



# 보도자료

담당자 손재희 소비자·디지털연구실장(3775-9023)

보도 2026. 3. 19.(목) 16:00부터

홍보담당 변철성 수석역(3775-9115)

매수 총 10매

## 보험연구원, 「사이버 리스크의 일상화, 보험산업의 과제와 대응전략은?」 공동국제세미나 개최

사이버 보안 및 보험업계, “사이버 리스크가 기업의 일상적 경영위험으로  
확대… 보험과 정책의 협력 대응 필요” 공감

- 보험연구원(원장 김헌수)과 유동수 국회의원, 포항공과대학교(AIRM연구센터)는 3월 19일(목) 한국경제인협회 컨퍼런스센터 에메랄드홀에서 「사이버 리스크의 일상화, 보험산업의 과제와 대응전략은?」이라는 주제로 국제세미나를 공동 개최하였음
- 이번 세미나는 대규모 개인정보 유출이 반복되는 환경에서 국내 사이버 보험시장의 현황과 과제를 진단하고, 기업의 사이버 보안 역량 강화와 사이버 보험시장 확대를 위해 제도와 시장 간 균형 있는 협력 모델을 모색하고자 마련됨
- 유동수 국회의원(더불어민주당 정무위원회)은 환영사에서 “대형 사이버 사고에 대비해 공공과 민간이 위험을 분담하는 협력 모델에 대한 본격적인 논의가 필요한 시점”이라고 강조하며, 이번 국제세미나가 “사이버 보안 제도와 사이버 보험시장의 균형 있는 발전을 위한 대응 전략을 모색하는 계기가 될 것”이라고 밝힘
- 김헌수 보험연구원장은 이날 축사를 통해 “사이버 보험의 핵심 과제는 점점 더 예측하기 어려워지는 위험을 시장 내에서 평가·인수·관리 가능한 체계로 정립해 나가는 데 있다고 화두를 제시하고,
  - “앞으로 국내 사이버 보험시장의 안정적인 성장을 위해서는 위험평가 역량의 고도화, 보장 구조에 대한 신뢰 제고, 사고 대응 체계와의 연계, 그리고

제도적 기반 정비라는 다각적인 논의가 필요함을 강조하였음

- 본 행사를 기획한 포항공과대학교 정광민 교수는 “인공지능 기술의 급속한 발전과 범용화는 개별 경제 주체의 사이버 위협의 관리를 더욱 어렵게 할 수 있음”을 강조하고,
  - “기업 경영 전반에서의 사이버 위협 인식을 제고하고 보안 투자와 역량을 강화하기 위한 제도적 체계를 마련함과 동시에, 사이버 보험시장이 개별 위협 관리의 공백을 메우는 효과적인 역할을 수행할 수 있도록 환경을 조성할 필요가 있음”을 강조하였음
- 김·장 법률사무소 김홍선 고문은 제1주제 『사이버 위협과 리스크관리, 그리고 사이버 보험의 등장』 발표를 통해 급증하는 사이버공격에 대처하는 방안을 제시하였음
- 안랩 박태환 ACSC센터장은 제2주제 『최신 사이버 보안 위협 동향과 대응방안』 발표를 통해 사이버 보안 위협의 현재 상황, 최근 사이버 공격의 특징, 사이버 상에서의 대한민국의 상황, 대응방안을 제언함
- 법무법인 세종 최광희 고문은 제3주제 『사이버 사고로 직면하게 되는 기업의 위협』 발표를 통해 사이버 사고가 단순히 기술적 위험을 넘어 기업 전반의 경영위험이 되고 있다고 강조함
- 삼성화재 Sie Lau 사이버 Head는 제4주제 『해외 사이버 보험시장 현황과 시사점』 발표를 통해 국내 사이버 보험시장 발전 전략 수립에 참고할 수 있는 해외사례 등을 제언함
- 보험연구원 손재희 실장은 제5주제 『국내 사이버 보험시장 현황과 도전과제』 발표를 통해 국내 사이버 보험시장의 낮은 성장을 극복하기 위한 대응 방안을 수요와 공급 측면에서 제안함
- 프로시스 언더라이팅 솔루션즈 최용민 부대표는 제6주제 『한국 사이버 보험 생태계 구축을 위한 실천적 로드맵』 발표를 통해 정부의 강력한 주도하에 시장 내 각 역할 주체가 함께하는 사이버 보험 생태계 구축과 관련한 로드맵 추진을 제안함

**- 프로그램 -**

시간	내 용
13:30 ~ 13:35	(환 영 사) 유동수 (인천 계양구(갑) 국회의원)
13:35 ~ 13:40	(축 사) 김현수 (보험연구원 원장)
13:40 ~ 13:50	단체사진 촬영(VIP 및 발표자)
<b>&lt;세션1 : 사이버 리스크 환경과 보안기술&gt;</b>	
13:50 ~ 14:10	(주제발표1) 사이버 위협과 리스크관리 그리고 보험의 등장 김홍선(김·장 법률사무소 고문)
14:10 ~ 14:30	(주제발표2) 최신 사이버 보안 위협 동향과 대응방안 박태환(안랩 사이버시큐리티센터(ASCS) 센터장)
14:30 ~ 14:50	(주제발표3) 사이버 사고로 직면하게 되는 기업의 위험 최광희(법무법인 세종 고문)
14:50 ~ 15:00	Break Time
<b>&lt;세션2 : 국내 사이버 보험시장 발전 전략&gt;</b>	
15:00 ~ 15:20	(주제발표4) 해외 사이버 보험시장 현황과 시사점 Sie Lau(삼성화재 Head of Cyber)
15:20 ~ 15:40	(주제발표5) 국내 사이버 보험시장 현황과 도전과제 손재희(보험연구원 실장)
15:40 ~ 16:00	(주제발표6) 한국 사이버 보험 생태계 구축을 위한 실천적 로드맵 최용민(프로시스 언더라이팅 솔루션즈 부대표)
16:00 ~ 16:10	Break Time
16:10 ~ 17:00	(패널토론) 좌 장 : 정광민(포항공과대학교 교수) 토 론 : 발제자 전원 자유토론

- (주제발표 1) 김홍선 고문은 ‘사이버 위협과 리스크관리, 그리고 사이버 보험의 등장’이라는 주제로 급증하는 사이버 공격에 대처하는 방안을 제시하였음
  - (사이버 위협 지형) 디지털 의존도가 높아지면서 사이버 위협은 조직적인 범죄로 지능화되어 갔는데, 랜섬웨어로 빠른 현금화가 가능해지면서 공격의 패러다임과 생태계가 크게 바뀌었음
    - 2025년 한국에 랜섬웨어 사고가 급증했고, 서비스 중단에 충격이 큰 기업을 대상으로 글로벌 해킹그룹의 조직적인 공격이 전개되고 있음
  - (침해사고대응) 침해사고는 사고대응과 복구부터 고객, 언론, 규제기관 등 다양한 주체들에게 신속하게 통지하고 소통하는 데 이르기까지 경영진의 위기관리 능력이 중요함
    - 특히 랜섬웨어 공격자는 백업체계도 공격하기에 사이버공격에 특화된 사이버 레질리언스 체계로 업그레이드해야 함
    - 또한 공급망 생태계에 미치는 영향에 대비하고, 향후 법적·재무적 리스크를 면밀하게 파악해서 대비해야 함
  - (리스크관리체계와 사이버 보험의 등장) 오늘날 대부분의 업무가 IT로 처리되는 환경에서 사이버 보안은 비즈니스 리스크이며, 이사회 어젠다로 규제가 강화되고 있음
    - 사이버 보안을 경영 리스크의 관점으로 준비하기 위해서는 ① 보안사고를 IT문제가 아닌 비즈니스 임팩트로 지표화하고, ② 리스크를 식별하고 통제하는 관리체계를 수립·운영하며, ③ 잔여리스크 관리와 침해사고 대비를 위한 방안을 준비해야 함
    - 사이버 보험은 ③ 단계의 해결책의 하나로 등장했으며, 정량적인 리스크 평가를 기반으로 정밀한 기법으로 발전하고 있음. 모든 기업은 전사적인 보안 거버넌스를 통해 AX 전환 시대에 대비해야 함

- (주제발표 2) 박태환 안랩 ACSC 센터장은 ‘최신 사이버 보안 위협 동향과 대응 방안’이라는 주제로 사이버 보안 위협의 현재 상황, 최근 사이버 공격의 특징, 사이버 상에서의 대한민국의 상황, 대응방안을 제언함
  - (사이버 보안 위협의 현재 상황) 확장된 공격 대상, 조직화된 공격 조직, 사이버 공격이 서비스 산업의 하나로 자리하게 된 사이버 보안 위협의 현재 상황을 주요 사건사고 사례를 통해 살펴 봄
  - (최근 사이버 공격의 특징) 가장 큰 특징은 조직화와 산업화임. 과거 개인해커 중심의 공격에서 현재는 조직화된 범죄 그룹(Qilin 랜섬웨어그룹, 랩서스(Lapsus)해킹그룹 등)이 활동 중이고, 공격 도구와 해킹 서비스(RaaS - 랜섬웨어 서비스)까지 판매 중임
    - AI 기술이 사이버 공격에 악용되면서 피싱, 딥페이크/딥보이스, 공격자동화 등이 증가한다는 소식까지 나오면서 단순 범죄에서 지속 진화하는 산업형 위협으로 자리 잡았음을 보여 줌
  - (사이버 상에서의 대한민국의 상황) 정치, 군사적인 이해관계에 따라 대한민국의 의지 여부와는 상관없는 사이버 공격이 발생하나 이것은 표면적으로 드러나는 공격에 해당하는 것일 뿐, 드러나지 않는 공격들은 꾸준함을 유지하고 있음
  - (대응방안) 기업과 조직은 기술적 보안체계를 준수 및 강화하고, 피해 최소화를 위한 대응/복구 계획도 수립하되, 국가와 정부, 기업 등 각자 맡은 분야에서 자신들의 역할을 충실히 하면서도, 사이버 위협에 대응하는 데 필요한 보안 기술, 사고대응 체계, 보안 정책 및 정보 공유 등은 다층적인 협력 모델을 구체화하려는 노력이 필요함

- (주제발표 3) 법무법인(유) 세종 최광희 고문은 그간 주요 사이버 침해사고 대응 경험을 바탕으로 사이버 사고가 단순히 기술적 위험을 넘어 기업 전반의 경영위험이 되고 있다고 강조하며, 사이버 보험도 사후 보상 중심에서 사이버 사고 현장에 필요한 서비스를 적시에 제공해 기업의 리스크를 완화할 수 있는 방향으로 발전해 나가야 한다고 제언함
- (사이버 사고의 위험) 사이버 사고는 매년 증가하고 있으며 사이버 공격 수단이 전략 무기로 사용될 만큼 이로 인한 기업의 피해도 커지고 있는 상황임
  - 과학기술정보통신부에 따르면 '25년 사이버침해사고 신고는 2,383건으로 전년 대비 26.3%가 증가하였고, 중소기업의 피해가 많은 랜섬웨어의 경우 해외 조사기관에 따르면 '31년에는 2초마다 한 개 기업꼴로 피해를 받을 것으로 예상됨
  - 반면 미국과 이란 전쟁에서 사이버 공격은 상대 국가의 통신과 중요 인프라를 마비 시키고 사회적 혼란을 초래하는 핵심 전략 무기로 사용될 만큼 위험도가 높음
- (사이버 사고로 인한 위험) 사이버 사고가 발생하는 순간 기업은 규제기관 조사, 부정적 여론, 법적 처벌, 사후 대응 비용 등 다양한 경영 위험이 발생하게 됨
  - 규제기관 조사 위험 : 사이버 사고로 개인정보가 유출될 경우 과기부, 개보위 등 복수의 규제기관의 조사가 진행되며 최종 처분까지 6개월 이상 조사를 받게 됨
  - 대외 평판 위험 : 사고 초기 명확한 원인과 피해 범위가 확인될 때까지 사고 은폐·축소 여론이 확산되고 국회 청문회로 이어져 기업의 부정적 이미지가 생성됨
  - 법적 위험 : 최근 조사기관의 엄정 대응 기조로 개인을 대상으로 한 형사상 처벌과 높은 과징금이 부과되고 있으며 대형 사고는 100여 건 이상의 민사소송이 발생됨
  - 재무적 위험 : 과징금 및 과태료뿐 아니라 사고 원인에 따른 보안 체계 강화를 위한 보안 투자비용, 법무비용, 손해배상 등 큰 규모의 장기 지출 소요가 발생할 것으로 전망됨
- (제언) 사이버 보험은 사후 보상 중심에서 사이버 사고 시 필요한 원인 조사, 법률 대응 등의 긴급 서비스를 제공하여 기업의 초기 위험을 완화할 수 있도록 개선이 필요함

- (주제발표 4) Sie Lau 삼성화재 사이버 Head는 ‘해외 사이버 보험시장 현황과 시사점’을 주제로 국내 사이버 보험시장 발전 전략 수립에 참고할 수 있는 해외사례 등을 제언함
  - (사이버 리스크의 확대) 사이버 위험은 이제 단순한 IT 문제를 넘어 기업과 국가 인프라를 위협하는 핵심 경제 리스크로 확대되고 있음
    - 최근 10년간 글로벌 사이버 보험시장은 급격히 성장하여 연간 약 160~180억 달러 규모로 확대되었으며, 특히 '20~'22년 랜섬웨어 공격 급증으로 보험회사들이 대규모 손실을 경험함
    - 이에 따라 보험 조건을 강화하고, 보험 약관을 명확히 하며, 위험 모델링을 고도화 하는 등 시장 전반의 리스크관리 체계 정비가 이루어지고 있음
  - (Systemic 위험의 증가) 클라우드 인프라와 소프트웨어 공급망의 상호 연결성 증가로 인해 단일 취약점이 전 세계로 확산되는 Systemic 위험이 확대되고 있음
    - 한국도 사이버 보험시장을 확대하는 과정에서 보험회사, 사이버 보안 기업, 규제 당국 간 협력 체계를 조기에 구축할 필요성이 강조됨
  - (예방적 생태계 조성 필요성) 단순히 보험 상품을 제공하는 것을 넘어 사이버 위험을 줄이는 예방 중심의 생태계를 구축하는 것이 중요함
    - 해외에서는 보험회사가 기업의 사이버 보안 수준을 평가하고 그 결과에 따라 보험료를 차등 적용하는 ‘보안 점수 연동 제도’가 도입되고 있으며, 이는 위험 관리의 책임을 보험 가입자에게도 분산시키는 효과를 보이고 있음
    - 한국은 아직 보험회사와 보안기업 간 데이터 공유가 제한적이며, 규제 프레임워크도 부족한 실정임. 이에 표준화된 사이버 위험 평가 지표를 마련하고, 보험회사가 이를 활용할 수 있도록 법·제도적 기반을 구축할 필요가 있음
    - 또한, 사이버 공격의 주요 표적이 되는 중소기업을 대상으로 한 보험 상품 개발과 보험료 지원 정책도 시급함. 중소기업에 대한 보호 장치가 부족할 경우 전체 경제 생태계의 안정성이 훼손될 가능성이 있음

- (주제발표 5) 손재희 실장(보험연구원)은 ‘국내 사이버 보험시장 현황과 도전과제’를 주제로 국내 사이버 보험시장의 낮은 성장을 극복하기 위한 대응방안을 수요와 공급 측면에서 제안함
  - (국내 사이버 보험시장 현황) 글로벌 공급망 의존 심화, 디지털화 진전으로 인한 클라우드 운영 확대, AI 기반 공격 고도화 등으로 국내 사이버 리스크도 높아지고 있으나, 사이버 보험시장 규모는 글로벌 대비 상대적으로 낮은 수준임
    - 인터넷진흥원(KISA)에 신고된 침해사고 건수는 2025년 기준 2,383건으로 연평균 36.6% 증가하는 등 지속적으로 증가하고 있는 추세임
    - 글로벌 사이버 보험시장은 2024년 기준 약 153억 달러 규모로 성장했으나, 국내는 사이버 관련 보험을 모두 포함해도 약 0.4억 달러로 매우 낮은 수준임
  - (국내 사이버 보험시장 성장 부진 원인) 국내 사이버 보험시장은 사이버 리스크를 보험으로 관리할 경영과제로 인지하지 못한 수요 측 한계와 고난이도 리스크를 완화하기 어려운 보험회사의 보수적 보험 공급, 그리고 이를 보완할 제도적 연결의 미흡으로 인해 성장동력이 막혀 있는 상황임
    - 사이버 리스크는 사고 확률 및 손해 추정이 어려울 뿐만 아니라 동시다발적으로 연계되어 발생되고 빠르게 진화하며 사고 후 평판 비용까지 포함된 복합 리스크임
    - 이러한 사이버 리스크의 특징은 소비자의 위험 인지를 저해하고, 보험의 필요성에 대한 인식 부족, 또는 인식 이후에도 가입과 활용 회피로 이어질 가능성을 높임
    - 사이버 리스크의 복합성은 부보가능성을 구조적으로 낮춰 사이버 보험 상품의 요율 상승, 인수 한도 축소, 면책 및 조건부 보장 확대, 심사 강화로 이어지며, 결과적으로 시장 내 사이버 보험의 침투율과 체감가치를 떨어뜨리는 요인으로 작용함
    - 소비자의 낮은 위험 및 보험 인식을 제고하기 위한 제도적 인센티브가 충분히 마련되어 있지 않으며, 표준화와 위험 관련 데이터 인프라의 부족도 보험회사의 불확실성 완화를 제약하는 요인으로 작용하고 있음
  - (낮은 성장 극복을 위한 방안) 기업의 낮은 리스크 인식을 제고하기 위해 행동 유인 모델을 도입하고, 표준화와 위험 데이터 인프라를 구축하는 한편, 소비자가

## 보험의 가치를 체감할 수 있도록 상품 설계와 서비스 제공 방식을 개선할 필요가 있음

- 기업의 자발적 리스크 인지를 위해 단순한 교육 제공이 아닌 행동의 변화를 이끌어낼 수 있는 경량형 인증제도와 보험을 결합한 모델을 도입해 볼 필요가 있음
- 사이버 리스크의 부보가능성을 높이기 위해 사고 분류·손해·청구 데이터를 표준화하여 언더라이팅에 활용할 수 있는 기반을 마련하고, 기업의 통제 수준·사고 이력·보험 가입여부 등을 종합 분석할 수 있는 데이터 인프라를 구축할 필요가 있음
- 가입자에게 단순 피해 보상을 넘어 체감 가능한 가치를 제공할 수 있도록, 보안인식 교육 등 예방 서비스나 실제 사고 발생 시 법률·포렌식·통지 등 대응 서비스를 연결하여 기업의 사이버 대응 역량을 높이는 서비스를 제공할 필요가 있음

○ (주제발표 6) 최용민 부대표 (프로시스 언더라이팅 솔루션즈)는 ‘한국 사이버 보험 생태계 구축을 위한 실천적 로드맵’이라는 주제로 정부의 강력한 주도하에 시장 내 각 역할 주체가 함께하는 사이버 보험 생태계 구축과 관련한 로드맵 추진을 제안함

- 한국의 사이버 보험시장은 수요자의 무관심, 공급자의 리스크 평가/ 인수역량 부족, 인프라 미비라는 ‘악순환의 고리’에 빠져 성장이 정체되어 있음. 반면 미국·일본·호주 등 글로벌 시장은 규제 강화라는 정부 정책의 주도하에 기술 기반의 ‘능동형 (Active)’ 보험 도입과 같은 민영 주체의 다양한 노력이 함께해 사이버 복원력 (Cyber Resilience)을 강화하는 추세임
- 국내 사이버 보험시장에서 과거 10년간의 과제가 2026년 오늘날까지 반복되고 있는 이 현실이야말로 우리 시장이 처한 가장 큰 리스크임. 이제는 ‘무엇을 해야 하는가 (What to do)’가 아니라, ‘어떻게 실행할 것인가(How to execute)’로 우리의 패러다임을 전환해야 할 시점임
- 사이버 보험시장의 활성화는 어느 한 주체의 노력만으로는 불가능함. 정부의 제도적 마중물, 감독당국의 투명한 데이터 공유, 보험회사의 고객 중심의 혁신성 있는 서비스 통합, 그리고 기업의 인식 전환이라는 네 개의 톱니바퀴가 동시에 맞물려 돌아가야 가능하다고 봄
- 정부 주도하에 각 역할 주체가 함께 하는 로드맵 추진을 제안함. 본 로드맵 추진을 통해 디지털 전환 시대의 ‘데이터 리더십 확보’, ‘표준화 모델 수립’, ‘의무보험 확대’를 축으로, 단순한 손해 보상을 넘어 사고 예방과 복구 지원이 결합된 실천적 사이버 보험 생태계를 조성하는 것을 목표로 함

• 본 자료를 인용하여 보도할 경우에는 출처(<http://www.kiri.or.kr>)를 표기하여 주시기 바랍니다