KiRi 리 포 트
글로벌 이슈

바이든 정부의 사이버보안과 보험산업의 역할

홍보배 연구원

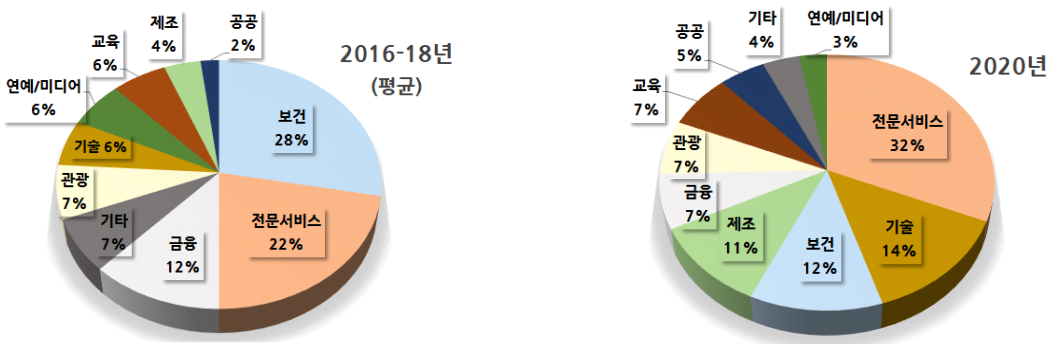
요 약

코로나19 확산의 영향으로 디지털 경제화가 가속화되면서 사이버보안 위험이 심화되고 있음. 특히 정부 및 대기업을 동시다발적으로 공격하는 시스템적 위험이 지속되는 상황임. 이에 따라 바이든 정부는 사이버보안 정책 강화를 국정의 우선순위로 표명하고 정부와 기업, 보험업계 간 정책공조 강화를 주문함. 보험업계는 이러한 정책 추진방향에 발맞춰 사이버 보안시장에서의 역할과 기능을 재정립 할 필요가 있음

○ 코로나19 확산의 영향으로 디지털 경제화가 가속화됨에 따라 사이버보안 위험이 심화되는 가운데 특히 정부 및 대기업을 동시 다발적으로 공격하는 시스템적 사이버위험(Systemic Cyber Risk)이 고조되고 있음

- 디지털 경제화가 가속화되는 동시에 이를 목표물로 한 사이버공격이 큰 폭으로 증가함에 따라 지난 '20년 사이버 범죄에 따른 글로벌 경제적 비용은 약 1조 달러, 세계 GDP의 1%에 달할 것으로 전망됨[1)]
- 미국 산업 전반적으로 사이버공격 빈도가 증가하는 추세지만, 특히 재택근무 확대에 따른 법률, 회계 등의 전문서비스(professional services) 산업의 피해가 심화되면서 '20년 북미 사이버 보험금 청구 건수 기준으로 전체의 32%를 차지함[2)]
  - 코로나19 발생 전체 기간(2016~2018년)에는 보건·금융산업의 피해가 집중되었던 데 비해, 최근에는 전문서비스·기술산업의 사이버공격 피해 비중이 높아지고 있음(〈그림 1〉 참고)
- 최근 외부세력이 미국 군대, 정보기관, 재무부 등 공공기관 및 포춘 500대 기업 다수가 사용하는 보안솔루션 제공업체의 소프트웨어를 해킹한 일명 'SolarWinds Hack' 사건 발생과 같은 시스템적 사이버위험이 커지고 있음

〈그림 1〉 북미 사이버위험 보험금 청구 건수 비중(산업별)



자료: Chubb(2020)

1) McAfee(2020. 12), "The hidden costs of cybercrime"
2) Chubb(2020), "Cyber Infocus"

○ 바이든 정부는 출범과 동시에 사이버보안 강화를 국정 정책방향의 최우선 순위(priority) 중 하나로 표명하고 정부와 기업, 보험업계 간 협력을 통한 효율적인 사이버위험 대응 시스템을 수립할 것을 주문함

- 바이든 정부는 2021년 1월 출범과 동시에 약 90억 달러에 달하는 사이버보안 예산을 편성하고 사이버보안 분야 최고 전문가들을 관련 정부기관 수장으로 대거 지명하였으며[3], 금융·보건기관 등 사이버위험 노출이 큰 기업에 사이버보험 가입을 의무화하는 규제를 도입할 예정임[4]
- 또한 사이버통계국(Central Bureau of Cyber Statistics)을 설립하여 정책당국과 시장 간 신뢰성 높은 사이버보안 데이터를 공유하고, 보험업계 및 사이버보안 전문가로 구성 된 작업반(working group)을 신설하여 보험료 산정 체계 표준화 등 사이버보험 시장 발전 방안을 모색하기로 함[5]
- 한편 금융당국은 사이버위험이 고조됨에 따라 보험사의 사이버위험 관리능력 점검 등 적극적 선제조치를 권고함
  - 뉴욕주금융국(NY Department of Financial Services)은 최근 손해보험업계에 사이버보험 인수와 관련하여 7가지 위험관리 프레임워크(Cyber Insurance Risk Framework)를 제시하고, 특히 사이버위험과 관련한 시스템적 위험과 묵시적 위험(silent risk)[6] 관리 능력을 보강할 것을 주문함[7]
  - 재무부(US Treasury)는 미국 공·사 협력 테러리즘 프로그램(Terrorism Risk Insurance Program: TRIP)을 통한 사이버테러 위험 보장 관련 세부내용 명료화 등 제도개선 방안 논의를 진행 중임[8]

○ 보험업계는 이와 같은 정책 추진방향에 발맞춰 정부와의 정책 공조를 강화하는 동시에 사이버보안 시장에서의 역할과 기능을 재정비할 필요가 있음

- '21년 사이버보험 시장의 성장은 지속될 것으로 전망되나, 시스템 또는 묵시적 위험 발생에 따른 보험사의 대규모 손실 가능성도 상존하는 상황으로, 이에 대비한 위험관리 능력 확충 등 사전 제도 마련이 중요할 것임
- 특히 시스템적 사이버위험은 다수의 기업에 대규모 피해를 초래하여 보험산업의 인수능력을 초과하는 손해를 발생시킬 가능성이 높기 때문에 이에 대한 정부 및 보험업계의 정책공조 강화가 필수적임
- 또한 바이든 정부가 사이버보안 정책 강화에 중점을 두는 만큼 보험업계는 사이버보안 시장에서 어떠한 핵심적인 기능을 할 것인지 역할 재정립의 과제가 남아있음
- 우리나라도 글로벌 및 미국 사이버공격 동향을 예의주시하는 동시에 국내 위험 발생가능성 점검 및 보험시장을 통한 대비책 강화 등의 논의가 지속되어야 함

---

3) Reuters(2021. 1. 22), "After big hack of U.S. government, Biden enlists 'world class' cybersecurity team"
4) Forbes(2021. 1. 19), "The next five years: Cyber Insurance Predicitions Through 2025"
5) Axios(2020. 12. 2), "Setting the Biden-era cybersecurity agenda"
6) 사이버 리스크에 대한 보장을 포함하는지, 제외하는지에 대해 명확히 하지 않은 보험계약과 관련된 리스크를 의미함. 상세한 내용은 변혜원(2018), 「일반손해보험에 내재된 사이버 리스크 관리」, 『KIRI리포트』, 보험연구원을 참조 바람
7) Department of Financial Services NY(2021. 2), "Insurance Circular Letter No. 2"
8) Department of Treasury(2020. 11), "Treasury Issues Notice of Proposed Rule Clarifying the Terrorism Risk Insurance Program"