보험금융연구 제37권 제2호(2026. 5) pp. 49-82
DOI: https://doi.org/10.23842/jif.2026.37.2.002

미국의 사이버위험 보험 판례 법리의 간접 규제 모델*

The Indirect Regulatory Model of U.S. Cyber Risk Insurance Case Law

최 자 유**
Choi Ja Yoo

Ward General 사건·America Online 사건에서 법원은 전자 데이터 손실·소프트웨어 오류를 재산보험·상업종합책임보험의 직접적인 물리적 손해와 유형 재산의 재산 손해에서 제외하였다. Ingram Micro 사건·National Ink 사건에서 법원은 기능 손해 개념을 인정하였지만, EMOI Services 사건에서 법원이 물리적 파괴·변형을 요구하여 논란이 지속 중이다. Merck 사건에서 법원은 전쟁 면책조항을 사이버공격에 적용할 수 없다고 판시하였다. Travelers 사건에서 법원은 보험 계약자의 보안 관리체계에 대한 중대 허위·누락 진술을 이유로 보험 계약을 소급 무효화하는 화해 계약을 승인하였다.

우리나라도 ① 기능 손해 개념을 도입하고, ② 사이버공격의 정치·군사적 성격과 보험자의 책임을 분리하며, ③ 보험 판례 법리로 기업의 보안 투자를 유도하고, ④ 단계적 접근 방식을 논의하는 등 사이버위험 보험 법제 정비가 필요하다.

국문 색인어: 사이버위험, 재산보험, 상업종합책임보험, 직접적인 물리적 손해, 유형 재산, 재산 손해, 기능 손해, 전쟁 면책조항, 랜섬웨어, 언더라이팅, 간접 규제
한국연구재단 분류 연구분야 코드: B130320

* 본 연구 내용은 저자의 개인 의견으로 소속 기관의 공식 견해가 아님을 밝힙니다.
** 금융감독원 선임검사역, 변호사·법학전문박사(jy_choi@yonsei.ac.kr)
논문 투고일: 2026.02.23, 논문 최종 수정일: 2026.05.07, 논문 게재 확정일: 2026.05.15

Ⅰ. 서론

미국에서는 재산보험(commercial property insurance)·상업종합책임보험(commercial general liability insurance)('재산보험 등') 판례 법리로 기업 영업·조직 운영, 공급망, 국가 경제·안보의 사이버위험을 간접 규제한다. 재산보험의 직접적인 물리적 손해(direct physical loss or damage)와 상업종합책임보험의 유형 재산(tangible property)의 재산 손해(property damage) 등에 대한 사이버위험 보험 판례 법리가 보험자에게 언더라이팅 과정의 위험 평가·보험료 산정·담보 범위 결정·보안 심사 지침을 제공하여 약관 설계·언더라이팅 기준·위험 배분 구조의 변화 등을 촉진[1]할 수 있다.

미국에서는 1990년대 후반 개발된 사이버보험[2]보다 재산보험 등 전통적인 보험상품으로 사이버사고에 대응[3]하는 경향이 발견된다. 우리나라에서는 사이버보험에 대한 인식 미비[4]로 2023년 기준 가입률이 7.4%에 불과[5]하여 재산보험 등으로 사이버사고에 대응[6]하는 경향이 미국과 동일하다. 미국의 사이버위험 보험 판례 법리의 간접 규제 모델은 우리나라의 사이버보험 정착 과정[7]에 시사점을 제공한다. 본 연구는 미국의 사이버위험 보험 판례 법리의 간접 규제 모델을 규명한다. Ⅱ장에서 미국의 사이버보안 법체계를 검토한다. Ⅲ장에서 사이버사고 손해 개념을 분석하고, Ⅳ장에서 사이버공격의 책임 귀속과 면책을 고찰한다. Ⅴ장에서 사이버위험 보험 판례 법리와 보험 실무를 탐구한다. Ⅵ장에서 우리나라의 사이버위험 보험 법제에 대한 시사점을 제언한다.

---

1) Aggeliki Tsohou et al., "Cyber insurance: State of the art, trends and future directions", 『International Journal of Information Security』, Vol. 22(3), 2023, p. 744.
2) 황정혜, "사이버공격 증가에 따른 사이버보험의 동향 및 법제에 관한 연구", 『법이론실무연구』, 제13권 2호, 2025, 452면.
3) 김원각, "사이버 위험에 대한 미국 보험사업자의 대응에 관한 연구", 『경제법연구』, 제21권 3호, 2022, 246면.
4) 신계하·손승우, "사이버보험 활용의 순기능과 역기능에 관한 연구", 『한국산업보안연구』, 제12권 3호, 2022, 176면.
5) 장영진, "사이버 보험 활성화를 위한 제언", 『이슈와 논점』, 제2392호, 2025.7.30.(국회입법조사처).
6) 황정혜, 앞의 논문, 451면.
7) 최근 사이버보험 제도화를 위해 사이버재해보험법안(박정훈 의원 대표발의, 의안번호 2215050, 2025.12.9., '박정훈 의원(안)')이 발의되었다.

II. 미국의 사이버보안 법체계

1. 보험 판례 법리의 간접 규제

가. 사이버보안 영역의 통일적 규범 부재

미국에서는 개인정보 보호[8]·통신 보안[9]·기반시설 보호[10] 등 개별적 규범 이외에 기업 영업·조직 운영, 공급망, 국가 경제·안보의 사이버위험을 규율하는 통일적 규범이 부재[11]하여 보험 판례 법리로 간접 규제[12]한다. 재산보험 등 개별 분쟁 사건에서 법원은 직접적인 물리적 손해·유형 재산의 재산 손해·전쟁 면책조항·국가 연계 의혹 등을 사이버 환경에 부합하게 해석하여 보험 판례 법리를 형성한다. 사이버보안은 통일적 규범이 아니라 개별 분쟁 사건에서 보험 판례 법리로 규율되는 위험 영역인 것이다.

나. 사이버위험 보험의 담보 범위 해석

기업 영업·조직 운영에 중대한 영향이 우려되는 신유형의 위험인 사이버사고 손해의 직접적인 물리적 손해 등을 전통적인 보험상품으로 특정하기에 한계가 있다. 1930년대 해상적하보험, 1940년대 내륙해상보험의 포괄위험(all-risk) 약관에서 무형 손해를 제외하는 취지로 재산보험의 직접적인 물리적 손해 요건이 도입[13]된 것으로 추정된다. 이는 신유형

8) 의료·건강정보 보호에 대한 건강보험 이동성 및 책임에 관한 법률(Health Insurance Portability and Accountability Act of 1996)·금융기관의 고객 금융정보 보호에 대한 금융서비스 현대화법(Gramm-Leach-Bliley Act of 1999)·13세 미만 아동의 온라인 개인정보 보호에 대한 아동 온라인 프라이버시 보호법(Children's Online Privacy Protection Act of 1998) 등.

9) 통신업자의 수사 협조의무에 대한 법 집행을 위한 통신지원법(Communications Assistance for Law Enforcement Act of 1994) 등.

10) 중요 기반시설의 사이버사고 보고에 대한 중요 기반시설 사이버사고 보고법(Cyber Incident Reporting for Critical Infrastructure Act of 2022) 등.

11) Jeff Kosseff, "Defining Cybersecurity Law", 『Iowa Law Review』, Vol. 103, 2018, p. 988.

12) Jeff Kosseff, "Upgrading Cybersecurity Law", 『Houston Law Review』, Vol. 61, 2023, p. 51.

13) Scott G. Johnson, "What Constitutes Physical Loss or Damage in a Property Insurance Policy?", 『Tort Trial & Insurance Practice Law Journal』, Vol. 54(1), 2019, p. 99.

의 위험인 사이버사고 손해를 재산보험의 담보 범위에서 제외하려는 의도로 해석할 수 없다. 사이버사고 손해가 재산보험의 직접적인 물리적 손해[14]·상업종합책임보험의 유형 재산의 재산 손해[15] 요건을 충족하는지 검토하여 담보 범위를 해석하여야 한다.

다. 보험 판례 법리의 규범 형성

사이버위험 보험 판례 법리는 성문법과 상이하게 사전에 공표된 규범이 아니라 개별 분쟁 사건에서 법원이 기존 법체계로 신유형의 위험인 사이버사고를 해석하여 도출한다. 개별 분쟁 사건의 보험 판례 법리가 보험시장에 확산되면 사실상의 규범으로 기능할 수 있다. 보험자는 보험 판례 법리를 기준으로 약관 설계·언더라이팅 기준·위험 배분 구조를 개선하여 모호성을 완화할 수 있지만, 변경될 수 있는 보험 판례 법리의 명확성·예측 가능성 등 규범으로서 한계도 명확하다.

2. 주(州) 보험법과 연방 규율의 결합

가. 맥캐런-퍼거슨법과 보험규제

미국에서 보험업은 주(州)의 규제 대상으로 1945년 제정 맥캐런-퍼거슨법(McCarran-Ferguson Act)으로 제도화[16]되었다. 맥캐런-퍼거슨법은 보험규제와 과세가 공익에 부합하고 연방의 침묵이 주(州)의 보험규제 권한 제한으로 해석될 수 없다는 입법 취지를 명시한다. 사이버사고 손해는 주(州) 보험 감독당국과 주(州) 법원의 해석 영역으로 사이버위험 보험 판례 법리는 연방의 통일적 규범이 아니라 주(州)의 약관 해석·시장 관행을 통해 발전하였다. 사이버사고 손해의 담보 범위는 주(州) 보험법과 보험 계약의 해석 영역이다.

---

14) 전통적으로 재산보험 약관은 'We will pay for direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss'로 규정하여 물리적 손해를 요구하였다.

15) 전통적으로 상업종합책임보험 약관은 '"Property damage" means: (a) Physical injury to tangible property, including all resulting loss of use; or (b) Loss of use of tangible property that is not physically injured'로 규정하여 유형 재산의 물리적 손상·사용 불능 상태를 요구하였다.

16) Daniel A. Lyons, "States and Systemic Risk: An Analysis of the Dodd-Frank Act's (Un)Cooperative Federalism", 『Nevada Law Journal』, Vol. 22, 2021, p. 317.

나. NAIC 모델 규범의 실질적 규범력

보험규제의 분절화에 대응하여 전국보험감독관협의회(National Association of Insurance Commissioners, 'NAIC') 등 주(州) 보험 감독당국의 조정 수단이 존재한다. NAIC는 보험자의 사이버위험 관리·정보 보안·내부통제에 대한 모델 규범(NAIC Insurance Data Security Model Law)[17]으로 주(州) 보험규제의 기준점을 제시하고 각 주(州)가 모델 규범을 보완·발전적으로 수용하여 실질적 규범력을 확보한다. 위험 평가·보험료 산정·담보 범위 결정·보안 심사는 주(州)별 상이한 형식에도 공통 요소를 공유한다. 이는 보험시장에 규범적 일관성을 부여하고 약관 해석·시장 관행으로 사이버위험을 간접 규제하는 경로를 강화한다.

다. NYDFS 사이버보안 규정의 선도적 역할

뉴욕은 사이버보안 관련 선도적인 규제 모델을 제시하였다. 2017년 뉴욕 금융서비스국(New York Department of Financial Services, 'NYDFS')은 금융기관의 보안 관리체계 등을 규정하는 사이버보안 규정(Cybersecurity Regulation)을 도입[18]하였고 2023년 거버넌스·보고·기술 통제·제재체계를 개선[19]하였다. 사이버보안 규정은 뉴욕 금융기관에 적용되므로 사이버위험 관리는 단순 내부 정책이 아니라 규제 준수의 대상이다. 뉴욕 금융기관 이외의 다수 보험자가 사이버보안 규정을 기준으로 보안 관리체계를 개선하고 타 주(州) 사업에 적용하여 규제 효과가 확산[20]되었다. 이는 주(州)의 보험규제가 보험시장을 통해 전국적 기준으로 전환되는 사례로 해석할 수 있다.

---

17) 보험자에 대한 운영·데이터 보호규제로 사이버보험 판매 시 보안 관리체계 개선을 유도하지만, 담보 범위·직접적인 물리적 손해 등은 별도 문제이다.

18) Andrew M. Cuomo, Governor of New York, "Governor Cuomo Announces First-In-The-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1", Press Release, 2017.2.16.

19) NYDFS, "DFS Announces Second Amendment to Nation-Leading Cybersecurity Regulation", Press Release, 2023.11.1.

20) Debevoise & Plimpton LLP, "Cybersecurity Requirements for Insurance Companies - The NYDFS Rules as the Emerging Standard", Debevoise Data Blog, 2020.8.19.

라. 연방 감독당국의 간접 개입

연방 감독당국의 조사·가이드라인·정책적 발언은 보험자의 약관 설계·언더라이팅 기준·위험 배분 구조의 참고 기준이다. 연방이 주(州)의 보험규제 권한을 존중하면서 사이버위험에 대한 문제의식을 시장에 전달한다. 사이버위험 보험 판례 법리는 주(州) 보험법을 중심으로 연방 차원의 정책 환경과 결합된 복합적 구조에서 발전하였다.

3. 사이버사고와 사이버위험 보험의 위험 이전

가. 전통적인 재산보험 등과 사이버사고

데이터 접근 불능·시스템 마비·네트워크 차단 등은 유형 재산의 물리적 파괴·변형이 없이도 기업 영업·조직 운영에 중대한 영향이 우려된다. 전자 데이터 손실·소프트웨어 오류 등 사이버사고 손해는 재산보험 등의 담보 범위에 포함하기에 구조적 한계[21]가 존재하여 유형 재산의 물리적 파괴·변형이 없다면 담보 범위에서 제외되는 사례가 발생하였다. 사이버사고 손해의 특수성은 사이버사고를 전통적인 재산 손해의 부수적 문제로 취급하기보다 신유형의 위험으로 규율할 필요성을 제기[22]하였다.

나. 사이버위험 보험의 위험 이전

사이버위험 보험은 손해 항목을 약관으로 특정하고 보상하여 기업의 사이버위험을 완화한다. 기업은 보험료를 납입하고 데이터 복구·시스템 복원·외부 전문업체 대응·영업 중단 손해 등 사이버사고 손해를 보험자에게 이전[23]하는 것이다. 발생 시점, 공격 방식, 손해 빈도·규모를 사전 예측하기 곤란[24]한 사이버사고에서 사이버위험 이전을 통해 기업의 치

21) Amy R. Willis, “Business Insurance: First-Party Commercial Property Insurance and the Physical Damage Requirement in a Computer-Dominated World”, 『Florida State University Law Review』, Vol. 37(4), 2010, p. 1004.
22) Tom Baker·Kyle D. Logue, “Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment”, 『Minnesota Law Review』, Vol. 102, 2017, p. 276.
23) Aggeliki Tsohou et al., op. cit., p. 737.
24) 권순일·한진현, “사이버 리스크 실태와 과제”, 『이슈 분석』, 2025.5.26.(보험연구원), 18면.

명적인 재무적 위험을 방지할 수 있다. 보험자는 사이버위험의 성격과 손해를 고려하여 언더라이팅을 진행하고 보험 계약자의 보안 관리체계를 평가한다. 사이버위험 보험 계약은 위험 이전의 결과이고 위험을 사전 평가·분류하는 절차를 포함[25]한다.

다. 보안 유인 장치로서의 사이버위험 보험 판례 법리

보험자는 기업의 보안 관리체계가 취약하다고 판단되면 보험료 인상·담보 범위 축소·인수 거절을 선택하여 기업이 사이버위험을 식별하고 보안 관리체계를 개선[26]하도록 유도한다. 보험자에게 언더라이팅 과정의 위험 평가·보험료 산정·담보 범위 결정·보안 심사 지침을 제공하는 사이버위험 보험 판례 법리는 약관 설계·언더라이팅 기준·위험 배분 구조의 변화 등을 촉진하여 행위 기준을 형성한다. 사이버공격의 빈도·규모가 증가하며 언더라이팅 과정에서 보험자가 요구하는 보안 관리체계는 구체·정형화[27]되는 경향이다. 사이버사고 손해는 재산보험 등 전통적인 보험 판례 법리로 규율되어 재산보험 등의 담보 범위에 포함되기도 한다. 사이버보험에 대한 인식이 미비한 우리나라의 사이버보험 정착 과정에서 미국의 사이버위험 보험 판례 법리[28][29]를 참고할 필요가 있다.

---

25) Aggeliki Tsohou et al., op. cit., p. 744.

26) Gareth Mott et al., "Between a rock and a hard(ening) place: Cyber insurance in the ransomware era", 『Computers & Security』, Vol. 128, 2023, p. 7.

27) Burns & Wilcox, "Cyber Insurance Outlook: Emerging Risks, Underwriting Trends, and Strategic Insights", 2025.9.25.

28) 사이버위험 보험은 ① 재산보험 등이 사이버위험을 담보 범위에 규정하지 아니하여 분쟁이 발생하는 형태인 침묵 사이버보험(silent cyber insurance), ② 재산보험 등에 사이버위험을 부가하는 형태인 사이버부가특약(cyber endorsement), ③ 사이버위험에 대한 특화적 보험인 사이버단독보험(standalone cyber insurance)으로 분류할 수 있다. 사이버위험 보험 판례 법리는 침묵 사이버보험을 중심으로 형성되었다.

29) Ward General Insurance Services, Inc. v. Employers Fire Insurance Co., 114 Cal. App. 4th 548 (Cal. Ct. App. 2003)('Ward General 사건'), America Online, Inc. v. St. Paul Mercury Insurance Co., 347 F.3d 89 (4th Cir. 2003)('America Online 사건'), American Guarantee and Liability Insurance Co. v. Ingram Micro, Inc., 2000 WL 726789 (D. Ariz. 2000)('Ingram Micro 사건'), National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Co., 435 F. Supp. 3d 679 (D. Md. 2020)('National Ink 사건'), EMOI Services, LLC v. Owners Insurance Co., 170 Ohio St. 3d 78, 2022-Ohio-4649 (Ohio 2022)('EMOI Services 사건'), Merck & Co., Inc. v. ACE American Insurance Co., No. A-1879-21 (N.J. Super. Ct. App. Div. 2023)('Merck 사건'), Travelers Property Casualty Co. of America v. International Control Services, Inc., No.

라. 간접 규제의 구조와 기능

개별 분쟁 사건의 보험 판례 법리는 사건 당사자(기판력의 주관적 범위), 주문에 포함된 내용(기판력의 객관적 범위) 이외에 타 분쟁 사건에 법적 효력이 없다. 그러나 재판 과정에서 당해 법원이 과거 타 법원이 제시한 보험 판례 법리에 위반되는 보험자의 영업행위를 위법하다고 판단할 수 있다. 이를 보험 판례 법리가 보험자에게 언더라이팅 과정의 위험 평가·보험료 산정·담보 범위 결정·보안 심사 지침을 제공하여 약관 설계·언더라이팅 기준·위험 배분 구조의 변화 등을 촉진하는 간접 규제로 정의할 수 있다.

공적 규제가 미비하고, 보험자의 위험 평가 역량[30]이 인정되며, 담보 범위·보험료 차등에 대한 보험 계약자의 행태 반응성[31]이 발견되고, 보험 판례 법리의 확산 경로[32]가 존재하면 간접 규제가 효율적으로 기능할 수 있다. 보험자와 보험 계약자의 정보 비대칭으로 보험 계약의 불공정성도 우려되므로 보험시장의 자율 규제를 무제한 인정할 수는 없다. 간접 규제는 감독당국의 공적 규제와 결합되어야 정당성을 제고할 수 있다.

2:22-cv-02145 (C.D. Ill. 2022)('Travelers 사건'), Mondelez International, Inc. v. Zurich American Insurance Co., No. 2018L011008 (Ill. Cir. Ct. 2018)('Mondelez 사건').

30) Omri Ben-Shahar·Kyle D. Logue, "Outsourcing Regulation: How Insurance Reduces Moral Hazard", 『Michigan Law Review』, Vol. 111, 2012, pp 205-206.

31) Ibid, p. 207.

32) Ibid, p. 234.

Ⅲ. 사이버사고 손해 개념

1. 직접적인 물리적 손해 개념과 전통적인 보험 판례 법리

가. 직접적인 물리적 손해 개념과 전자 데이터·소프트웨어의 성질

Ward General 사건[33][34]에서 법원[35]은 전자 데이터 손실·소프트웨어 오류가 무형 손해를 초래할 수 있으나, 물리적 매체·장비의 파괴·변형이 없다면 재산보험의 담보 범위인 직접적인 물리적 손해로 해석할 수 없다고 판시하였다. 직접적인 물리적 손해를 외형적으로 인식 가능한 물리적 파괴·변형으로 제한 해석한 것이다.

America Online 사건[36]에서 법원은 유형 재산이 아니라 정보인 전자 데이터·소프트웨어의 기능 상실 상태는 상업종합책임보험의 재산 손해로 해석할 수 없다고 판시하였다. 상업종합책임보험의 담보 범위인 유형 재산의 재산 손해를 외형적으로 인식 가능한 물리적 파괴·변형으로 제한 해석하여 사이버사고의 기업 영업·조직 운영에 대한 실질적 타격보다 유형 재산의 물리적 파괴·변형으로 환원될 수 있는지에 주목한 것이다.

나. 전자 데이터 손실·소프트웨어 오류의 담보 범위 제외

Ward General 사건·America Online 사건에서 법원은 무형 손해인 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에서 제외하였다. 이는 재산보험 등을 통한 사이버사고 손해 보상의 한계로 보험 실무에서 사이버사고 손해를 전통적인 재산 손해와

33) 2000년대 초반 사이버경제의 태동으로 분쟁이 급증하는 시기의 초기 판례이다.
34) 전자 데이터 손실·소프트웨어 오류로 복구 비용·영업 중단 손해가 발생한 사안에서 전자 데이터 손실·소프트웨어 오류가 재산보험의 직접적인 물리적 손해에 해당하는지가 쟁점이다. 캘리포니아 항소법원은 물리적 매체의 파괴·변형이 없다면 전자 데이터 손실·소프트웨어 오류를 직접적인 물리적 손해로 해석할 수 없다고 판단하였다. 직접적인 물리적 손해가 전제인 복구 비용·영업 중단 손해 등 부수적 손해도 담보 범위에서 제외된다.
35) 사건을 최초 언급 시 법원을 특정하고, 이후 언급 시 법원으로 기술한다.
36) America Online, Inc.가 배포한 소프트웨어 오류로 전산 시스템이 오작동하여 복구 비용이 발생한 사안에서 소프트웨어가 상업종합책임보험의 유형 재산에 해당하는지가 쟁점이다. 제4연방항소법원은 소프트웨어를 유형 재산이 아니라 정보로 해석하여 담보 범위에서 제외하였다. 소프트웨어 오류가 전제인 복구 비용·영업 중단 손해 등 부수적 손해도 담보 범위에서 제외된다.

구별하는 경향을 강화하였다. 기업 영업·조직 운영에 중대한 영향이 우려되는 사이버사고는 재산보험 등의 약관 해석이 아니라 입법을 통한 손해 개념 규정·사이버위험에 대한 특화적 보험 설계로 대응하여야 한다.

2. 기능 손해 개념

가. 시스템의 핵심 기능 상실 상태

Ward General 사건·America Online 사건 이전 Ingram Micro 사건[37]에서 법원은 재산보험의 직접적인 물리적 손해로 사이버사고 손해를 해석하기 어렵다는 문제의식에 기반하여 기능 손해 개념을 제시하였다. 법원은 사이버 환경에서 직접적인 물리적 손해를 전산 장치의 물리적 파괴·변형에 제한하지 아니하고 접근 상실·사용 상실·기능 상실(loss of access, loss of use, and loss of functionality) 등 시스템의 핵심 기능 상실 상태를 포함[38]하였다. 재산의 실질적 가치 상실을 의미하는 시스템의 핵심 기능 상실 상태를 재산보험의 직접적인 물리적 손해로 해석할 가능성을 제기한 것이다.

나. 기능 손해 판단 기준

Ingram Micro 사건에서 법원은 시스템의 핵심 기능 상실 상태[39]는 재산의 효용 상실로 해석할 수 있다는 기능 손해 개념을 제시하였다. 기업 영업·조직 운영에 중대한 영향이 우려되는 컴퓨터 시스템의 작동 불능 상태는 유형 재산의 재산 손해인 시스템의 핵심 기능

37) 전산 시스템의 8시간 작동 불능 상태로 발생한 전자 데이터 손실·소프트웨어 오류가 재산보험의 직접적인 물리적 손해에 해당하는지가 쟁점이다. 애리조나 연방지방법원은 물리적 설비가 외형적으로 파괴·변형되지 아니하여도 컴퓨터 시스템의 핵심 기능 상실 상태를 재산의 실질적 가치 상실 상태로 해석할 수 있다고 판단하였다.

38) At a time when computer technology dominates our professional as well as personal lives, the Court must side with Ingram's broader definition of "physical damage". The Court finds that "physical damage" is not restricted to the physical destruction or harm of computer circuitry, but includes loss of access, loss of use and loss of functionality.

39) 8시간 작동 불능 상태는 시스템의 핵심 기능 상실 상태이지만, 전면·영구적 기능 상실 상태는 아니다. National Ink 사건에서 법원은 'Case law cited by State Auto does not suggest that, for damage to be covered, a computer system must be completely and permanently inoperable'이라고 판시하였다.

상실 상태로 해석할 수 있다. 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에서 제외하는 기존 보험 판례 법리와 상이하게 유형 재산의 기능을 손해 판단 기준으로 규정한 것이다.

다. 기능 손해 개념과 약관 정비

Ingram Micro 사건에서 법원은 물리적 파괴·변형이 없는 시스템의 핵심 기능 상실 상태를 기능 손해로 해석하였다. Ward General 사건·America Online 사건에서 법원은 Ingram Micro 사건의 보험 판례 법리를 배척[40]하고 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에서 제외하였다. 보험 판례 법리의 분화는 침묵 사이버보험으로 발생하는 분쟁을 명시적 약관으로 해소하려는 경향을 강화하였다. 보험자는 전자 데이터 손실·소프트웨어 오류 등 사이버사고 손해를 담보 범위에서 제외하는 문구를 약관에 도입[41]하여 모호성을 해소한 것이다. 보험 판례 법리가 보험자의 약관 설계·언더라이팅 기준·위험 배분 구조의 변화 등을 촉진하는 간접 규제 모델의 사례로 해석할 수 있다.

3. 랜섬웨어와 손해 개념의 확장

가. 랜섬웨어의 법적 성격

National Ink 사건[42]에서 법원은 랜섬웨어 손해를 재산보험의 직접적인 물리적 손해로 해석할 수 있다고 판시하였다. 랜섬웨어는 물리적 파괴·변형은 없지만, 암호화로 인한 시스템의 핵심 기능 상실 상태를 초래하여 기업 영업·조직 운영의 불능 상태가 발생하였다. 기능 손해 개념을 부정하는 전통적인 손해 개념으로는 랜섬웨어를 해석할 수 없다.

40) Amy R. Willis, op. cit., p. 1013.
41) Ibid, p. 1012.
42) 랜섬웨어로 National Ink and Stitch, LLC의 전자 데이터·소프트웨어가 암호화되었다. 시스템의 핵심 기능 상실 상태가 재산보험의 직접적인 물리적 손해에 해당하는지가 쟁점이다. 메릴랜드 연방지방법원은 하드웨어의 물리적 파괴·변형이 없이도 시스템의 핵심 기능 상실 상태로 재산의 실질적 효용이 상실되면 직접적인 물리적 손해로 해석할 수 있다고 판단하였다. 랜섬웨어로 인한 시스템의 핵심 기능 상실 상태는 재산보험의 담보 범위에 포함된다.

나. 암호화로 인한 시스템의 핵심 기능 상실 상태

National Ink 사건에서 법원은 전자 데이터·소프트웨어의 물리적 파괴·변형이 없이도 암호화로 인한 기업 영업·조직 운영에 필수적인 시스템의 핵심 기능 상실 상태를 기능 손해로 해석하였다. 기능 손해 개념을 신유형의 위험인 랜섬웨어에 적용하여 직접적인 물리적 손해를 확장 해석한 것이다. 법원은 전자 데이터·소프트웨어의 비물리성을 이유로 손해를 부정하는 Ward General 사건·America Online 사건의 보험 판례 법리를 적용하는 것은 부적절하다고 판단하였다.

다. Ingram Micro 사건의 보험 판례 법리와의 연속성

National Ink 사건에서 법원은 물리적 파괴·변형이 없는 시스템의 핵심 기능 상실 상태에 Ingram Micro 사건의 기능 손해 개념을 수용하였다. 신유형의 위험인 랜섬웨어에 기능 손해 개념을 적용하여 재산보험의 직접적인 물리적 손해에 상대적으로 유연한 해석을 제시한 것이다. 랜섬웨어로 시스템의 핵심 기능 상실 상태가 발생하면 기능 손해 법리가 판단 기준으로 작동할 수 있다. National Ink 사건에서 법원은 기능 손해 개념을 수용하여 사이버사고 손해를 재산보험의 직접적인 물리적 손해로 해석하였다.

4. 기능 손해로의 개념 전환

가. 손해 판단 기준 전환의 경로

Ingram Micro 사건에서 법원은 시스템의 핵심 기능 상실 상태를 직접적인 물리적 손해로 해석할 수 있다는 문제의식으로 손해 개념의 물리적 파괴·변형 제한에 대한 의문을 제기하였다. 이는 손해 개념을 기능적 관점에서 구성하려는 시도[43]로 해석되지만, 2010년대 중반 이전에는 예외적 보험 판례 법리이다. Ward General 사건에서 법원은 재산보험의 직접적인 물리적 손해를 유형 재산의 물리적 파괴·변형으로 제한 해석하였다.

43) Deborah L. Johnson, "Demystifying the Elusive Quest for Cyber Insurance Protection: The Need for New Contract Language", 『Cardozo Law Review』, Vol. 44(6), 2023, p. 2379.

America Online 사건에서 법원은 전자 데이터 손실·소프트웨어 오류를 상업종합책임보험의 유형 재산의 재산 손해가 아니라고 해석하여 담보 범위에서 제외하였다. 기존 재산보험 등으로 사이버사고 손해를 해석하는 과정에서 사이버위험의 특수성을 소극적으로 고려하는 접근 방식이다. National Ink 사건에서 법원은 암호화로 인한 시스템의 핵심 기능 상실 상태에 기능 손해 개념을 적용[44]하였다.

나. 담보 범위에 대한 보험 판례 법리의 영향

National Ink 사건에서 법원이 기능 손해 개념을 제시하여 보험자는 물리적 파괴·변형이 없는 사이버사고 손해를 담보 범위에서 제외하기 어려운 상황에 직면하였다. 사이버사고 손해의 특수성을 고려하여 재산보험 등이 예정하지 아니한 신유형의 위험이 보험 판례 법리를 통해 형성되는 사례이다. 담보 범위는 약관 문언의 형식적 해석이 아니라 기업 영업·조직 운영에 대한 실질적 영향을 고려하는 방향으로 조정되었다.

다. 사이버위험 보험 판례 법리와 기업의 인식 전환

사이버위험 보험 판례 법리는 기업의 보안 관리체계에 대한 인식을 전환하였다. 초기 분쟁 사건에서 사이버사고 손해가 담보 범위에서 제외될 수 있기에 기업은 사이버사고의 재무적 위험을 자체 부담하여야 한다. 기능 손해 개념을 통해 랜섬웨어 손해를 담보 범위에 포함하는 보험 판례 법리의 영향으로 사이버사고의 담보 범위에 대한 해석이 변화되었다. 이는 기업이 보안 관리체계를 개선할 필요성을 인식하는 요인으로 기능하였다. Ward General 사건의 직접적인 물리적 손해와 America Online 사건의 유형 재산의 재산 손해로 사이버사고를 해석할 수 없지만, National Ink 사건의 기능 손해 개념으로 사이버위험 보험 판례 법리가 발전하였다.

44) Ibid, p. 2384.

라. 기능 손해 개념에 대한 논란

코로나-19로 인한 기업휴지보험(business interruption insurance) 판례 법리는 바이러스·정부의 봉쇄 명령으로 인한 직접적인 물리적 손해를 특정할 수 없다는 이유로 영업 중단·사용 불능 상태를 재산보험의 담보 범위에서 제외[45]하였다. 기업휴지보험 판례 법리의 영향으로 EMOI Services 사건[46]에서 법원은 전자 데이터·소프트웨어의 직접적인 물리적 손해를 물리적 파괴·변형으로 제한 해석하였다. 2026년 5월 현재 다수 법원이 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에서 제외하여 EMOI Services 사건의 보험 판례 법리와 유사하게 해석[47][48]한다. 보험 판례 법리의 분화로 기업 영업·조직 운영에 중대한 영향이 우려되는 랜섬웨어 등 사이버사고를 담보 범위에 포함할지에 대한 논란이 지속[49] 중이다.

45) Natalie E. deLatour, "Insuring the "Uninsurable": Business Interruption Insurance Coverage & COVID-19", 『Georgia State University Law Review』, Vol. 37, 2021, p. 17.

46) 랜섬웨어로 EMOI Services, LLC의 전자 데이터·소프트웨어가 암호화된 사안에서 시스템의 핵심 기능 상실 상태가 재산보험의 직접적인 물리적 손해에 해당하는지가 쟁점이다. 오하이오 대법원은 하드웨어의 물리적 파괴·변형이 없는 전자 데이터 손실·소프트웨어 오류는 직접적인 물리적 손해로 해석할 수 없다고 판단하였다. 랜섬웨어로 인한 시스템의 핵심 기능 상실 상태는 재산보험의 담보 범위에서 제외된다.

47) Site Jab v. Hiscox Insurance Co., No. 4:23-cv-03853 (S.D. Tex. 2024). Site Jab, LLC 직원의 절도로 발생한 고객 정보·웹사이트의 전자 데이터 손실이 재산보험의 직접적인 물리적 손해에 해당하는지가 쟁점이다. 텍사스 남부지방법원은 하드웨어의 물리적 파괴·변형이 없는 고객 정보·웹사이트의 전자 데이터 손실을 직접적인 물리적 손해로 해석할 수 없다고 판단하였다. 고객 정보·웹사이트의 전자 데이터 손실은 재산보험의 담보 범위에서 제외된다.

48) Home Depot, Inc. v. Steadfast Insurance Co., No. 23-3720 (6th Cir. 2025). Home Depot, Inc. 고객의 결제 카드의 전자 데이터가 유출된 사안에서 금융기관의 카드 재발급 비용·사용 감소 손실이 상업종합책임보험의 유형 재산의 재산 손해에 해당하는지가 쟁점이다. 제6연방항소법원은 카드 재발급 비용·사용 감소 손실을 유형 재산의 재산 손해로 해석할 수 없다고 판단하였다. 카드 재발급 비용·사용 감소 손실은 상업종합책임보험의 담보 범위에서 제외된다.

49) Deborah L. Johnson·William Simpson, "Cyber Insurance For Public Housing: Confronting Market Barriers and Forging Policy Solutions", 『Student Journal of Information Privacy Law』, Vol. 3(1), 2025, p. 151.

Ⅳ. 사이버공격의 책임 귀속과 면책

1. 사이버공격의 국가 연계 의혹과 책임 귀속

가. 사이버공격의 국가 연계 의혹과 보험자의 책임

Merck 사건[50]에서 법원은 정치·군사적 판단이 요구되는 낫페트야[51]의 국가 연계 의혹과 별도로 보험자의 책임을 판단하였다. 약관 설계·언더라이팅 기준·위험 배분 구조 등 보험법 기준을 적용하여 보험자의 책임을 판단하는 접근 방식을 채택한 것이다. 사이버공격의 공격 주체·배후의 정치·군사적 의혹으로 보험자를 면책할 수 없다.

나. 전쟁 면책조항의 전통적인 의미와 사이버공격

광범위한 손해에서 보험자를 면책하는 전쟁 면책조항 적용 범위는 제한 해석되어야 한다. 사이버공격을 전통적인 의미의 전쟁으로 해석할 수 없다. 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁 대상의 전쟁 면책조항을 신유형의 위험인 사이버공격에 적용하기는 곤란[52]하다. 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁과 직접 대응되지 아니하는 사이버공격을 전쟁 면책조항 적용 대상으로 포함하기 위해 약관 문언의 근거가 필요하다.

50) 국가 연계 사이버공격인 낫페트야(NotPetya)로 Merck & Co., Inc.의 전자 데이터 손실·소프트웨어 오류가 발생한 사안에서 전쟁 면책조항 적용이 쟁점이었다. 뉴저지 고등법원 항소부는 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁 대상의 전쟁 면책조항 적용을 차단하였다. 항소심 판결 이후 Merck & Co., Inc.는 ACE American Insurance Co. 등과 화해(settlement)하여 청구 금액과 근접한 보험금을 수령하였다.

51) 2017년 6월 러시아 군사정보기관이 배후로 지목된 와이퍼 악성코드(wiper malware) 사이버공격이다. 복구 불가능한 전자 데이터 손실·소프트웨어 오류를 발생시키기 위해 우크라이나 세금 소프트웨어(M.E.Doc)에 초기 침투 이후 미국 국가안보국(National Security Agency) 개발 이터널블루(EternalBlue)를 이용하여 급속 확산되었다.

52) 홍보배, “사이버 전쟁 면책 조항 도입”, 『이슈 분석』, 2023.8.14.(보험연구원), 20면.

다. 법원의 전쟁 면책조항 해석과 약관 설계 방향

Merck 사건에서 법원은 약관이 사이버공격을 전쟁 면책조항 적용 대상[53]으로 규정하지 아니하기에 보험자의 면책 주장을 차단하였다. 보험자가 전쟁 개념을 확장하여 사이버공격을 포섭하려는 해석은 허용될 수 없고 신유형의 위험인 사이버공격에 전쟁 면책조항을 적용하기 위해 약관에 규정하여야 한다. 보험자는 사이버위험을 규율하는 전쟁 면책조항·사이버 전용 면책조항을 설계[54]할 필요가 있다. 이는 사이버공격의 정치·군사적 성격과 보험자의 책임을 분리하는 사법 통제로 해석할 수 있다.

2. 국가 연계 의혹과 보험자의 책임 유지

가. 보험자의 책임

Merck 사건에서 보험자는 사이버공격의 국가 연계 의혹을 근거로 전쟁 면책조항 적용을 주장하였지만, 법원은 전쟁 면책조항 적용을 차단하였다. 공격 주체·배후 특정이 모호[55]한 사이버공격의 국가 연계 의혹은 고도의 정치·군사적 분석을 요구한다. 사이버공격의 추상·간접적 국가 연계 의혹으로 약관의 명시적 근거 없이 보험자를 면책하면 보험 계약의 위험 배분 구조에 부합하지 아니하고 형평성을 훼손한다.

53) 약관은 통상 전쟁 면책조항으로 'loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combating, or defending against an actual, impending, or expected attack: a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval, or air forces; b) or by military, naval, or air forces; c) or by an agent of such government, power, authority or forces'를 규정하였다.

54) Angad Chopra, "Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims", 『Ohio State Law Journal』, Vol. 82, 2021, p. 147.

55) 송윤아·조용운, "국가 배후 사이버공격을 둘러싼 전쟁면책 적용 논쟁", 『이슈 분석』, 2022.1.10.(보험연구원), 16면.

나. 면책 제한의 근거

국가 연계 의혹을 근거로 약관의 확장 해석은 허용될 수 없기에 보험자를 면책할 수 없다. 신유형의 위험인 사이버공격에 전쟁 면책조항을 적용하기 위해 약관에 규정할 필요가 있다. Merck 사건에서 법원은 사이버공격의 국가 연계 의혹에 대한 모호성을 이유로 전쟁 면책조항 적용을 부정하고 보험자의 책임은 약관 설계·언더라이팅 기준·위험 배분 구조에 근거하여 해석되어야 한다는 기준을 제시하였다.

3. 보험자의 책임 법리의 확장 가능성

가. 금융 인프라로의 확장

사이버공격의 국가 연계 의혹을 이유로 보험자를 면책하지 아니하는 보험 판례 법리는 금융 인프라에도 적용할 수 있다. 사회 전반에 중대한 영향이 우려되는 금융 인프라에 대한 국가 연계 사이버공격에서 보험자를 면책하면 보험 계약자의 손해 구제 가능성이 현저히 저하되고 위험 이전이라는 보험에 대한 사회적 신뢰를 훼손[56]할 수 있다. 공격 주체·배후의 모호성을 이유로 전쟁 면책조항을 적용하기보다 약관 설계·언더라이팅 기준·위험 배분 구조에 근거하여 보험자의 책임을 판단하여야 한다.

나. 보험자의 책임 법리의 일반화 가능성과 한계

Merck 사건의 보험자의 책임 법리는 사이버공격의 정치·군사적 성격을 이유로 보험자를 면책하지 아니하려는 사법 통제를 의미한다. 사이버사고가 기업 영업·조직 운영, 공급망, 국가 경제·안보의 구조적 위험으로 인식되는 환경에서 보험자의 담보 범위 조정 시도로 해석할 수 있다. Merck 사건에서 법원은 사이버공격을 규정하지 아니하는 전쟁 면책조항 적용을 차단하였지만, 보험자가 사이버공격을 별도 면책조항으로 규정하면 분쟁 사건별 상이한 결론이 도출될 수 있다. Merck 사건의 보험 판례 법리는 사이버공격의 책임 귀속에 법원이 개입·통제하는 기준을 제시하는 사례로서 의의가 인정된다.

56) Giacomo Assenza et al., “Redefining Systemic Cybersecurity Risk in Interconnected Environments”, 『Applied Cybersecurity & Internet Governance』, Vol. 3(2), 2024, p. 151.

V. 사이버위험 보험 판례 법리와 보험 실무

1. 사이버공격과 전쟁 면책조항

가. 사이버공격을 규정하는 특화적 면책조항

영국의 로이드 보험조합(Lloyd's of London)은 대규모 국가 연계 사이버공격을 재산보험 등의 담보 범위에서 제외[57]하는 약관을 설계하였다. 1930년대 대규모 전쟁위험에 대한 우려로 재산보험 등에 전쟁 면책조항을 도입[58]할 당시 예상할 수 없었던 사이버공격을 규정하여 약관의 명확성·예측 가능성을 제고한 것으로 해석할 수 있다. 신유형의 위험인 사이버공격을 규정하는 특화적 면책조항으로 위험 배분 구조의 합리성을 강화할 수 있다.

나. 분쟁과 화해 과정을 통한 약관 개정

Mondelez 사건[59]에서 국가 연계 사이버공격인 낫페트야에 전쟁 면책조항을 적용할 수 있는지가 쟁점이었다. 국가 연계 사이버공격을 전쟁 면책조항으로 규율하기 어렵기에 분쟁과 화해 과정에서 특화적 면책조항의 필요성이 제기되었다. 보험자는 유사한 분쟁 사건에서 법적 위험을 우려하여 국가 연계 사이버공격을 약관에 특정하는 등 보험 실무에 영향이 발생[60]하였다.

57) Isabella Brunner, "Insurance Policies and the Attribution of Cyber Operations under International Law: A Commentary", 『New York University Journal of International Law and Politics』, Vol. 55, 2022, p. 185.

58) Lloyd's, "Market Bulletin Y4483: The Underwriting of War, Civil War and Related Perils", 2011.4.4.

59) 국가 연계 사이버공격인 낫페트야로 Mondelez International, Inc.에 대규모 손해가 발생한 사안에서 재산보험의 전쟁 면책조항을 적용할 수 있는지가 쟁점이었다. Zurich American Insurance Co.가 사이버공격에 전쟁 면책조항을 적용하여 Merck 사건과 유사한 쟁점을 포함하였지만, 화해로 종결되었다. 보험자는 사이버공격에 전통적인 전쟁 면책조항을 적용하려는 시도가 법적 위험을 수반한다는 사실을 인식하였다.

60) Justine Ferland, "Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case", 『Computer Law & Security Review』, Vol. 35, 2019, p. 375.

다. 전쟁 면책조항과 사이버공격의 분리

보험자는 국가 연계 사이버공격 면책조항을 도입하여 사이버공격을 전쟁 면책조항과 분리하는 약관을 설계[61]하였다. 개별 분쟁 사건의 보험 판례 법리가 약관 내용을 직접 규정하지 아니하여도 약관 해석·시장 관행이 약관 설계에 실질적인 제약 조건으로 기능하는 것이다. 이는 보험 판례 법리가 보험자와 보험 계약자의 위험 배분 구조를 조정하여 약관 해석·시장 관행을 통해 보험시장의 자율 규제를 형성하는 과정이다.

2. 보안 관리체계 개선 효과

가. 보안 진술과 위험 배분 구조

Travelers 사건[62]에서 법원은 보안 관리체계에 대한 보험 계약자의 중대 허위·누락 진술이 발견되면 보험자를 면책할 수 있다고 시사[63]하였다. 보험 계약자의 보안 진술에 기반하여 보험 사고 발생 가능성, 손해 빈도·규모, 위험 배분 구조를 판단할 수 있다. 보험 계약자의 중대 허위·누락 진술이 발견되면 보험자는 보험료 인상·담보 범위 축소·인수 거절을 선택하므로 언더라이팅 과정에서 위험 배분 구조가 형성된다. 중대 허위·누락 진술이 발견되어도 보험자의 책임을 인정하는 것은 위험 배분 구조와 정합적이지 아니하다.

61) K&L Gates, “After Important Cyber Insurance Victory for Policyholders, Focus Turns to Insurers’ Proposed Changes to War Exclusions”, Alerts/Updates, 2023.6.13.

62) Travelers Property Casualty Co. of America가 랜섬웨어의 피해자인 International Control Services, Inc.에 보험 계약의 효력을 부인하며 제기한 확인소송이다. 보험자는 다중 요소 인증(multi-factor authentication) 등 핵심 보안 조치를 이행하였다는 보험 계약자의 중대 허위·누락 진술에 기초하여 보험 계약이 체결되었다고 주장하였다. 일리노이 중부지방법원은 당사자의 화해 계약을 승인하여 사이버보험 계약을 소급 무효화하였다. 법원의 본안 판결은 아니지만, 보험 계약자의 보안 진술이 보험 계약에 중대한 영향을 발생시킬 수 있는 사례로 해석된다. 보험금 지급 없이 화해 계약이 승인되어 실질적으로 보험자가 승소하였다.

63) Lockton, “Travelers v. ICS underscores need to respond carefully to cyber insurance application questions”, News & Insights, 2022.9.15.

나. 보안 투자 유도와 규범 확산

보험자에게 보안 심사 지침을 제공[64]하는 보험 판례 법리가 보험시장에 보안 기준을 형성할 수 있다. 보험 계약자가 보안 기준을 위반하면 보험자는 위험 인수를 거절하므로 사이버위험을 이전하려는 기업의 보안 투자를 유도하는 것이다. 보험 계약자의 중대 허위·누락 진술이 발견되면 면책되므로 보험자는 보안 진술을 신뢰하고 효율적으로 언더라이팅을 진행할 수 있다. 보험 계약자는 사이버사고 손해로 인한 재무적 위험을 보험자에게 이전하기 위해 선제적으로 보안 관리체계를 개선하여야 하므로 사이버보안 생태계에 보안 투자를 유도하는 규범적 효력[65]이 기대된다.

Ⅵ. 우리나라의 사이버위험 보험 법제에 대한 시사점

1. 판례 법리의 규범 형성과 손해 개념 이식

가. 판례 법리의 규범 형성

성문법 국가인 우리나라도 행정기관은 판례 법리로 위법성이 확인된 사실관계·법적 판단에 기반한 행위의 방지·회피의무가 부과[66]되어 판례 법리는 행정기관이 준수하여야 하는 규범을 제시한다. 보험자가 판례 법리로 위법성이 확인된 영업행위를 지속하면 감독당국의 제재 대상이 될 수 있기에 판례 법리가 규범을 형성[67]하는 것이다. 감독당국은 판례 법리에 근거한 백내장 실손보험금 관련 보험자의 영업행위가 적법하다고 보도[68]하기도 하였다. 판례 법리는 선례 구속의 원칙이 채택되지 아니한 우리나라에서 통합성의 이념과

64) Qihao He et al., “Insuring the ‘uninsurable’ cyberwarfare: rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance”, 『The Geneva Papers on Risk and Insurance—Issues and Practice』, Vol. 50, 2025, p. 490.
65) Ibid, p. 490.
66) 대법원 2007. 5. 10. 선고 2005다31828 판결.
67) 최자유, “신용카드 결제시스템의 3-당사자(신용카드업자·가맹점·회원)에 대한 몇 가지 쟁점 검토”, 『금융감독연구』, 제8권 2호, 2021, 249면.
68) 금융감독원, “최근 판례로 알아보는 실손보험 등 관련 소비자 유의사항”, 보도자료, 2025.3.11.

헌법 제11조 평등원칙에 기반하여 법관에게 규범적 효력도 인정[69]된다. 판례 법리가 규범을 형성하는 일련의 과정을 선도하는 것이다.

나. 우리나라 법체계의 손해 개념

재산보험 등의 담보 범위는 보험 종류·약관[70] 문언·위험의 특성을 고려하여 해석할 수 있다. 전통적으로 재산보험 등의 손해 개념은 유형 재산의 물리적 파괴·변형[71]을 의미하지만, 우리나라 법체계는 유형 재산의 물리적 파괴·변형 이외에 사용 이익 상실·영업 중단·시설 이용 불능 등 기능 손해 개념을 인정한다. 재산보험 등의 손해 개념을 물리적 파괴·변형이 없는 시스템의 핵심 기능 상실 상태 등 무형 손해로 확장할 수 있다. 보험 계약의 목적·당사자의 합리적 기대·보험 목적물의 특성 등을 기준으로 사이버사고 손해 등 무형 손해를 포섭하는 접근 방식이 타당하다. 기능 손해 개념을 과도하게 확장하면 담보 범위의 모호성이 증가하여 보험자의 무분별한 보험료 인상·담보 범위 축소·인수 거절 등 시장 실패 가능성도 고려할 필요가 있다.

다. 기능 손해 개념의 해석론적 수용

Ingram Micro 사건·National Ink 사건의 기능 손해에 대한 보험 판례 법리를 재산보험 등의 약관 해석 과정에서 참고할 수 있다. 우리나라 법체계에서도 사용 이익 상실·영업 중단·시설 이용 불능 등을 손해로 해석[72]할 수 있다. 기업 영업·조직 운영에 중대한 영향이 우려되는 전자 데이터·소프트웨어의 암호화로 인한 시스템의 핵심 기능 상실 상태를 재산보험 등의 담보 범위에서 제외하면 손해의 실질을 반영하기 어렵다. 시스템의 핵심 기능 상실 상태, 손해의 지속 기간, 대체 수단의 존재, 복구 가능성 등을 고려하여 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에 포함할 수 있다.

---

69) 송민경, "판례의 규범력에 관한 연구", 『저스티스』, 통권 제167호, 2018, 255면.
70) 미국은 ISO 표준 재산보험 서식(building and personal property coverage form)·표준 상업종합책임보험 서식(commercial general liability coverage form)을 기반으로 보험자가 약관을 작성하고 우리나라도 이를 참고하는 경향이다.
71) 김이수, "코로나바이러스감염증(Covid-19) 팬데믹과 손해보험", 『비교사법』, 제29권 4호, 2022, 86면.
72) 위의 논문, 89면.

라. 재산보험 등의 담보 범위 확장과 한계

면책조항이 없는 우연한 위험은 원칙적으로 포괄위험 구조인 재산보험[73][74]의 담보 범위에 포함된다. 전자적 오염·기능 상실 상태는 재산보험의 급격하고 우연한 직접적인 물리적 파괴·손해[75][76]로 담보 범위에 포함될 수 있다. 랜섬웨어는 전자적 장치의 전자기적 배열을 파괴·변형하여 시스템의 핵심 기능 상실 상태를 발생시키므로 전자적 장치의 급격하고 우연한 직접적인 물리적 파괴·손해로 해석할 수 있다. 컴퓨터 기록·데이터[77]는 재산보험 등의 담보 범위에서 제외[78]되지만, 하드웨어 오염·기능 상실 상태로 급격하고 우연한 직접적인 물리적 파괴·손해가 발생하면 담보 범위에 포함될 수 있다.

2. 사이버공격의 정치·군사적 성격과 보험자의 책임 분리

가. 정치·군사적 성격과 보험자의 책임 판단

사이버공격의 정치·군사적 성격은 보험자의 책임과 상이한 영역이므로 국가 연계 의혹과 보험자의 책임을 분리하여 위험 배분 구조를 검토하여야 한다. 우리나라도 국가 연계 의혹이 보험자의 책임 판단에서 고려되는 구조가 아니므로 유사한 통제 구조를 상정할 수 있다. 국가 연계 의혹은 보험자의 면책 기준으로 설계된 것은 아니다.

---

73) package insurance policy. 영문본이 원본이고 국문본은 참고 목적으로 제공된다.
74) 대형 보험자의 약관은 대부분 유사하여 2개 보험자의 약관을 검토하였다.
75) sudden and accidental direct physical destruction of or damage to the property.
76) A 보험자의 재산종합보험 약관 Section I Property All Risks Cover(Scope of Cover)는 급격하고 우연한 직접적인 물리적 파괴·손해를 규정하고, B 보험자의 약관도 동일하다.
77) computer records or data.
78) A 보험자의 재산종합보험 약관 Section I Property All Risks Cover(B. Excluded Property)는 컴퓨터 기록·데이터를 담보 범위에서 제외하고, B 보험자의 약관도 동일하다.

나. 보험자의 책임 구조와 약관 해석

사이버공격의 정치·군사적 성격과 국가 연계 의혹은 전쟁 면책조항 적용 근거로 해석하기 어렵다. Merck 사건의 보험 판례 법리는 신유형의 위험인 사이버공격에서 법원의 판단 영역을 특정하여 사이버공격의 정치·군사적 성격과 보험자의 책임을 분리하는 과정에 참고할 수 있다. 예외적 규정인 재산보험의 전쟁·침략·외적의 행위·적대행위·전쟁 유사 군사행위(전쟁 선포 여부 불문)·내전[79] 등 전쟁 면책조항[80]은 약관 문언으로 제한 해석[81] 되어야 한다. 사이버공격이 국가와 연계되어도 무력 충돌·군사 작전·무기 사용 등 군사적 교전이 아니라면 전쟁으로 해석할 수 없다. 민간 기업 대상 비군사적 사이버공격은 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁과 상이하다.

3. 사이버위험 보험을 통한 보안 관리체계 개선 유도

가. 금융감독체계와 결합

Travelers 사건에서 법원은 보험자의 위험 평가·보험료 산정·담보 범위 결정·보안 심사와 보험 계약자의 보안 진술을 간접 규제로 인정하였다. 우리나라에서도 보험자의 위험 평가·보험료 산정·담보 범위 결정·보안 심사로 기업의 보안 관리체계를 평가하고 보험 계약 조건에 반영하여 기업의 보안 관리체계 개선을 유도[82]한다. 간접 규제 모델은 감독당국이 보안 관리체계 개선을 요구하지 아니하여도 해석 기준이 시장 전반에 확산되는 경로를 제공한다. 이는 공적 규제 권한 확장·신유형의 규제 수단 도입을 요구하지 아니하는 자율 규제로 금융감독체계와 정합적이다.

79) war, invasion, act of foreign enemy, hostilities or warlike operations (whether war be declared or not), civil war.
80) A 보험자의 재산종합보험 약관 Section I Property All Risks Cover(General Exclusions)는 (a) 전쟁·침략·외적의 행위·적대행위·전쟁 유사 군사행위(전쟁 선포 여부 불문)·내전을 규정하고 B 보험자의 약관도 동일하다.
81) 대법원 1994. 11. 22. 선고 93다55975 판결.
82) 장영진, 앞의 자료, 2025.

나. 감독당국의 심사·표준 약관

Merck 사건에서 법원이 사이버공격에 전쟁 면책조항 적용을 부정하여 사이버위험을 약관 설계 단계에서 규율할 필요성이 제기되었다. 약관 문언이 모호하면 해석의 불이익이 귀속[83]되는 보험자는 법적 위험을 우려하여 사이버사고와 전쟁을 구분하는 약관 설계를 시도하였다. 감독당국의 심사[84]·표준 약관[85] 등을 통해 사이버위험의 정의·담보 범위인 손해 유형·면책 사유 등을 제시하는 접근 방식을 고려할 수 있다. 이는 약관 설계 기준을 제시하여 보험시장의 자율 조정을 유도하는 간접 규제로 감독당국의 심사·표준 약관 등 가이드라인은 보험자의 언더라이팅 과정에서 요구되는 보안 관리체계를 제시한다.

다. 랜섬웨어 손해의 담보 범위

National Ink 사건에서 법원은 랜섬웨어로 인한 암호화를 기능 손해로 해석하여 재산보험의 담보 범위에 포함할 수 있다고 판시하였다. 우리나라에서도 감독당국이 사이버사고에 적극 대응하는 과정[86]에서 랜섬웨어 손해를 재산보험의 담보 범위에 포함할 수 있는지가 중요 쟁점으로 부각될 것이다. 랜섬웨어 손해를 재산보험의 담보 범위에 전면 포함·제외하기보다 보안 관리체계를 반영하여 보험료·담보 범위·자기 부담금·면책 사유 등을 차등화하는 구조가 타당하다.

라. 보안 투자 유도와 사이버위험 보험 판례 법리

Travelers 사건에서 법원은 보험자의 위험 평가·보험료 산정·담보 범위 결정·보안 심사가 기업의 보안 투자를 유도할 수 있다고 시사하였다. 사이버위험 보험에도 상법의 보험법리가 적용[87]된다. 우리나라에서도 사이버종합보험 보험자의 언더라이팅 과정에서 보안

83) 약관의 내용이 모호하면 작성자 불이익 원칙(약관해석법 제5조 2항)이 적용된다.
84) 감독당국은 보험자가 기초서류 작성·변경 원칙(보험업법 제128조의3), 보험요율 산출 원칙(보험업법 제129조)을 위반하면 변경 권고(보험업법 제127조의2)를 할 수 있다.
85) 보험업 감독업무 시행세칙 [별표 15]는 생명보험, 화재보험, 자동차보험, 질병·상해보험, 실손의료보험, 배상책임보험, 채무이행보증보험, 신용보험, 신용보증보험 등의 표준 약관을 규정한다. 재산보험 등은 표준 약관이 도입되지 아니하였다.
86) 금융위원회, "금융권 침해사고가 재발하지 않도록 철저히 대비하고 점검하겠습니다", 보도자료, 2025.7.30.

서비스 진행 상황에 대한 기업의 중대 허위·누락 진술을 고지의무(상법 제651조) 위반으로 해석하여 보험자를 면책하는 보험 판례 법리[88]를 고려하면 유사하게 해석할 수 있다. 보안서비스 진행 상황에 대한 기업의 중대 허위·누락 진술을 보험자가 인식하였다면 보험료 인상·담보 범위 축소·인수 거절을 선택하였을 것이다.

4. 단계적 접근 방식

가. 단계적 접근 방식의 필요성

간접 규제 모델을 이식하는 과정에서 단계적 접근 방식이 요구된다. ① 감독당국은 명확성·예측 가능성·비례성을 기준으로 약관 등 기초서류를 검토하여 합리성을 제고하여야 한다. ② 재산보험 등 전통적인 보험 유형에 표준 약관을 도입하기보다 가이드라인을 통한 자율 규제를 유도하여야 한다. ③ 입법적 개선 방안으로 사이버보험을 제도화할 수 있다.

나. 기초서류 심사 기준

감독당국은 명확성[89]·예측 가능성[90]·비례성[91]을 기준으로 약관 등 기초서류를 검토할 수 있다. 평균적 보험 계약자의 관점에서 담보 범위·면책 사유 등 보험 계약의 주요 내용을 해석할 수 있는지 판단하는 명확성은 보험자와 보험 계약자의 정보 비대칭을 완화하고 약관의 모호성으로 인한 분쟁을 예방하기 위해 요구된다. 약관 문언으로 담보 범위·면책 사유 등을 해석할 수 있는지 판단하는 예측 가능성은 보험 계약자가 사이버사고 손해 등이 담보 범위에 포함되는지 인지하여 위험 관리·의사 결정에 참고할 수 있도록 필요하다. 보험 계약 해지·취소 사유의 합리성을 판단하는 비례성은 보험자와 보험 계약자의 위험 배분 구조의 형평성을 확보하고 보험의 사회적 신뢰 제고에 기여할 수 있다.

87) 권진홍·김새움, "사이버보험의 주요 내용 및 쟁점", 『BFL』, 제105호, 2021, 45면.
88) 서울중앙지방법원 2019. 5. 17. 선고 2018가합528105 판결.
89) 평균적 보험 계약자가 약관의 담보 범위·면책 사유를 이해할 수 있는지 심사한다.
90) 기능 손해, 전자 데이터 손실·소프트웨어 오류, 시스템 마비, 복구 비용 등 약관의 담보 범위·면책 사유를 해석할 수 있는지 심사한다.
91) 보험 계약자의 경미한 고지의무 위반 등을 이유로 보험자를 면책하거나 보험 계약을 소급 무효화하는 것은 불공정하므로 약관에 보험 계약 해지·취소 사유가 합리적으로 규정되어 있는지 심사한다.

다. 약관 규제 방향

재산보험 등 전통적인 보험 유형에 표준 약관을 도입하기보다 가이드라인을 통한 자율규제를 유도하여 보험시장의 자율성을 존중하고 약관의 모호성으로 인한 분쟁을 완화하는 절충적 접근 방식이 타당하다. 감독당국이 재산보험 등 약관에 ① 사이버사고, 전자 데이터·소프트웨어, 기능 손해, 복구 비용, 랜섬웨어 손해 정의, ② 직접 손해와 간접 손해 구분, ③ 보안 질문서의 고지 사항과 보험 계약 해지·취소 사유, ④ 중대 허위·누락 진술의 판단 기준을 규정하도록 권고할 수 있다. 시스템의 핵심 기능 상실 상태, 영업 중단, 복구 가능성, 대체 수단 등을 고려하여 담보 범위를 해석하는 약관을 설계하여야 한다. 국가 연계 사이버공격에 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁 대상의 전쟁 면책조항을 적용하는 약관은 허용될 수 없다.

라. 입법적 개선 방안

개인정보 처리자에게 손해배상 책임 이행을 위한 보험 등 가입의무를 부과하는 현행 법제는 정보 유출로 인한 제3자 손해배상 책임 확보[92]에 주목하여 사이버손해를 포섭하기에 한계[93]가 있다. 현행 의무보험을 사이버사고 전반에 대한 위험 보장체계로 확대하여야 한다. 일정 규모 이상 디지털 서비스 제공자·주요 정보통신 기반시설 운영자에게 사이버위험 보험 가입의무를 부과[94]하고 정보 유출 이외에 서비스 중단 손해·복구 비용·사고 대응 비용·제3자 손해배상 책임 등 최소 담보 항목[95]을 제시할 필요가 있다. 중소기업·스타트업은 동일한 가입의무를 부과하기보다 모범 약관 제시, 보안 개선 계획 제출, 조건부 인수와 연계한 단계적 가입의무를 설계하여 보험 접근 가능성을 보장[96]하여야 한다. 손해 개념,

92) 일정 규모 이상 개인정보 처리자에게 손해배상 책임 이행을 위한 보험·공제 가입, 준비금 적립 등 의무가 부과(개인정보보호법 제39조의7)된다.
93) 송윤아·홍보배, "주요국 정부의 사이버보험 시장 참여 배경 및 동향", 『이슈보고서』, 2021-19, 2022.1.14.(보험연구원), 58면.
94) 박정훈 의원(안) 제4조는 일정 규모 이상 정보통신서비스 제공자에게 사이버재해보험 가입의무를 부과한다.
95) 박정훈 의원(안) 제2조는 손해 유형으로 제3자 손해배상 책임, 데이터 복구 비용, 사업 중단 손해, 사고 조사 비용 등을 열거한다.
96) 박정훈 의원(안) 제20조는 중소기업에 대한 보험료 지원을 규정한다.

전쟁 면책조항, 보안 고지의무 등은 보험 판례 법리로 규범이 형성되는 구조를 완화하여 감독당국의 전문성을 기반[97]으로 규제를 검토하여야 한다.

Ⅶ. 결론

미국에서는 사이버위험을 규율하는 통일적 규범이 부재하여 보험 판례 법리로 공적 규제를 보완하는 간접 규제 모델이 규범을 형성한다. 약관 설계·언더라이팅 기준·위험 배분 구조의 변화 등을 촉진하여 행위 기준을 형성하는 사이버위험 보험 판례 법리는 사이버보안 생태계에 규범적 효력이 기대된다.

Ward General 사건·America Online 사건에서 법원은 기업 영업·조직 운영에 중대한 영향이 우려되는 무형 손해인 전자 데이터 손실·소프트웨어 오류를 재산보험 등의 담보 범위에서 제외하였다. Ingram Micro 사건에서 법원은 시스템의 핵심 기능 상실 상태인 기능 손해를 재산보험의 담보 범위에 포함하였지만, 2010년대 중반 이전 예외적 보험 판례 법리로 일반화하기 어렵다. National Ink 사건에서 법원은 Ingram Micro 사건의 보험 판례 법리의 연장선에서 사이버 환경에 부합하게 전자 데이터 손실·소프트웨어 오류로 인한 시스템의 핵심 기능 상실 상태를 재산보험의 담보 범위에 포함하였다. EMOI Services 사건에서 법원은 코로나-19로 인한 기업휴지보험 판례 법리와 유사하게 재산보험의 담보 범위를 물리적 파괴·변형으로 제한 해석하여 기능 손해 개념에 대한 논란이 지속 중이다. Merck 사건에서 법원은 무력 충돌·군사 작전·무기 사용 등 물리적 전쟁 대상의 전쟁 면책조항을 신유형의 위험인 국가 연계 사이버공격에 적용할 수 없다고 판시하였다. 보험자의 책임은 약관 설계·언더라이팅 기준·위험 배분 구조에 근거하여 해석하여야 한다. Travelers 사건에서 법원은 보험 계약자의 보안 관리체계에 대한 중대 허위·누락 진술을 이유로 보험 계약을 소급 무효화하는 화해 계약을 승인하였다. 보험자의 위험 평가·보험료 산정·담보 범위 결정·보안 심사는 기업의 보안 투자를 유도하는 수단이다.

97) 박정훈 의원(안) 제8조는 사이버재해보험 사업 영위를 위해 과학기술정보통신부 장관과 약정을 체결하도록 규정한다. 과학기술정보통신부 장관은 약정 체결 과정에서 금융위원회와 협의하여야 한다.

디지털 전환이 가속화되는 상황에서 우리나라도 사이버위험 보험 법제를 시급하게 정비하여야 한다. ① 보험 계약의 목적·당사자의 합리적 기대·보험 목적물의 특성 등을 기준으로 기능 손해 개념을 도입하여 사이버사고 손해 등 무형 손해를 재산보험의 담보 범위에 포함할 수 있다. ② 사이버공격의 정치·군사적 성격을 이유로 약관의 명시적 근거 없이 보험자를 면책하면 보험 계약의 위험 배분 구조에 부합하지 아니한다. ③ 보험자에게 보안 지침을 제공하는 보험 판례 법리는 사이버위험을 이전하려는 기업의 보안 투자를 유도하여 보안 관리체계를 개선할 수 있다. ④ 약관과 담보 범위에 대한 감독의 제도적 근거인 기초서류 심사 과정의 명확성·예측 가능성·비례성 기준, 가이드라인을 통한 자율 규제, 사이버보험을 제도화하는 입법적 개선 방안 등 단계적 접근 방식을 논의하여야 한다.

참고문헌

김원각, “사이버 위험에 대한 미국 보험사업자의 대응에 관한 연구”, 『경제법연구』, 제21권 3호, 2022.

김이수, “코로나바이러스감염증(Covid-19) 팬데믹과 손해보험”, 『비교사법』, 제29권 4호, 2022.

신계하·손승우, “사이버보험 활용의 순기능과 역기능에 관한 연구”, 『한국산업보안연구』, 제12권 3호, 2022.

송민경, “판례의 규범력에 관한 연구”, 『저스티스』, 통권 제167호, 2018.

최자유, “신용카드 결제시스템의 3-당사자(신용카드업자·가맹점·회원)에 대한 몇 가지 쟁점 검토”, 『금융감독연구』, 제8권 2호, 2021.

황정혜, “사이버공격 증가에 따른 사이버보험의 동향 및 법제에 관한 연구”, 『법이론실무연구』, 제13권 2호, 2025.

금융감독원, “최근 판례로 알아보는 실손보험 등 관련 소비자 유의사항”, 보도자료, 2025.3.11.

금융위원회, “금융권 침해사고가 재발하지 않도록 철저히 대비하고 점검하겠습니다”, 보도자료, 2025.7.30.

권순일·한진현, “사이버 리스크 실태와 과제”, 『이슈 분석』, 2025.5.26.(보험연구원).

권진홍·김새움, “사이버보험의 주요 내용 및 쟁점”, 『BFL』, 제105호, 2021.

송윤아·홍보배, “주요국 정부의 사이버보험 시장 참여 배경 및 동향”, 『이슈보고서』, 2021-19, 2022.1.14.(보험연구원).

송윤아·조용운, “국가 배후 사이버공격을 둘러싼 전쟁면책 적용 논쟁”, 『이슈 분석』, 2022.1.10.(보험연구원).

장영진, “사이버 보험 활성화를 위한 제언”, 『이슈와 논점』, 제2392호, 2025.7.30.(국회입법조사처).

홍보배, “사이버 전쟁 면책 조항 도입”, 『이슈 분석』, 2023.8.14.(보험연구원).

대법원 1994. 11. 22. 선고 93다55975 판결.

대법원 2007. 5. 10. 선고 2005다31828 판결.

서울중앙지방법원 2019. 5. 17. 선고 2018가합528105 판결.

Aggeliki Tsohou et al., “Cyber insurance: State of the art, trends and future directions”, 『International Journal of Information Security』, Vol. 22(3), 2023.

Amy R. Willis, “Business Insurance: First-Party Commercial Property Insurance and the Physical Damage Requirement in a Computer- Dominated World”, 『Florida State University Law Review』, Vol. 37(4), 2010.

Angad Chopra, “Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims”, 『Ohio State Law Journal』, Vol. 82, 2021.

Daniel A. Lyons, “States and Systemic Risk: An Analysis of the Dodd-Frank Act’s (Un)Cooperative Federalism”, 『Nevada Law Journal』, Vol. 22, 2021.

Deborah L. Johnson, “Demystifying the Elusive Quest for Cyber Insurance Protection: The Need for New Contract Language”, 『Cardozo Law Review』, Vol. 44(6), 2023.

Deborah L. Johnson·William Simpson, “Cyber Insurance For Public Housing: Confronting Market Barriers and Forging Policy Solutions”, 『Student Journal of Information Privacy Law』, Vol. 3(1), 2025.

Ellen S. Pryor, “The Economic Loss Rule and Liability Insurance”, 『Arizona Law Review』, Vol. 48, 2006.

Gareth Mott et al., “Between a rock and a hard(ening) place: Cyber insurance in the ransomware era”, 『Computers & Security』, Vol. 128, 2023.

Giacomo Assenza et al., “Redefining Systemic Cybersecurity Risk in Interconnected Environments”, 『Applied Cybersecurity & Internet Governance』, Vol. 3(2), 2024.

Isabella Brunner, “Insurance Policies and the Attribution of Cyber Operations under International Law: A Commentary”, 『New York University Journal of International Law and Politics』, Vol. 55, 2022.

Jeff Kosseff, “Defining Cybersecurity Law”, 『Iowa Law Review』, Vol. 103, 2018.

Jeff Kosseff, “Upgrading Cybersecurity Law”, 『Houston Law Review』, Vol. 61, 2023.

Justine Ferland, “Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case”, 『Computer Law & Security Review』, Vol. 35, 2019.

Natalie E. deLatour, “Insuring the ‘Uninsurable’: Business Interruption Insurance Coverage & COVID-19”, 『Georgia State University Law Review』, Vol. 37, 2021.

Omri Ben-Shahar·Kyle D. Logue, “Outsourcing Regulation: How Insurance Reduces Moral Hazard”, 『Michigan Law Review』, Vol. 111, 2012.

Qihao He et al., “Insuring the ‘uninsurable’ cyberwarfare: rethinking war exclusions in cyber policies and the role of insurance in global cybersecurity governance”, 『The Geneva Papers on Risk and Insurance —Issues and Practice』, Vol. 50, 2025.

Scott G. Johnson, “What Constitutes Physical Loss or Damage in a Property Insurance Policy?”, 『Tort Trial & Insurance Practice Law Journal』, Vol. 54(1), 2019.

Tom Baker·Kyle D. Logue, “Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment”, 『Minnesota Law Review』, Vol. 102, 2017.

Andrew M. Cuomo, Governor of New York, "Governor Cuomo Announces First-In-The-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1", Press Release, 2017.2.16.

Burns & Wilcox, "Cyber Insurance Outlook: Emerging Risks, Underwriting Trends, and Strategic Insights", 2025.9.25.

Debevoise & Plimpton LLP, "Cybersecurity Requirements for Insurance Companies - The NYDFS Rules as the Emerging Standard", Debevoise Data Blog, 2020.8.19.

K&L Gates, "After Important Cyber Insurance Victory for Policyholders, Focus Turns to Insurers' Proposed Changes to War Exclusions", Alerts/Updates, 2023.6.13.

Lloyd's, "Market Bulletin Y4483: The Underwriting of War, Civil War and Related Perils", 2011.4.4.

Lockton, "Travelers v. ICS underscores need to respond carefully to cyber insurance application questions", News & Insights, 2022.9.15.

NYDFS, "DFS Announces Second Amendment to Nation-Leading Cybersecurity Regulation", Press Release, 2023.11.1.

American Guarantee and Liability Insurance Co. v. Ingram Micro, Inc., 2000 WL 726789 (D. Ariz. 2000).

America Online, Inc. v. St. Paul Mercury Insurance Co., 347 F.3d 89 (4th Cir. 2003).

EMOI Services, LLC v. Owners Insurance Co., 170 Ohio St. 3d 78, 2022-Ohio-4649 (Ohio 2022).

Home Depot, Inc. v. Steadfast Insurance Co., No. 23-3720 (6th Cir. 2025).

Merck & Co., Inc. v. ACE American Insurance Co., No. A-1879-21 (N.J. Super. Ct. App. Div. 2023).

Mondelez International, Inc. v. Zurich American Insurance Co., No. 2018L011008 (Ill. Cir. Ct. 2018).

National Ink and Stitch, LLC v. State Auto Property and Casualty Insurance Co., 435 F. Supp. 3d 679 (D. Md. 2020).

Site Jab v. Hiscox Insurance Co., No. 4:23-cv-03853 (S.D. Tex. 2024).

Travelers Property Casualty Co. of America v. International Control Services, Inc., No. 2:22-cv-02145 (C.D. Ill. 2022).

Ward General Insurance Services, Inc. v. Employers Fire Insurance Co., 114 Cal. App. 4th 548 (Cal. Ct. App. 2003).

Abstract

In the Ward General and America Online cases, courts held that electronic data loss and software malfunction do not constitute direct physical loss or damage under commercial property insurance or property damage to tangible property under commercial general liability insurance. In the Ingram Micro and National Ink cases, courts recognized the concept of functional loss. However, in the EMOI Services case, the court limited coverage to physical destruction or alteration. In the Merck case, the court held that traditional war exclusion clauses could not be applied to cyberattacks. In the Travelers case, the court approved the rescission of a cyber insurance policy based on misrepresentations regarding cybersecurity controls.

As digital transformation accelerates, Korea should reform its cyber risk insurance framework by recognizing the concept of functional loss, limiting broad war exclusion clauses for cyberattacks, encouraging cybersecurity investment through insurance law, and adopting a phased regulatory approach.

※ Key words: cyber risk, commercial property insurance, commercial general liability insurance, direct physical loss or damage, tangible property, property damage, functional loss, war exclusion clause, ransomware, underwriting, indirect regulation