한 비공개정보는 주기적으로 안전하게 파기해야 하며, 정보시스템에 대한 실제 또는 시도된 공격을 탐지하기 위해 정기적인 테스트와 모니터링이 필요함
- 이 외에도 제3자 서비스제공자[7]가 접근할 수 있는 비공개정보 및 정보시스템의 보안이 적절하게 관리되고 조치되는지 감독하고 필요 시 기술적 보호장치를 요구해야 함

■ 비공개정보의 기밀성과 무결성[8]을 저해하는 사이버보안 사건 발생 시 보험회사는 즉각적으로 이를 조사하고 주(州)보험감독청장에게 관련 내용을 신고해야 하며, 해당 기록은 5년 이상 보관·유지해야 함

- 사이버보안 사건이 발생했거나 발생할 가능성을 인지하였을 경우, 사건의 실제 발생여부 및 사건의 성격과 범위, 정보공개에 관련된 비공개정보 등을 신속하게 조사하여야 함
  - 추가적인 피해를 방지하기 위해 손상된 시스템보안 복원에도 적절한 조치를 병행해야 함
- 실제 발생한 사이버보안 사건은 5년 이상 모든 기록을 보관·유지해야 하며, 사이버보안 사건 발생이 확인된 경우 72시간 이내에 주보험감독청장에게 관련 내용을 신고해야 함
- 또한 각 보험회사는 매년 2월 15일까지 데이터모델법에 명시된 정보보안프로그램의 요구사항을 준수하고 있음을 증명하는 연간 보고서를 해당 보험감독청장에게 제출해야 함 KiRi

6) 비밀번호, 휴대전화를 통한 인증메세지, 생체특성과 같은 내재적 요인 중 최소 두 가지 유형의 인증요소를 검증하여 인증
7) 보험회사와의 계약을 통해 비공개정보를 유지, 처리, 저장 또는 접근할 수 있는 자
8) 데이터의 정확성을 보장하기 위해 데이터의 저장이나 전송이 승인되지 않은 방법 등으로 변경할 수 없도록 일관성을 유지하고 보증하는 것을 의미