2026.08.18. 제38호

KiRi 보험법 리뷰

| 포커스 |

사이버 사고 관련 최근 미국 보험 판례
: 약관 해석의 원칙을 중심으로

최유리 연구위원

요 약

○ 사이버 사고가 기업 운영에 중대한 위험으로 부상하며 사이버보험의 중요성도 커지고 있으나, 비교적 새로운 상품인 사이버보험에 대해 누적된 판례가 적어 약관 해석의 불확실성이 존재하므로 최근 미국 판례를 통해 사이버보험약관 해석 사례 및 시사점을 살펴보고자 함

○ Kane 사건에서 뉴멕시코주 항소법원은 해킹으로 발생한 공급업체 미지급 대금의 보장 여부와 관련하여 사이버보험약관에 사용된 전치사 'for'의 의미가 불명확하다고 보아 작성자 불이익의 원칙을 적용하였는바, 일상적인 단어라도 다의적으로 해석되지 않도록 명확한 약관 작성이 중요함

○ CiCi 사건에서 텍사스 북부 연방 지방법원은 랜섬웨어 한도 특약이 랜섬웨어 공격으로 인해 발생한 손실에 적용되는지에 관하여 해당 특약과 약관 본문의 구성 및 세부 조항을 명백한 의미의 원칙 및 조화 해석의 원칙에 따라 해석하여 그 적용을 부인하였는바, 약관 작성 시 특약과의 연결 등 계약 구조의 정합성을 면밀히 검토할 필요가 있음

○ Merck 사건에서 뉴저지주 항소법원은 대규모 사이버 사고와 관련하여 전통적인 전쟁 면책 조항은 명백한 의미의 원칙 및 제한해석의 원칙에 의해 사이버 사고에 적용되지 않는다고 판단하였는바, 변화하는 사이버 환경의 리스크에 대응하기 위해 현행 약관의 적정성을 주기적으로 점검할 필요가 있음

○ 위 판례들은 우리나라 약관 해석 법리와도 일부 유사한 면이 있으므로 사이버보험약관에 관한 판례가 드문 실정에서 잠재적 분쟁 요소를 가늠할 수 있는 초기 참고 자료가 되고, (i) 보험계약자 측면에서는 가입 시 보장 범위를 명확히 파악할 필요성과 (ii) 보험회사 측면에서는 최신 판례 동향을 반영하여 약관의 명확성을 제고할 필요성이 있음을 시사함

1. 검토배경

○ 사이버 사고는 기업 운영에 중대한 위험 요소이며 이에 대응하기 위한 사이버보험의 중요성이 대두되고 있음

- Munich Re의 '글로벌 사이버 리스크 및 보험 설문조사 2026'에 따르면 한국 C-레벨 임원의 59%는 사이버 공격에 대해 우려하고 있음[1)]
- Allianz가 위험관리 전문가를 대상으로 한 2026년도 조사에서는 사이버 사고를 가장 큰 위험으로 손꼽고 있음[2)]

○ 그러나 사이버보험은 누적된 판례가 많지 않고 이는 약관 해석의 불확실성으로 이어질 수 있음

- 사이버보험은 비교적 새로운 상품이어서 사법적 판단을 받을 기회가 많지 않았으므로 사이버보험약관, 특히 전통적인 보험상품에서 통용되었던 약관 조항이 사이버 사고에는 어떻게 적용될지에 대한 불확실성이 존재함
- 사이버 분야의 특성상 진화하는 사이버 공격 방식 및 그에 따른 다양한 피해 양상으로 인해 불확실성이 가중됨
- 우리나라의 저조한 사이버보험 침투율을 고려할 때 판례의 축적이 더딜 가능성이 높음
  - 2025년 기준 우리나라 사이버보험 시장 규모는 약 300만 달러로 아시아·태평양의 주요국과 비교해도 미미한 수준임[3)]

○ 이에 최근 미국 판례 중 사이버보험약관을 심도 있게 다룬 판례를 살펴보아 약관 해석에 적용된 다양한 법리 및 국내 사이버보험에 대한 시사점을 살펴보고자 함

- 아래 소개하는 판례에서 적용된 약관 해석의 원칙에는 작성자 불이익의 원칙, 면책 조항에 대한 제한해석의 원칙 등 우리나라 약관 해석의 법리와 맥을 같이하는 부분이 있어 판례가 적은 사이버보험 시장에서 유의미한 참고자료가 될 수 있음
- 약관 해석의 불확실성은 당사자 간 권리관계 문제에서 나아가 사이버보험 시장 가입자의 신뢰 및 보험회사의 정확한 요율 산정에 부정적인 영향을 끼칠 수 있는바, 최근 판례 동향을 살펴 잠재적 분쟁 요소를 파악한 뒤 선제적으로 약관 문구를 수정한다면 불확실성 리스크를 줄이는 데 기여할 수 있음

---

1) Munich Re Global Cyber Risk and Insurance Survey 2026(https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/Cyber_Survey_2026_Whitepaper.pdf/_jcr_content/renditions/original./Cyber_Survey_2026_Whitepaper.pdf)

2) 이러한 사이버 사건 리스크의 예시로는 사이버 범죄, IT 네트워크 및 서비스 장애, 맬웨어/랜섬웨어, 데이터 침해, 벌금 및 과태료가 포함됨; Allianz Risk Barometer 2026(https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026.pdf)

3) 권순일·한진현(2025), 「사이버 리스크 실태와 과제」, KIRI 리포트, 보험연구원, p. 17(Gallagher Re(2024), "Protecting the Digital Revolution" 재인용)

2. Kane 사건[4)]

가. 사건 배경

○ 2025년 6월 뉴멕시코주 항소법원은 사이버보험약관에 사용된 전치사 'for'의 해석에 따라 해킹으로 발생한 공급업체 미지급 대금의 보장 여부가 달라지는 사건에서, 작성자 불이익의 원칙을 적용하여 보험금 지급을 명하는 판결을 선고함

- 이 사건 원고(보험계약자)[5)]는 정당한 공급업체에 지급할 거래대금을 해커가 원고의 컴퓨터와 이메일 시스템에 침투하여 위조한 공급업체 명세서에 따라 해커 지정 계좌로 송금하였음. 원고는 피고(보험회사)의 종합 사이버 침해 대응 보험에 가입되어 있었고, 정당한 공급업체로부터 미지급 대금의 지급을 요구받자 이에 대해 피고에게 보험금 지급을 청구하였음
- 이 사건의 핵심쟁점은 제3자 청구 담보 관련하여 '보안 침해에 대해(for)[6)] 보험계약자에게 제기된 청구로 인한 손해에 대해 보장한다'는 취지의 문구에서 'for'의 해석이었음[7)]
  - 원고는 'for'를 ~로 인한(because of), ~로부터 발생한(arising out of), 또는 ~의 결과로 발생한(as a result of)의 의미로 넓게 해석함. 즉, 공급업체의 대금 청구는 원고가 보안 침해로 인해 공급업체에 대금을 미지급하게 되어 발생한 것이므로 이에 대한 손실도 보장 범위에 포함된다고 주장함
  - 피고는 'for'가 명백히 등가(等價, equivalent to)만 의미하므로 보안 침해와 직접적으로 연관된 손실만 보장된다고 주장함. 이에 따르면 실질적인 보장은 원고 컴퓨터 시스템 내의 데이터 손실 또는 유출에 대한 청구로만 국한됨
- 뉴멕시코주 지방법원(1심)과 항소법원(2심) 모두 약관 해석상 보장 범위에 해당한다고 판단하였고, 이에 따라 약 350만 달러[8)]의 보험금 지급이 결정됨

---

4) *Kane v. Syndicate 2623-623 Lloyd's of London*, 584 P.3d 1079(N.M. Ct. App. 2025)
5) 이 사건 원고 New Mexico Health Connections, Inc.는 의료보험회사였으나, 청산 절차에 따라 뉴멕시코주 보험감독원장(Superintendent of Insurance) Alice Kane이 청산관리인(Receiver)로서 이 사건 원고의 지위를 승계받음
6) 후술하는 바와 같이 전치사 'for'의 의미가 이 사건의 핵심 쟁점이나 이 부분에서는 가독성을 위해 '~대해'로 번역함
7) 이 사건 보험약관은 제3자 청구 담보 외에도 사기성 지시로 인해 발생한 손실에 대한 담보(Fraudulent instruction coverage)도 제공하였으나, 그 보장한도는 25만 달러로 이 사건 손실액에 미치지 못하였음. 양 당사자는 사기성 지시로 인해 발생한 손실에 대한 담보가 이 사건에 적용된다는 점에 동의하였고, 피고 역시 해당 담보만이 배타적으로 적용된다고 주장하지 않았음. 따라서 본건의 약관 해석에 관한 쟁점은 제3자 청구 조항에 한정되었음. 다만 이처럼 사이버 사고로 인해 발생하는 손실은 그 성격에 따라 여러 담보의 적용 대상이 될 수 있으므로 만약 특정 담보에 한정하여 적용하고자 한다면 사고의 원인, 손실의 유형, 청구의 주체 및 보장 항목 등을 기준으로 각 담보의 적용 범위를 명확히 규정할 필요가 있음
8) 미지급된 공급자 거래대금 전액에서 수사당국이 해커로부터 회수한 액수를 제외한 금액에 해당함

보험약관 관련 조항

(국문 번역)

데이터 및 네트워크 배상책임

다음 각 호의 사유에 대해[1] 피보험기간 중 피보험자에 대하여 최초로 제기된 청구로 인하여 피보험자가 법적으로 지급할 의무를 부담하는 [손해배상금 및 청구 비용에 대한 보장을 제공함][2]

…

2. 보안 침해

(원문)

Data and Network Liability

[Coverage is provided for damages and claims expenses] which the insured is legally obligated to pay because of any claim first made against an insured during the policy period for:

….

2. a security breach.

주: 1) 가독성을 위하여 편의상 'for'를 '~대해'로 번역함
2) 판결문에는 약관 조항의 일부만 직접 인용되어 있어 문맥상 필요한 부분은 판결문의 설명을 바탕으로 대괄호([ ])에 보충하여 기재하였음. 판결문의 인용 과정에서 사용된 대소문자 및 문장부호에 관한 편집표시는 가독성을 위해 생략하였음

나. 약관 해석 법리 - 불명확성과 작성자 불이익의 원칙

○ 항소법원은 (i) 먼저 관련 문구 의미의 불명확성(Ambiguity)을 판단하고, (ii) 불명확성이 인정된 후 비로소 작성자 불이익의 원칙을 적용함

○ 항소법원은 다음 요소 등을 종합적으로 고려하여 이 사건 보험약관에서 'for'의 의미의 불명확성을 인정함

- 첫째, 약관의 다른 조항에 대해 이 사건 보험약관은 (i) 'for'에 대한 별도 정의 조항이 없고, (ii) '보안 침해'에 더해 '데이터 손실'이 별도의 보장 항목으로 존재하므로 '보안 침해' 항목이 직접적인 데이터 손실만 보장한다는 해석은 타당하지 않고, (iii) 보험약관의 다른 조항에서는 '직접적인 결과'로 인한 비용만 보장된다는 표현을 명시적으로 사용하였지만 문제가 된 조항에서는 그러한 표현을 사용하지 않았다는 것을 고려함
- 둘째, 사전적 의미에 대해 원고와 피고가 주장하는 'for'의 의미 모두 사전에 등재되어 있다는 것을 고려함
- 셋째, 판례 검토에 대해 사이버보험약관 해석과 관련된 판례는 극히 드물고, 전통적인 보험약관 해석에 대한 판례도 'for'의 의미에 대해 여러 견해가 있다는 것을 고려함
- 넷째, 업계 관행 및 작성 경위에 대해 이 사건 사이버보험 작성 경위에 대한 구체적 자료는 없으나, (i) 사이버보험 상품은 비교적 최근에 만들어진 상품이고, (ii) 가입자들은 사이버 보안 사고에 대해 이해도가 낮은 경우가 많아 많은 정보가 있는 보험회사와 정보 비대칭이 존재하며, (iii) 보험회사들 사이에서도 표준 사이버보험약관이 존재하지 않으며, (iv) 가입자는 더욱 정교해지는 보안 침해 수법이 초래할 수 있는 모든 결과를 예상하기 어렵고 사이버보험에 가입하기만 하면 특별히 예외로 명시되지 않는 이상 모든 위험이 보장되리라 생각할 수 있다는 것을 고려함

○ 불명확성이 인정된 후 법원은 작성자 불이익의 원칙을 적용하여 원고의 주장대로 'for'을 넓게 해석하여 원고의 손실이 약관상 보장 범위에 포함된다고 판단함

다. 시사점

○ 본 판례에서 법원은 불명확성이 인정된 후 작성자 불이익의 원칙을 적용하였는데, 이는 우리나라 판례에서 약관 해석상 의미가 불명확할 때 작성자 불이익 원칙을 적용한다는 점과 유사함

○ 보험회사 측에서는 작성자 불이익의 원칙이 적용되지 않도록 그 전 단계인 불명확성 판단 단계에서 명확성을 입증하는 것이 중요한데, 사이버보험의 특성상 명확성 입증을 어렵게 하는 요소가 있을 수 있으므로 명확한 약관 작성이 더욱 중요함

- 작성자 불이익의 원칙이 적용되면 보험약관은 특별한 사정이 없는 이상 작성자인 보험회사에 불리하게 해석되므로 보험금 지급 판결로 이어질 가능성이 커짐
- 위에서 살펴본 바와 같이, 항소법원은 2025년 판례임에도 (i) 사이버보험이 비교적 최근 만들어졌다는 점, (ii) 통상 가입자보다 보험회사가 사이버 보안 침해의 리스크에 대해 이해도가 높다는 점 등을 들어 '업계 관행' 요소에 대해 모호성 인정 방향으로 판단함. 이러한 판단 근거는 사이버보험의 일반적인 특성에 기초한 것이므로 다른 사이버보험 사건에도 적용될 수 있음
- 또 다른 불명확성 판단 요소인 '판례 검토'와 관련하여 항소법원은 사이버보험약관 해석에 대한 판례가 미국 전역에서 드물다고 설시하고 전통적인 보험 판례를 적용했음. 이처럼 직접적인 사이버보험 판례가 제한적이라는 점은 사이버보험약관 해석의 불확실성을 높이는 요인이 될 수 있음

○ 이 사건에서는 일상적으로 사용하는 전치사 'for'의 해석이 쟁점이 되어 결국 약 350만 달러의 보험금 지급이 결정된바, 보편적으로 활용되는 단어라도 다의적으로 해석되지 않도록 약관 작성 시 유의하여야 함[9)]

- 예컨대, 이 사건 보험약관에서 보안 침해에 대해 '직접적인 데이터 손실에 대한 제3자 청구'만 보장된다고 명시하거나 관련 정의 조항을 기재하였다면 불명확성의 리스크를 줄일 수 있었을 것으로 생각됨. 다만 'for'와 같이 매우 광범위하고 자주 쓰이는 전치사를 일괄적으로 정의하는 것은 다른 문제를 초래할 수 있으므로, '보안 침해에 대해(for) 제기된 청구'등 관련 문구를 정의하는 방안을 고려할 수 있음

9) 이와 유사하게 최근 Connelly 사건에서도 사이버보험약관상 'for'의 해석이 쟁점이 되었음. 해당 사건에서는 원고가 A업체에 지급할 대금을 해커가 이메일 해킹 및 전화 사칭을 통해 편취하였고, 원고는 A업체에 대금을 지급하기 위해 당시 가입되어 있던 사이버보험에 따라 보험금 지급을 요청하였음. 피고 보험회사는 보험약관상 보장 범위인 'Claim for Security Breach'(보안 침해에 대한(for) 청구)에서 'for'를 좁게 해석하여 지급을 거절하였고 추후 소송에서도 같은 이유로 '청구 원인 미비로 인한 소 각하 신청'(Fed. R. Civ. P. 12(b)(6))을 하였으나, 워싱턴 연방법원(1심)은 2025년 8월 'for'의 해석에 대해 불명확성을 인정하고 작성자 불이익의 원칙을 적용하여 일부 기각하였음; Connelly Law Offs., PLLC v. Cowbell Cyber, Inc., No. 25-cv-00302-JHC, 2025 WL 2256657 (W.D. Wash. Aug. 7, 2025)

3. CiCi 사건[10)]

가. 사건 배경

○ 2026년 2월 텍사스 북부 연방 지방법원은 특정 사이버보험의 랜섬웨어 관련 특약이 랜섬웨어 공격으로 인해 발생한 손실에 적용되는지가 쟁점이 된 사건에서 명백한 의미의 원칙 및 조화 해석의 원칙에 따라 약관을 해석한 결과 그 적용을 부인함

- 원고(보험계약자)는 랜섬웨어 공격으로 인해 약 120만 달러의 손실이 발생했다고 주장함
- 원고가 당시 가입되어 있던 피고(보험회사)의 사이버보험약관은 (i) 본문 제I조 D항 사이버 협박(Cyber Extortion) 조항에서 사이버 협박에 대해 최대 300만 달러를 보장하고, (ii) 부칙(Attachment) 랜섬웨어 사건 세부 한도 특약(Ransomware Event Sublimit Endorsement, 이하 '랜섬웨어 특약')에서 랜섬웨어 사건 관련 보험금 지급 한도를 25만 달러로 설정함
- 이 사건 보험약관에 포함된 랜섬웨어 특약은 25만 달러 한도가 적용되는 보장 항목이 무엇인지 및 약관 본문의 사이버 협박 보장 조항과 어떻게 연계되는지 등을 명확히 규정하고 있지 않아 해당 특약의 명칭이 랜섬웨어 특약임에도 불구하고 랜섬웨어로 인해 발생한 이 사건 손실에 대한 적용 여부가 쟁점이 됨
- 법원은 후술하는 바와 같이 명백한 의미의 원칙 및 조화 해석의 원칙을 적용하여 이 사건 랜섬웨어 특약이 적용되지 않는다고 판단함

나. 약관 해석 법리 – 명백한 의미의 원칙 및 조화 해석의 원칙

○ 법원은 랜섬웨어 이 사건 랜섬웨어 특약이 적용되지 않는다고 판단 함에 있어 (i) 명백한 의미의 원칙(Plain meaning rule) – 보험약관에 달리 정하지 않은 이상 약관의 용어는 '명백하고, 통상적이며, 일반적으로 인정되는 의미(Plain, ordinary and generally accepted meaning)'로 해석해야 함 – 및 (ii) 조화 해석의 원칙 – 모든 조항이 조화를 이루고 유효하도록 문서 전체를 통합적으로 해석해야 한다는 원칙 – 에 따라 이 사건 보험약관을 해석하였으며, 구체적으로 이 사건 랜섬웨어 특약 및 보험약관을 살펴본 내용은 다음과 같음

- 랜섬웨어 특약은 형식적인 구성에 그쳐 25만 달러 한도의 적용 방식을 명확하게 규정하고 있지 않음. 특히, 해당 특약에서 제공되고 있는 보장에 '한하여'(solely) 한도가 적용된다는 문구가 있으므로 그 외의 보장에는 한도의 적용이 배제된다고 해석되는데, 해당 특약에서는 제공되는 보장이 무엇인지 명확하지 않음
- 랜섬웨어 특약은 약관 본문의 제II조(보험 한도)에 추가된다고 명시되어 있을 뿐, 보장 항목이 포함된 제I조에 적용된다는 내용이 없음

---

10) *CiCi Enters., LP v. HSB Specialty Ins. Co.*, No. 3:23-CV-2155-L, 2026 WL 502954 (N.D. Tex. Feb. 23, 2026); 본 건은 텍사스 북부 연방 지방법원(1심) 약식판결 결정(Order for Motion for Summary Judgment)으로, 타 법원에 대한 권고적 선례(Pursuasive Authority)로서의 효력이 있고 구속력(Binding Authority)은 없음. 그러나, (i) 사이버보험약관에 대한 법원의 상세한 해석을 담고 있다는 점, (ii) 2026년 2월에 결정된 최신 판례라는 점, (iii) 비교적 드문 사이버보험 관련 판례인 점에서 유의미한 판례로 보여 소개하고자 함

- 랜섬웨어 특약은 사이버 협박 보장 조항과의 연관성에 대해서 명시하고 있지 않을 뿐 아니라 '특약에서 명시되지 않은 다른 조항은 변경되지 않는다'라고 규정하고 있음[11)]
- 피고는 이 사건 보험약관의 다른 특약에서는 적용 범위를 명확하게 규정하였는바, 랜섬웨어 특약이 사이버 협박 보장 조항에 적용되도록 할 의도였다면 해당 특약에 그 적용 관계를 명확하게 규정했어야 함
- 피고는 의미상 랜섬웨어 사건이 사이버 협박의 하위 개념이므로 당연히 랜섬웨어 특약이 사이버 협박 보장에 적용되어야 한다고 주장하나, 약관의 다른 부분에 랜섬웨어 사건과 사이버 협박이 한 문장에 열거된 것으로 보아 별개의 개념으로 보임

다. 시사점

○ **보험약관 작성 시 계약 구조가 의도한 바대로 정교하게 작동하는지 및 전체적인 조항이 조화롭게 해석되는지 등 정합성을 면밀하게 검토하는 것이 필요하고, 특약이 본문의 보장을 변경하는 경우 그 변경의 대상과 범위를 명확히 규정할 필요성이 있음**

- 보험약관은 통상 내용이 방대하고 중요한 특약은 부칙 등으로 추가되는 경우가 많은데, 약관의 다른 조항과 유기적으로 작동하는지 검토하여야 함. 예컨대, 이 사건 랜섬웨어 특약에서 적용되는 조항 번호를 정확히 기재하였거나, 본문의 사이버 협박 보장에 적용된다고 기재하였거나, 랜섬웨어 사건과 사이버 협박을 한 문장에 열거하지 않는 등 문구가 달리 작성되었다면 이 사건 랜섬웨어 특약이 적용되었을 가능성이 높아졌을 것으로 보임
- 형식적으로 자주 쓰이는 문구일지라도 전체적인 맥락에서 어떤 효력을 미칠지 검토해야 함. 법원은 부칙에 통상 형식적으로 쓰이는 문구인 '특약의 조항은 해당 특약에 한해서 적용되고 다른 조항은 변경되지 않는다'는 취지의 문구를 문언 그대로 해석하여 본문 조항에의 적용을 배제함

○ **또한, 사이버보험에는 정립되지 않은 용어가 많이 사용될 수 있고 관련 판례도 충분치 않으므로 용어를 명확하게 정의하는 것이 중요함**

- 피고는 사이버 협박과 랜섬웨어 사건의 의미상 후자가 전자에 포함된 개념이라고 주장하였으나 법원은 이를 받아들이지 않았고, 비교적 새롭게 도입되어 보편적으로 통용되는 의미가 정립되지 않은 용어일수록 약관에서 정확하게 정의하는 것이 필요함
- 법원은 랜섬웨어 특약 해석과 관련된 판례가 없다고 설시하였는바, 이러한 사이버보험약관 해석 판례의 희소성은 불확실성을 높이므로 명확한 약관 작성이 필요함

11) 원문 조항은 "[a]ll other terms, conditions, and exclusions of the Policy shall remain unchanged"(약관의 다른 용어, 조건 및 제한은 변경 없이 유지된다)이며, 이는 약관의 부칙 또는 부속서류 등에 통상적으로 사용하는 문구로 보임

4. Merck 사건[12)]

가. 사건 배경

○ 대규모 사이버 공격으로 입은 손실에 대한 전쟁 면책 조항[13)]의 적용 여부가 쟁점인 사건에서 2023년 뉴저지주 항소법원은 명백한 의미의 원칙 및 제한해석의 원칙에 의해 적용이 안 된다고 판단함

- 2017년 6월경 NotPetya 사이버 공격으로 인해 원고 Merck의 기기가 수십 초 만에 약 1만 대, 종국적으로 약 4만 대 감염되었고 제조부터 판매까지 이르는 전반적인 운영에 막대한 지장을 초래함
- 사이버 공격의 배후는 러시아 연방을 위하거나 대신하여 활동한 주체들로 지목되었고, 원고의 경우 사이버 공격 주체가 우크라이나에서 사용하던 민간 제3자 회계 소프트웨어에 악성코드를 심어 감염된 것으로 밝혀짐
- 당시 원고는 다수의 보험회사에 전위험재산보험(All risk property policy)이 가입되어 있었고, 보장 범위에는 컴퓨터 데이터 또는 프로그램의 손상 및 악의적 행위로 인한 전산 마비 등도 포함되었음. 원고는 항소 단계에서 피고 보험회사들을 상대로 약 7억 달러의 보험금 지급을 청구함
- 피고는 '적대적 또는 전쟁과 같은 행위'로 발생하는 손실에 대해 보험회사를 면책시키는 전쟁 면책 조항(Hostile/Warlike action clause)이 적용된다고 주장하였으나, 법원은 명백한 의미 및 제한해석 원칙에 따라 해당 조항이 적용되지 않는다고 판단함

전쟁 면책 조항

(국문 번역)

본 보험증권은 다음을 [보장하지 않습니다:][1)]

평화의 시기 또는 전시를 막론하고 실제의, 임박한, 또는 예상되는 공격을 저지, 전투, 또는 방어하는 행위를 포함하는 적대적 또는 전쟁과 같은 행위로 인하여 발생한 손실 또는 손해로써:

(a) 정부, 주권적 권력(법률상 또는 사실상), 또는 육군, 해군 또는 공군을 유지하거나 사용하는 당국에 의한 것;

(b) 또는 육군, 해군 또는 공군에 의한 것;

(c) 또는 그러한 정부, 권력, 당국 또는 군대의 대리인에 의한 것.

(원문)

This policy does not insure [against:]

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.

주: 1) 판결문에는 약관 조항의 일부만 직접 인용되어 있어 문맥상 필요한 부분은 판결문의 설명을 바탕으로 대괄호([ ])에 보충하여 기재하였음. 판결문의 인용 과정에서 사용된 대소문자 및 문장부호에 관한 편집표시는 가독성을 위해 생략하였음

12) *Merck & Co. v. Ace Am. Ins. Co.*, 293 A.3d 535 (N.J. Super. Ct. App. Div. 2023)

13) Merck 사건을 포함한 전쟁 면책 적용 논쟁에 대해서는 송윤아·홍보배(2021), 「주요국 정부의 사이버보험 시장 참여 배경 및 동향」에서 자세히 다루고 있음. 본고에서는 이후 2023년 선고된 Merck 사건의 항소심 판결문의 전쟁 면책 조항 관련 약관 해석 법리를 중심으로 살펴보고자 함

나. 약관 해석 법리 – 명백한 의미 및 제한해석의 원칙

○ 항소법원은 전쟁 면책 조항의 명백한 의미상 이 사건에 적용되지 않으며, 달리 해석하는 것은 제한해석의 원칙에 반하는 것으로 판단함

- 보장을 제한하는 조항(이하 '제한 조항')이 적용되기 위해서는 관련 상황이 제한 조항의 문언상 명백하게 해당되어야 하고, 법원은 제한 조항을 좁게 해석해야 함
- 항소법원은 전쟁 면책 조항의 명백한 문언상 전투적 행위와 관련된 것이어야 하며, 원고와 같은 민간 고객을 상대로 상업 회계 소프트웨어를 파는 민간 회사를 공격한 행위에는 적용되지 않는다고 판단함
- 또한, 전투 행위에 참여하지 않는 기업(Non-combatant firm) 등이 관련된 이 사안에 전쟁 면책 조항을 적용하기 위해서는 해당 조항의 '적대적 행위'를 넓게 해석하여야 하며, 이는 제한 조항을 좁게 해석하는 원칙에 어긋남

○ 이에 더해 항소법원은 전쟁 면책 조항의 역사 및 관련 판례에 비추어 적용을 배제함

- 전쟁 면책 조항은 수 세기 동안 사용되었으며 이 사건 전쟁 면책 조항과 같이 '적대적 또는 전쟁과 같은 행위'를 포함하는 형태의 문구는 1950년경부터 존재했음
  - 항소법원은 이에 대한 구체적인 의견을 제시하지 않았으나, 1심법원은 국가 차원의 사이버 공격이 자행되는 빈도가 증가하는 것에 대해 보험회사들이 인지하였음에도 수년간 전쟁 면책 조항을 수정하지 않고 유지했다는 점을 피고에게 불리하게 판단함
- 사이버 공격과 관련한 전쟁 면책 조항 판례는 없으나, 다른 판례에서는 전쟁 면책 조항을 최소한 군사적 행위 또는 목적과 관련된 사안에 적용하였으므로, 민간 소프트웨어 기업에 대한 비군사적 사이버 공격인 이 사건과는 구분됨

다. 시사점

○ 우리나라의 계약 해석 원칙에도 권리의 제한·포기, 의무의 면제·축소 등을 제한적으로 해석하는 제한해석의 원칙이 존재하므로, 보험약관의 면책 조항, 특약 한도 등 보장 내역을 제한하는 조항은 특별한 주의를 기울여 명확하게 작성할 필요가 있음

○ 이 판례에서는 전통적으로 유지되어 온 전쟁 면책 조항을 이 사건 사이버 사고에 적용시키지 않았는바, 현재의 보험약관이 변화하는 사이버 환경에서 발생할 수 있는 다양한 문제들을 포괄해서 규정하고 있는지 주기적으로 점검하는 것이 필요함

○ 이 사건을 전후하여 Lloyd's of London은 (i) 2022년 8월 16일 국가 지원(State-backed) 사이버 공격에 대한 면책 조항의 최소 기준을 마련하고 독립형 사이버보험약관에 이를 의무적으로 반영하도록 규정하였고,[14]

14) Lloyd's of London, Market Bulletin Y5381: State Backed Cyber-Attack Exclusions(Aug 16, 2022)(https://www.lloyds.com/market-resources/market-bulletins)

(ii) 2024년 5월 14일 시장에서 사용되는 국가 지원 사이버 공격 면책 조항을 유형별로 분류하고 사용 기준을 명확히 하는 후속 공지를 발표함[15)]

○ 아울러, 사이버위험의 규모와 성격에 따른 보험시장의 위험인수 역량 및 위험분산 문제는 약관의 명확화만으로 해결하기 어려우므로 별도로 고려할 필요가 있음

5. 결론

○ 앞서 살펴본 판례들은 사이버보험약관 해석에 다양한 법리를 적용한 최근의 사례들을 보여줌

- 세 판례는 비교적 최근인 2023~2026년에 결정된 판례임에도 불구하고, 각 쟁점과 직접적으로 관련된 사이버보험 판례가 없거나 사이버보험에 관련된 판례 자체가 매우 드물다고 언급하고 있는 것으로 비추어 보아, 사이버보험약관에 대한 판례는 정립되어 가는 중이며 최신 판례 동향을 파악하는 것이 중요함
- 위 판례들은 불명확성 판단, 작성자 불이익의 원칙, 제한해석의 원칙 등 다양한 약관 해석 법리를 적용하였는데, 우리나라 약관 해석 법리에도 일견 유사한 부분이 있으므로 사이버보험약관상 분쟁 소지가 있는 사안들을 위 판례들로 가늠해 볼 수 있음[16)]

○ 앞서 살펴본 판례에서와 같이 사이버보험의 보장 범위가 불명확할 경우 예상하지 못한 분쟁으로 이어질 수 있으므로, 보험계약자 측면에서는 사이버보험 가입 시 보장 범위를 명확히 파악하는 것이 중요하며, 특히 예상되는 사고가 어떠한 보장 항목에 해당하는지와 세부 한도 및 면책에 따라 어떠한 보장 공백이 발생할 수 있는지를 확인할 필요가 있음

- 또한 사이버보험은 다양한 보장과 면책이 상호 연계되어 그 구조와 적용 범위를 파악하기 쉽지 않을 수 있다는 점에서 보험계약자가 보장 범위를 스스로 정확히 파악하는 데에는 일정한 한계가 있으므로 보험회사 및 판매·중개 주체의 정확한 설명과 안내도 중요하며, 이는 보험시장에 대한 신뢰 형성에도 기여할 수 있음

○ 보험회사는 관련 판례 및 업계 동향을 참고하여 사이버보험약관의 명확성을 지속적으로 제고할 필요가 있음

- Merck 사건이 진행되는 중에 Lloyd's of London이 전쟁 면책 조항의 리스크에 대응하기 위해 문구 기준을 마련한 것과 같이, 이러한 판례들은 사이버보험약관 개선의 계기로 작용하고 있음
- 이러한 배경지식 없이 기존 문구를 사용하거나, 특히 해외 사이버보험약관을 차용할 때 관련 조항에 업데이트가 반영되었는지 확인하지 않을 경우, 잠재적 분쟁 요소까지 함께 도입할 수 있으므로 주의가 필요함
- 이에 더해 우리나라 시장 및 규제 환경의 동향을 반영하여 사이버보험약관의 내용을 지속적으로 점검하고 명확히 정비하려는 노력이 중요함

---

15) Lloyd's of London, Market Bulletin Y5433: State Backed Cyber Attack Wordings(2024. 5. 14.)(https://www.lloyds.com/market-resources/market-bulletins)

16) 다만 약관 해석에 대한 미국과 우리나라 법리의 취지가 유사하더라도 세부적인 내용은 상이할 수 있으므로 적용 시 주의가 필요함