



제 432회 국회 (임시회)
제3차 과학기술정보방송통신위원회

사이버재해보험법안

검 토 보 고

〈사이버재해보험 제도 도입〉

■ 박정훈의원 대표발의(의안번호 제2215050호)

2026. 2.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I. 제안경위	1
II. 제안이유 및 주요내용	1
III. 검토의견	4
1. 제정안의 체계	4
2. 총괄적 검토	5
3. 총칙(제1장)	9
4. 사이버재해보험사업의 운영(제2장)	18
5. 사이버재해보험사업의 지원(제3장)	29
※ 참고자료	36
1. 개인정보 보호법 시행령 [별표 1의4]	36
2. 과학기술정보통신부 의견	37
3. 금융위원회 의견	39
4. 손해보험협회 의견	40
5. 한국인터넷기업협회 의견	42
6. 한국인터넷기업협회 추가 의견	45

I. 제안경위

가. 발 의 자 : 박정훈의원 등 10인

나. 발 의 일 : 2025. 12. 9.

다. 회 부 일 : 2025. 12. 22.

II. 제안이유 및 주요내용

제안이유

디지털 전환 가속화에 따라 기업과 국민에게 사이버 위협으로 인한 피해를 보호하기 위한 다양한 제도를 마련하고 있으나, 침해사고 발생 시 신속하고 실질적인 손해를 보상하는 종합적인 보험 제도는 미비한 실정임.

최근 기업과 국민은 급증하는 랜섬웨어 등 지능화·고도화된 사이버 공격으로 인하여 심각한 정보자산 손실과 영업 중단 등 막대한 경제적 피해를 입고 있으며, 특히 중소기업의 경우 자체적인 피해 복구가 어려워 경영상의 큰 위기에 직면하는 사례가 발생하고 있음.

이에 침해사고 발생 시 피해 기업과 정보통신망 이용자에 대한 신속하고 공정한 손해 보상이 이루어지도록 사이버재해보험을 제도화하고, 일정 규모 이상의 정보통신서비스 제공자에게 해당 보험의 가입을 의무화하며, 전문적인 손해평가 제도를 마련하는 등 사이버재해에 대한 기업의 사이버복원력을 강화하고 사회안전망을 구축하려는 것임.

주요내용

- 가. 침해사고로 인한 정보자산 피해와 정보통신망 이용자의 손해를 신속하고 공정하게 보상하기 위한 사이버재해보험에 필요한 사항을 규정함으로써 국민과 기업의 디지털 생활 안정에 이바지함을 목적으로 함(안 제1조).
- 나. 사이버재해보험을 침해사고로 인한 제3자 손해배상책임, 데이터 복구비용, 사업 중단 손해 등을 보상하는 보험으로 정의하고, 보험 목적물의 범위를 정보시스템, 전자상거래 플랫폼 등으로 구체화함(안 제2조 및 제5조).
- 다. 사이버재해보험사업에 관한 주요 사항을 심의하기 위하여 과학기술정보통신부장관 소속으로 사이버재해보험심의위원회를 둠(안 제7조).
- 라. 정보통신서비스 제공자 중 사업 분야, 매출액 및 이용자 수 등을 고려하여 대통령령으로 정하는 자에게 사이버재해보험 가입 의무를 부과함(안 제4조).
- 마. 보험료를 산정 시 보험목적물의 위험도, 피보험자의 보안 수준, 사이버위험지표 등을 반영하도록 기준을 마련함(안 제10조).
- 바. 침해사고로 인한 손해액을 조사·확정하고 보험금을 산정하는 손해평가 업무의 전문성과 공정성을 확보하기 위하여 손해평가인 제도를 도입하고, 자격 요건 및 결격사유 등을 규정함(안 제15조부터 제17조까지).

사. 정부는 중소기업 또는 소상공인이 사이버재해보험에 가입하는 경우 예산의 범위에서 보험료의 일부를 지원할 수 있도록 함(안 제20조).

아. 과학기술정보통신부장관은 침해사고 예방과 보험사업의 적정한 운영을 위하여 업종별·규모별 사이버재해 위험 정도를 표시하는 사이버위험지표를 작성·관리하고, 보험사업자는 이를 보험료율 산정 등에 활용할 수 있도록 함(안 제22조).

Ⅲ. 검토의견

1. 제정안의 체계

- 제정안은 「사이버재해보험법안」이라는 제명(題名) 하에 총 5개 장 31개 조문으로 구성되어 있고, 시행일은 공포 후 6개월이 경과한 날로 규정되어 있음.

제1장 총칙

제1조(목적)

제2조(정의)

제3조(보험사업의 관장)

제4조(보험가입의무)

제5조(보험목적물)

제6조(피보험자)

제2장 사이버재해보험사업의 운영

제7조(사이버재해보험심의위원회)

제8조(보험사업자)

제9조(침해사고의 통지)

제10조(보험료율의 산정)

제11조(보험가입금액의 한도)

제12조(기초서류의 변경)

제13조(보험의 모집)

제14조(보험사업의 회계구분)

제15조(손해평가)

제16조(손해평가인)

제17조(손해평가인의 자격취소 등)

제18조(재보험계약의 체결)

제19조(보험가입의 촉진 등)

제20조(보험료 지원)

제3장 사이버재해보험사업의 지원

제22조(사이버위험지표의 작성)

제23조(학술 조사·연구의 진흥)

제4장 보칙

제24조(자료제출 요구)

제25조(보고 등)

제26조(분쟁조정)

제27조(권한 등의 위임·위탁)

제28조(「보험업법」 등의 적용)

제5장 벌칙

제29조(벌칙)

제30조(양벌규정)

제31조(과태료)

2. 총괄적 검토

- 최근 지속적으로 발생하는 사이버 침해사고¹⁾는 정보자산 자체의 손실뿐 아니라 서비스 중단에 따른 영업 손실, 사고 대응 및 복구에 필요한 비용, 평판 훼손 등 연쇄적 피해를 유발하는바, 이러한 사이버 리스크 관리는 국가와 기업의 핵심과제로 부상하고 있음.
- 최근 10년간 글로벌 사이버보험 시장이 빠르게 성장하고 있는 것과는 달리, 우리나라의 사이버보험 활성화는 여전히 부진한 실정임²⁾. 침해사고 신고 건수가 빠르게 증가하고 있으며,³⁾ 특히 중소기업을 대상으로 하는 공격이 매우 증가하는 추세임⁴⁾.
- 이러한 맥락에서, 제정안은 사이버 침해사고 발생 시 피해 기업과 이용자에 대한 신속하고 공정한 손해배상이 이루어지도록 ‘사이버 재해보험’을 제도화하고, 일정 규모 이상의 정보통신서비스 제공자에게 보험 가입 의무를 부과하는 한편, 전문적인 손해평가 제도(보험료 지원 체계 및 평가 체계 구축 등)를 마련하고, 중소기업 또는 소상공인에 대한 보험료 지원의 근거를 마련하여 사이버재해보험시장 활성화 및 정보통신서비스 제공자의 보안 수준 향상 유인을 제공하려는 것임.

1) 랜섬웨어, 서버 해킹, DDoS 등

2) 우리나라의 사이버보험은 3백만 달러 수준으로, 일본(1.96억 달러)나 호주(4.76억 달러) 등 주요 국가와 비교했을 때 현저히 낮은 수준이며, 필리핀이나 태국 등과 유사한 수준에 머무르고 있음.

3) 2024년 1,887건으로 전년 대비 47.8% 증가함.

4) 권순일·한진현, 「사이버 리스크 실태와 과제」, 보험연구원, 2025.5.26

- 제정안은 「농어업재해보험법」, 「농어업인의 안전보험 및 안전재해 예방에 관한 법률」, 「풍수해 · 지진재해보험법」, 「산업재해보상보험법」 등의 기존 보험 관련 개별법의 구조를 참고한 것으로 보임.
- 다만, 의무가입 규정이 사업자에게 새로운 규제로 작용할 수 있고, 이미 개인정보보호와 관련하여 다층적인 규율 체계가 존재하는 점을 고려할 때, 의무가입 규정이 목적 달성에 필요한 최소한의 수단인지 검토할 필요성이 있음.
- 또한, 중소기업 · 소상공인에 대한 보험료의 일부 지원은 이들의 위험흡수 능력을 보완한다는 정책적 타당성이 있으나, 반대로 정보보호에 대한 자발적 노력 유인을 저해할 수 있다는 우려도 제기되는바, 도덕적 해이를 방지할 수 있는 제도적 설계가 가능한지 추가적인 논의가 필요함.
- 아울러 사이버위험지표가 최신 IT 환경의 다양성과 변화를 충분히 반영하지 못하여 사이버 보안 위험이 왜곡되어 평가될 우려가 있음.
- 현행 「보험업법」 체계에서도 보험시장의 원리에 따라 사이버 재해관련 대응 보험 상품들이 설계될 가능성이 있음을 고려해야 할 것임.
- 이미 실제로 일부 국내 보험사⁵⁾는 사이버사고 종합보험을 판

5) 삼성사이버종합보험(삼성화재), 사이버종합보험(DB 손해보험), 사이버프로텍션보험(한화손해보험) 등

매하고 있으며, 국내 사이버재해보험 활성화를 위해 보험개발원, 보험사 등이 보험료 산정에 참고할 수 있는 리스크 산출 모델, 비용 추정 모델링 등의 연구 용역을 추진하고 있으므로, 정부의 관여를 법률에 직접 규정하는 것보다 민간영역의 연구 개발을 자율적으로 보완 및 규율할 수 있는 환경을 조성하는 방안도 검토할 필요가 있음.

- 국회예산정책처 비용추계서에 따르면, 제정안 시행에 따라 2027년부터 2031년까지 5년간 총 1억 1,400만 원(연평균 2,300만 원)의 추가 예산 소요가 발생하는 것으로 추계 됨. 구체적으로는 사이버재해보험심의위원회 운영과 관련하여 연평균 1,100만 원⁶⁾, 손해평가 요령 마련과 관련하여, 연평균 1,200만 원⁷⁾임.
- 과학기술정보통신부는 침해사고 발생 시 피해기업과 정보통신망 이용자에게 신속하고 실질적인 손해를 보상하는 사이버재해 보험 활성화 취지에 공감하나, 보험 가입 의무화 등 법제화에 대해선 신중한 검토가 필요하다는 의견을 제시함.
- 손해보험협회는 사이버 리스크가 국가적 재난으로 확대되는 현 상황에서 사이버보험의 제도화 등의 제정 취지에는 적극 공감하나, 다만 기존 법령과의 정합성, 제도 운용의 실효성 등을 추가적으로 고려할 필요가 있다는 의견을 제시함.

6) 유사 사례인 '농업재해보험심의회'의 경우를 참고하여 회의를 연 4회 개최하고, 총 15인의 위원으로 구성되며, 1회 회의 개최 시 1인당 30만 원을 지급하는 것으로 가정함.

7) 추계 첫해에는 연구 용역을 통하여 마련하고, 이후 개정이 필요한 경우에는 과학기술정보통신부가 별도의 연구 용역 없이 자체적으로 손해평가요령을 개정하는 것을 가정함.

- 한국인터넷기업협회는 보험 가입 의무화에 따른 기업자율성 침해 및 재정 부담이 가중될 수 있고, 보험 목적물 정의가 불명확하고 광범위하여 과도한 보험료 산정 우려가 있으며, 다양한 성격의 IT 환경을 반영할 수 있는 평가 체계가 선행되어야 하므로 신중히 검토해야 한다는 의견을 제시함.
- 보다 구체적인 사항에 대해서는 이하의 조문별 검토에서 논의하겠음.

3. 총칙(제1장)

가. 정의(안 제2조, 제5조)

(1) 제정안 요지

- “침해사고”, “사이버재해보험” “보험가입금액”, “보험료”, “보험금”, “손해평가” 및 “손해평가인” 등에 대하여 정의함(안 제2조).
- “보험목적물”의 내용을 정의함(안 제5조).
- “보험사업자”가 될 수 있는 회사의 범위를 정의함(안 제8조).

(2) 제정안 조문

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “침해사고”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항제7호에 따른 침해사고를 말한다.
2. “사이버재해보험”이란 침해사고로 인하여 발생하는 다음 각 목의 손해를 보상하는 보험을 말한다.
 - 가. 제3자에 대한 손해배상책임
 - 나. 데이터 복구비용, 사업 중단 손해 및 사고조사 비용
 - 다. 그 밖에 대통령령으로 정하는 손해
3. “보험가입금액”이란 보험사고 발생 시 보험자가 부담하는 최고한도액으로서 보험계약에서 정한 금액을 말한다.
4. “보험료”란 보험계약에 따라 보험계약자가 보험사업자에게 지급하는 금액을 말한다.
5. “보험금”이란 보험사고 발생 시 보험사업자가 피보험자에게 지급하는 금액을

말한다.

6. “손해평가”란 침해사고로 인한 손해액을 조사·확정하고 보험금을 산정하는 것을 말한다.

7. “손해평가인”이란 제16조에 따른 자격을 취득하여 손해평가업무를 수행하는 자를 말한다.

② 이 법에서 사용하는 용어의 뜻은 제1항에서 정하는 것 외에는 「지능정보화 기본법」, 「전기통신사업법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 다른 법률에서 정하는 바에 따른다.

제5조(보험목적물) 사이버재해보험이 담보할 수 있는 보험의 목적물(이하 “보험목적물”이라 한다)은 다음 각 호의 정보자산으로 한다.

1. 개인정보 및 고객정보를 처리하는 정보시스템
2. 전자상거래 플랫폼 및 온라인 서비스 시스템
3. 클라우드컴퓨팅서비스 및 데이터베이스
4. 사물인터넷 기기 및 스마트 기기
5. 산업제어시스템 및 중요인프라 시스템
6. 그 밖에 침해사고의 가능성과 보험의 효용성 등을 종합적으로 고려하여 대통령령으로 정하는 정보자산

제8조(보험사업자) ① 사이버재해보험사업을 할 수 있는 자(이하 “보험사업자”라 한다)는 다음 각 호와 같다.

1. 「보험업법」 제2조제6호에 따른 보험회사
2. 그 밖에 다른 법률에 따라 사이버재해 관련 보험 또는 공제사업(共濟事業)을 할 수 있는 기관이나 단체

② 보험사업자가 사이버재해보험사업을 하려면 다음 각 호의 서류를 과학기술정보통신부장관에게 제출하고, 과학기술정보통신부장관과 사이버재해보험사업에 관한 약정을 체결하여야 한다.

1. 사업방법서, 보험약관, 보험료 및 책임준비금 산출방법서(이하 “기초서류”라 한다)

2. 그 밖에 정관, 법인등기부등본 등 대통령령으로 정하는 서류

③ 과학기술정보통신부장관은 제2항에 따라 약정을 체결하려면 기초서류의 적정성에 대하여 금융위원회와 협의하여야 한다.

④ 제2항에 따른 사이버재해보험사업에 관한 약정에 관하여 필요한 사항은 과학기술정보통신부령으로 정한다.

(3) 검토사항

- 안 제2조, 제5조 및 제 8조는 제정안에서 사용되는 용어인 ‘침해사고’, ‘사이버재해보험’, ‘보험가입금액’, ‘보험료’, ‘보험금’, ‘손해평가’, ‘손해평가인’, ‘보험목적물’ 및 ‘보험사업자’의 의미를 분명히 규정하려는 것임.
- 제정안은 일정한 요건을 갖춘 사업자에게 사이버재해보험에 의무적으로 가입하도록 규정하므로, 법규정의 침익적 성격을 고려할 때 법률에서 사용되는 개념에 대한 명확성의 원칙이 더욱 엄격하게 요구됨.
- 이러한 관점에서, 제정안은 ‘침해사고’의 정의를 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 정의에 연동⁸⁾시켜 개념의 정합성은 확보하고는 있으나, 침해사고의 범위가 넓고 기술환경 변화에 따라 해석이 달라질 수 있어 보험사고 해당성 판단에서 분쟁이

8) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

7. “침해사고”란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

나. 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

발생할 소지가 있음.

- 특히, 개인정보 유출, 영업비밀 유출, 서비스 장애 등은 각각 「개인정보 보호법」, 「부정경쟁방지 및 영업비밀보호에 관한 법률」, 「전기통신사업법」 상 책임 및 제재와 중첩될 수 있음.
- 또한, 안 제2조제1항제2호 나목의 ‘사업 중단 손해’의 정의를 별도로 명확하게 규정할 필요가 있음.
- 일반적인 손해와는 달리, 사이버재해로 인한 손해의 경계가 모호하여, 어느 범위까지 손해로 인정되는지에 대한 분쟁이 발생할 수 있음. 예컨대, 해킹 피해로 인해 사이트 운영이 일시 중지된 쇼핑몰의 경우, 사업 중단 손해가 직원 인건비 등 고정비용에 한정되는지, 혹은 매출 손실까지 포함하는지 불명확함.
- 따라서 법률에서 ‘사업 중단 손해’에 대하여 큰 틀을 정의하고, 시행령에서 세부기준을 정하도록 위임하는 것이 필요함.
- 손해보험협회는 법령상 ‘사업 중단 손해’에 대한 명확한 정의를 신설함으로써 기업이 의무적으로 가입해야 하는 보험에 대한 불확실성을 해소할 필요가 있다는 의견을 제시함.

손해보험협회의 수정 의견

「사이버재해보험법」 제2조 (정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. “사업 중단 손해”란 침해사고로 인해 피보험자의 시스템의 전체적 또는 부분적 이용 불가능으로 발생한 직접적인 고정비용 손실 및 총이익 손실을 의미한다.

- 또한, 안 제5조의 보험목적물의 정의와 관련하여, 목적물이 지나치게 광범위하게 정의되는 경우 보험자는 불확실성을 반영해 보수적으로 보험료를 책정하거나, 당사자 간에 분쟁 위험이 커질 수 있으므로 시행령 등에서 추가적인 판단 기준을 규율하여 구체성을 높일 필요가 있음.
- 한국인터넷기업협회는 보험목적물의 광범위성과 불명확성으로 인해 보험료가 적정 수준보다 과도하게 산정 우려가 있으므로, 보험목적물의 범위를 더욱 구체적이고 한정적으로 명시해야 한다는 의견을 제시함. 특히 제3항의 ‘클라우드컴퓨팅서비스 및 데이터베이스⁹⁾’, 제4항의 ‘사물인터넷 기기 및 스마트 기기¹⁰⁾’의 경우 기업의 전체 서비스가 대상이 될 수 있음에 반해, 침해사고 발생 시 기업 운영에 영향이 미미한 대상까지 포함될 가능성이 있다는 입장임.

9) 테스트/개발 서버, 단순 아카이빙 및 로그 저장소, 단순 정보성 사내 인트라넷 서비스

10) 단순 전시 및 홍보용 디스플레이 장치, 테스트 모바일 및 사물인터넷 기기

나. 보험가입의무(안 제4조)

(1) 제정안 요지

- 정보통신서비스 제공자 중 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 자에게 사이버재해보험에 가입할 의무를 부과함.

(2) 제정안 조문

제4조(보험가입의무) ① 정보통신서비스 제공자 중 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 사이버재해보험에 가입하여야 한다. 다만, 다른 법률에 따라 사이버재해를 보상하는 보험에 가입한 경우로서 대통령령으로 정하는 요건을 충족하는 경우에는 이 법에 따른 보험에 가입한 것으로 본다.

② 제1항에 따른 정보통신서비스 제공자는 사이버재해보험계약을 매년 갱신하여야 한다.

③ 제1항에 따른 보험가입의 시기, 절차 및 방법, 제2항에 따른 계약 갱신의 증명서 제출방법 등에 필요한 사항은 대통령령으로 정한다.

(3) 검토사항

- 최근 쿠팡, SKT 해킹과 관련하여, 개인정보 유출 배상책임 보험의 최소 가입금액이 실제 피해 규모와 비교하면 턱없이 부족하다는 비판이 제기된다는 점에서, 가입금액을 상향하거나 의무적인 보험 가입을 규정해야 한다는 의견이 제시되고 있음.

- 제정안은 정보통신서비스 제공자 중 사업 분야, 매출액, 이용자 수 등을 고려하여 대통령령으로 정하는 자에게 사이버재해보험 가입 의무를 부과하도록 규정하여, 하위법령을 통해 의무가입 대상자를 탄력적으로 규율할 수 있게 하는 것임.
- 이와 같은 의무가입을 규정한 법률로는 「화재로 인한 재해보상과 보험 가입에 관한 법률」이 있음. 해당 법률에 따르면 특수건물의 소유자에 대해 보험 가입 의무를 규율하며, 이러한 특약부화재보험에 가입하지 아니한 자는 벌금을 부과하도록 규정하고 있는데¹¹⁾, 특수건물 화재는 제3자에게 피해를 미치는 외부효과가 매우 크며, 무자력 가해자가 실효적인 배상을 하지 못하는 상황이 발생할 수 있는바, 피해자에 대한 실효적인 구제를 위해 의무가입 규정이 마련된 것으로 보임.
- 일정 규모 이상의 정보통신서비스 제공자에서 사이버재해가 발생할 경우 피해가 광범위하게 확산되는 등 외부효과가 크고, 책임이 있는 사업자가 배상할 여력이 안 되는 경우 피해자에 대한 실효적인 구제가 어렵다는 점을 고려할 때,

최소한의 보상 재원을 사전에 확보하고 위험을 분산시킴으로써 규모의 경제를 실현하기 위한 측면에서 제정안과 같이 일정 요건을 충족하는 사업자에 보험 가입 의무를 부과할 타당성이 인정될 수 있음.

11) 「화재로 인한 재해보상과 보험가입에 관한 법률」 제5조(보험 가입의 의무) ① 특수건물의 소유자는 그 특수건물의 화재로 인한 해당 건물의 손해를 보상받고 제4조제1항에 따른 손해배상책임을 이행하기 위하여 그 특수건물에 대하여 손해보험회사가 운영하는 특약부화재보험에 가입하여야 한다. 다만, 종업원에 대하여 「산업재해보상보험법」에 따른 산업재해보상보험에 가입하고 있는 경우에는 그 종업원에 대한 제4조제1항에 따른 손해배상책임 중 사망이나 부상에 따른 손해배상책임을 담보하는 보험에 가입하지 아니할 수 있다.
제23조(벌칙) 제5조제1항을 위반하여 특약부화재보험에 가입하지 아니한 자는 500만원 이하의 벌금에 처한다.

- 현행 제도에서는 보험 가입을 유도할 수 있는 세제 혜택 등의 유인이 부족하며, 의무보험 가입 대신 준비금 적립방식이 인정¹²⁾되고 있어 실질적인 보험 가입 유인이 낮다는 한계가 있는바¹³⁾, 이에 대한 대안으로 보험 가입 의무를 규정하는 것은 합리적인 대안이 될 수 있음.
- 그러나 기존 법령체계를 활용하거나 완화된 의무 부과 규정으로도 입법 목적을 상당 부분 달성할 수 있는지 추가적인 검토가 필요함.
- 사이버사고 대응과 피해 구제를 위해 이미 「개인정보 보호법」상 안전 조치 의무¹⁴⁾ 및 손해배상 책임¹⁵⁾, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”)상 침해사고 대응·신고¹⁶⁾ 및 기술적·관리적 보호조치, ISMS/ISMS-P 인증을 통한 정보보호 관리체계 구축, 민사상 불법행위책임 등 다층적 규율이 존재하므로, 보험 가입 의무를 별도로 부과하지 않더라도 정책적 목적 달성이 가능할 수 있음.
- 특히 보험 가입을 의무화하는 것은 (1) 보험료 부담이 이용요금 인상 등으로 전가될 우려가 있고, (2) 담보 범위·면책 조항에 따라 가입은 했으나 실질 보상은 제한되는 형태가 될 수 있으며, (3) 보험사가 요구하는 보안 수준을 충족하기 어려운 사업자는 사실상 시장에서 배제되거나 과도한 비용을 부담할 가능성이 있어, 규제의 효과 대비 침해의 정도가 크지 않은지 검토가 필요함.

12) 개인정보 보호법 시행령 [별표 1의4], 참고자료 1 참조

13) 권순일·한진현, 「사이버 리스크 실태와 과제」, 보험연구원, 2025.5.26

14) 제28조의4

15) 제39조

16) 제48조의2, 제48조의3

- 따라서, 특정한 요건을 갖춘 사업자에게 보험 가입을 의무화하는 것이 아닌, 보험료 세액공제·보조 등 인센티브를 통한 자율가입 확대, 대규모 사고에 대비한 공적 재보험 또는 정부 지원 마련, 표준약관·표준담보 제정 및 비교공시를 통한 시장 투명성 제고와 같은 침해적인 효과가 완화된 수단을 고려할 수 있음.
- 과학기술정보통신부는 실효성이 부재한 사이버재해보험 가입 의무화는 기업에게 과도한 규제로 작용할 수 있으며, 유사 사례 감안 시 의무 가입 규정의 실효성에 대해서도 신중한 검토가 필요하다는 입장임¹⁷⁾.
- 한국인터넷기업협회는 사이버 리스크 관리는 기업이 자체적인 준비금 적립¹⁸⁾, 자율적인 보험 가입, 보안 투자 확대 등 기업의 재무 상황과 리스크 성향에 맞춰 자율적으로 선택해야 할 경영상의 판단이므로, 이를 법률로 일률적으로 강제하는 것은 기업의 경영 자율성을 침해하는 과도한 규제이며, 특히 이미 높은 수준의 보안 투자를 진행하고 있는 기업에게는 이중 비용 부담으로 작용하여 ‘준조세’ 성격의 비용이 될 우려가 있으므로, 의무 가입보다는 기업이 자율적으로 리스크를 관리할 수 있도록 인센티브를 제공하는 방식이 바람직해 보인다는 의견을 제시함.

17) 실제로 유사 보험인 개인정보배상책임보험은 법률로 가입을 의무화하고 있으나, 최근 5년간 실제 보험금 지급 규모는 2억원으로, 보험료 납부액인 약 770억원에 비하면 매우 적은 비율임.

18) 침해사고가 발생하지 않는 경우 자체 준비금은 기업 내부에 적립되고, 이를 보안 시스템 고도화를 위한 투자나 다른 분야의 연구개발 등 기업 성장을 위한 생산적인 분야에 유연하게 재투자할 수 있는 기회를 갖는 반면, 지출한 사이버재해보험료의 경우 고정적인 지출이 되어 기업에게 부담이 갈 수 있다는 의견을 밝힘.

4. 사이버재해보험사업의 운영(제2장)

가. 사이버재해보험심의위원회의 설립(안 제7조)

(1) 제정안 요지

- 사이버재해보험사업에 관한 사항들을 심의하기 위하여 과학기술정보통신부장관 소속으로 사이버재해보험심의위원회(이하 “심의위원회”라 한다)를 둔다(안 제7조 제1항).
- 심의위원회는 위원장 1명과 부위원장 1명을 포함한 15명 이내의 위원으로 구성함. 위원장은 과학기술정보통신부차관이 되고, 부위원장은 위원 중에서 호선(互選)하며, 심의위원회의 구성과 운영에 필요한 사항은 대통령령으로 정함.(안 제7조 제2항부터 제4항까지).

(2) 제정안 조문

제7조(사이버재해보험심의위원회) ① 사이버재해보험사업에 관한 다음 각 호의 사항을 심의하기 위하여 과학기술정보통신부장관 소속으로 사이버재해보험심의위원회(이하 “심의위원회”라 한다)를 둔다.

1. 보험목적물의 범위 조정에 관한 사항
2. 보험가입의무 대상자 지정에 관한 사항
3. 재정지원 대상 및 범위에 관한 사항
4. 손해평가기준에 관한 사항
5. 그 밖에 과학기술정보통신부장관이 부의하는 사항

- ② 심의위원회는 위원장 1명과 부위원장 1명을 포함한 15명 이내의 위원으로 구성한다.
- ③ 위원장은 과학기술정보통신부차관이 되고, 부위원장은 위원 중에서 호선(互選)한다.
- ④ 심의위원회의 구성과 운영에 필요한 사항은 대통령령으로 정한다.

(3) 검토사항

- 안 제7조는 사이버재해보험사업에 대한 사항을 심의하기 위해 과학기술정보통신부장관 소속으로 심의위원회를 두는 것에 대한 근거를 규정하고, 그 밖에 운영 등에 필요한 사항은 대통령령으로 위임하는 규정임.
- 행정안전부는 제7조에 규정된 사이버재해보험심의위원회는 「정보통신망법」 개정안¹⁹⁾들에도 유사한 목적의 위원회 신설 조항이 포함되어 있으므로, 향후 법안 심사 시 신설 추진 위원회 간 통합 또는 분과 및 전문위원회 체계로의 연계를 적극적으로 검토할 필요가 있으며, 아울러, 「행정기관위원회법」 제11조²⁰⁾에 따라 해당 법령 내 5년 이내의 존속기한을 명시할 필요가 있다는 의견을 제시함.

19) 의안번호 2214896, 침해사고조사심의위원회의 설치를 규정한 일부개정법률안

20) 「행정기관위원회법」제11조(위원회의 존속기한) ① 「정부조직법」 제5조에 따라 행정위원회를 설치할 경우 목적 달성을 위하여 필요한 최소한의 기한 내에서 존속기한을 정하여 법률에 명시하여야 한다. 이 경우 존속기한은 5년을 초과할 수 없다.

나. 침해사고의 통지(안 제9조)

(1) 제정안 요지

- 피보험자는 침해사고 발생 사실을 안 날로부터 3일 이내 대통령령으로 정하는 방법과 절차로 보험사업자에게 통지해야 하며, 피보험자가 정당한 사유 없이 통지를 지연한 경우 보험사업자는 그로 인하여 증가된 손해에 대하여는 보상책임을 지지 않게 함(안 제9조).

(2) 제정안 조문

제9조(침해사고의 통지) ① 피보험자는 침해사고 발생 사실을 안 날부터 3일 이내에 보험사업자에게 통지하여야 한다.

② 제1항에 따른 통지의 방법과 절차는 대통령령으로 정한다.

③ 피보험자가 정당한 사유 없이 제1항에 따른 통지를 지연한 경우 보험사업자는 그로 인하여 증가된 손해에 대하여는 보상책임을 지지 아니한다.

(3) 검토사항

- 안 제9조는 피보험자가 평판의 훼손을 우려하여 침해사고가 발생했음에도 이를 은폐하는 것을 막기 위하여 보험사업자에 대한 통지를 의무화하는 규정임.
- 또한, 정당한 사유 없이 통지의 지연이 발생한 경우, 보험사업자의 일부 책임을 면제하여 피보험자의 은폐유인을 감소시킴과 동시에,

보험사업자는 피보험자의 전략적 행동으로 인해 적정 수준보다 더 많은 보상액을 지급해야 할 위험을 감경하는 것으로, 이는 「상법」의 기본적인 체계²¹⁾를 제정안에 도입한 것으로 볼 수 있음.

- 피보험자는 침해사고에 대한 공시를 대외적으로 하는 것이 아닌 보험사업자에게 하는 것이고 통지 내용에 침해사고 발생 사실 외에 발생원인이나 정확한 피해 규모까지 포함하여야 하는 것은 아니므로, 통지를 의무화하더라도 사업자의 대외적인 평판이 심각하게 훼손되거나 부담이 지나치게 가중된다고 보기는 어려운 측면이 있음.
- 다만, 보험은 국제적인 업무의 성격을 갖는바, 국제적으로 통용되는 약관을 사용하는 경우가 많으므로, 법률에서 이와 다르게 규율하는 것이 가져올 파급효과에 대해서도 검토할 필요가 있음.
- 제정안에서는 명시적으로 ‘침해사고 발생 사실을 안 날부터 3일 이내’ 사업자에게 통지할 의무를 규율하는 반면, 국제적으로 통용되는 ISO(Insurance Services Office) 영업배상 책임보험²²⁾(Commercial General Liability) 표준약관에서는 소송이 제기되면 피보험자가 보험자에게 가능한 한 신속히 통지하도록²³⁾ 규정하고 있고, 국내 보험 약관의 경우에도 지체없이라는 용어를 사용하고 있음.

21) 「상법」 제657조(보험사고발생의 통지의무) ① 보험계약자 또는 피보험자나 보험수익자는 보험사고의 발생을 안 때에는 지체없이 보험자에게 그 통지를 발송하여야 한다.

② 보험계약자 또는 피보험자나 보험수익자가 제1항의 통지의무를 해태함으로써 인하여 손해가 증가된 때에는 보험자는 그 증가된 손해를 보상할 책임이 없다.

22) 기업이 영업활동 중 제3자에게 입힌 신체·재산 손해 등에 대한 배상책임을 담보하는 보험

23) 원문 : Notify us as soon as practicable.

「보험 표준약관 및 관련 법률」

제5조(손해의 통지 및 조사) ① 계약자 또는 피보험자는 아래와 같은 사실이 있는 경우에는 지체없이 그 내용을 회사에 알려야 합니다.

1. 사고가 발생하였을 경우 사고가 발생한 때와 곳, 피해자의 주소와 성명, 사고상황 및 이들 사항의 증인이 있을 경우 그 주소와 성명
2. 피해자로부터 손해배상책임에 관한 소송을 제기받았을 경우

② 계약자 또는 피보험자가 제1항 각호의 통지를 게을리하여 손해가 증가된 때에는 회사는 그 증가된 손해를 보상하여 드리지 않으며, 제1항제3호의 통지를 게을리 한 때에는 소송비용과 변호사비용도 보상하여 드리지 않습니다. (이하 생략)

- 따라서 특별한 사정이 없는 한, 일반적으로 통용되는 약관²⁴⁾의 규정을 사용하는 것이 바람직해 보임.
- 한편 정보통신망법 제48조의3²⁵⁾의 ‘즉시’라는 의미란, ‘침해사고가 발생하는 바로 그때’가 아니라 ‘침해사고를 인지한 때’로 볼 수 있고²⁶⁾²⁷⁾, 같은 법 시행령에서도 정보통신서비스 제공자가 침해사고를 신고하려는 경우에는 침해사고의 발생을 알게 된 때부터 24시간 이내에 과학기술정보통신부장관 또는 한국인터넷진흥원에 신고할 의무를 규정하고 있음.
- 따라서 정보통신서비스 제공자가 다른 주체에 비해 침해사고 발생 사실을 보험사업자에게 더 늦게 통지하도록 허용할 만한 특별한

24) 「보험 표준약관 및 관련 법률」 제5조(손해의 통지 및 조사) ① 계약자 또는 피보험자는 아래와 같은 사실이 있는 경우에는 지체없이 그 내용을 회사에 알려야 합니다.

1. 사고가 발생하였을 경우 사고가 발생한 때와 곳, 피해자의 주소와 성명, 사고상황 및 이들 사항의 증인이 있을 경우 그 주소와 성명
2. 피해자로부터 손해배상책임에 관한 소송을 제기받았을 경우

② 계약자 또는 피보험자가 제1항 각호의 통지를 게을리하여 손해가 증가된 때에는 회사는 그 증가된 손해를 보상하여 드리지 않으며, 제1항제3호의 통지를 게을리 한 때에는 소송비용과 변호사비용도 보상하여 드리지 않습니다. (이하 생략)

25) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다.

26) KISA, 침해사고 신고 안내서

<https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000127&nttId=27050&menuNo=205021>

27) 현재 정보통신망법 제48조의3제1항 전단 중 “즉시 그 사실”을 “그 침해사고의 발생 사실을 알게 된 때부터 24시간 이내에 침해사고의 발생 일시 및 대응 현황 등 대통령령으로 정하는 사항”으로 하는 개정안이 현재 과학기술정보통신위원회 전체 회의에서 의결되었으며, 현재 법제사법위원회에서 계류 중임.

사정이 없는 한, 정보통신망법 시행령에서 정하고 있는 ‘24시간 이내’의 통지 규정과 정합성을 맞추는 것이 바람직함.

- 손해보험협회는 정보통신망법에서 규정된 신고 기한을 일치시킬 필요가 있으므로, ‘3일’이라는 문구를 ‘24시간 이내’로 수정하는 것이 바람직하다는 의견을 제시함.

손해보험협회 수정 의견

개 정 안	수 정 안
제9조(침해사고의 통지) ① 피보험자는 침해사고 발생 사실을 안 날부터 <u>3일</u> 이내에 보험사업자에게 통지하여야 한다.	제9조(침해사고의 통지) ① 피보험자는 침해사고 발생 사실을 안 날부터 <u>24시간</u> 이내에 보험사업자에게 통지하여야 한다.

- 한국인터넷기업협회는 고도화된 사이버 공격의 특성상 사고 발생 초기에는 원인분석과 피해 규모 파악에 상당한 시일이 소요되므로 침해사고 사실을 안 날로부터 3일 이내에 보험사에 통지하도록 의무화하는 것은 기업에 과도한 부담이 될 수 있으며, 오히려 성급한 신고로 인해 부정확한 정보 전달이 일어날 수 있으므로 신중한 검토가 필요하다는 견해를 밝힘.

다. 사이버재해보험료율의 산정(안 제10조)

(1) 제정안 요지

- 보험료율 산정 시 보험목적물의 위험도, 피보험자의 보안 수준, 사이버위험지표 등을 반영하도록 기준을 마련함(안 제10조).

(2) 제정안 조문

제10조(보험료율의 산정) ① 보험사업자는 사이버재해보험의 보험료율을 다음 각 호의 기준에 따라 산정하여야 한다.

1. 「보험업법」 제129조에 따른 보험료율 산출원칙의 준수
2. 보험목적물의 위험도에 따른 차등적용
3. 제22조에 따른 사이버위험지표의 반영
4. 피보험자의 보안 수준 및 침해사고 이력

② 제1항에 따른 보험료율 산정의 구체적 기준과 방법은 대통령령으로 정한다.

(3) 검토사항

- 안 제10조는 보험료율 산정 시 보험목적물 위험도, 피보험자 보안 수준, 사이버 위험지표 등을 반영하고, 과기정통부장관이 위험지표 작성 및 전산체계 구축을 하도록 하여 위험평가 인프라를 제도화하는 것을 목적으로 함.
- 현재, 국내 사이버재해보험 활성화를 위해 보험개발원 및 보험사 등이 리스크 산출 모델, 비용 추정 모델링 연구 용역을 추진 중이며, 「사이버 침해사고의 경제·사회적 비용추적 연구」가 2026년 상반기까지 진행 중임.
- 보험료율 산정, 사이버위험지표 및 손해평가 기준은 제도 설계의 핵심 요소인

바, 특히 보험 가입을 의무화하는 경우에는 관련된 인프라의 구축 수준을 고려하여 시행 초기의 혼선과 이행 부담을 최소화할 필요가 있음.

- 따라서, 현재 민간에서 관련 연구가 진행 중인 점을 고려할 때, 경과규정을 두어 시행 시점을 합리적으로 조정하거나, 시범사업을 거쳐 적용 대상을 단계적으로 확대하는 등 점진적 도입 방안을 함께 검토할 수 있음.
- 한편, 보험료율 산정의 자율성 확보를 위해 강행 규정을 임의 규정으로 완화하는 것도 고려할 수 있음.
- 사이버재해보험법 제10조의 규정은 「풍수해·지진재해보험법」²⁸⁾의 틀을 빌려온 것으로 보임.
- 그러나 유형이 상대적으로 한정된 풍수해 및 지진재해와는 달리, 사이버 재해의 경우 기술의 발전과 더불어 새로운 유형의 재해가 지속적으로 발생할 가능성이 높음. 즉 새로운 유형의 사고가 발생했을 때, 각 유형의 특수성을 반영하여 보험료율 산정을 할 필요성이 있으나, 위와 같이 강행규정²⁹⁾으로 규율하는 경우, 보험료율 산정의 자율성이 제한되어 대응이 경직적으로 될 우려가 있음.
- 특히 사이버재해보험 시장은 다른 보험 시장과는 달리 보험가입자의 표본이 매우 부족하고³⁰⁾, 단 한 번의 비정형적 사고가 발생하는 경우 보험회사의

28) 「풍수해·지진재해보험법」 제11조(보험료율의 산정) 보험사업자는 풍수해·지진재해보험의 보험료율을 객관적이고 합리적인 통계자료를 기초로 하여 다음 각 호의 기준에 따라 산정하여야 한다.

1. 「보험업법」 제129조에 따른 보험료율 산출의 원칙을 적용할 것

2. 개별 보험목적물의 피해 발생 빈도에 따라 보험료율을 다르게 적용할 것

3. 제25조제1항에 따른 풍수해·지진재해보험관리지도에 표시된 위험 정도에 따라 지역별로 보험료율을 다르게 적용할 것

29) 「사이버재해보험법」 제10조제1항에 제5호를 추가하여 ‘기타 대통령령으로 정하는 사항’ 등으로 규율하는 방법도 있으나, 이 또한 경직성을 효과적으로 해결할 수 있을지 논의할 필요성이 있음.

30) 통상적으로 몇 천 ~ 몇 만 정도의 표본이 필요함.

재무건전성이 크게 훼손될 수 있을 정도로 위험도가 상당히 높은 영역임.

- 이러한 시장의 특수성을 고려할 때, 보험사업자에게 보험료율 산정에서의 자율성을 제약하는 경우, 보험사업자가 사이버재해보험시장에 참여할 유인이 감소할 수 있음. 따라서 사이버재해보험시장의 활성화라는 입법 취지를 살리기 위해선 어느 정도의 보험료율 산정의 자율성을 보장할 필요가 있음.
- 손해보험협회는 강행 규정으로 법안이 제정될 경우 새로운 보험사고 유형이 계속 발생하고 있는 사이버보험 특성을 고려할 때 보험료율 산정의 자율성이 제한될 우려가 있으므로, 강행 규정이 아닌 임의 규정으로 완화가 필요하다는 의견을 제시함.
- 금융위원회는 「보험업법」 제129조³¹⁾에 따라 보험회사는 보험료율을 산출할 때 객관적이고 합리적인 통계자료를 기초로 대수(大數)의 법칙 및 통계 신뢰도를 바탕으로 하여야 하므로, 제정안의 제10조 제1항제2호 내지 제4호³²⁾가 객관적이고 합리적인 수준의 통계 신뢰도 등을 갖춘 경우에만 보험료율에 반영할 수 있다는 의견을 밝힘.

31) 「보험업법」 제129조(보험료율 산출의 원칙) 보험회사는 보험료율을 산출할 때 객관적이고 합리적인 통계자료를 기초로 대수(大數)의 법칙 및 통계신뢰도를 바탕으로 하여야 하며, 다음 각 호의 사항을 지켜야 한다.

1. 보험료율이 보험금과 그 밖의 급부(給付)에 비하여 지나치게 높지 아니할 것
2. 보험료율이 보험회사의 재무건전성을 크게 해칠 정도로 낮지 아니할 것
3. 보험료율이 보험계약자 간에 부당하게 차별적이지 아니할 것
4. 자동차보험의 보험료율인 경우 보험금과 그 밖의 급부와 비교할 때 공정하고 합리적인 수준일 것

32) 「사이버재해보험법」 제10조(보험료율의 산정) ① 보험사업자는 사이버재해보험의 보험료율을 다음 각 호의 기준에 따라 산정하여야 한다.

2. 보험목적물의 위험도에 따른 차등적용
4. 피보험자의 보안 수준 및 침해사고 이력

라. 보험가입 촉진 및 보험료 지원(안 제19조 및 제20조)

(1) 제정안 요지

- 정보통신서비스 제공자의 보험가입 촉진을 위한 정부의 교육·홍보 및 가입자에 대한 정책자금지원 및 신용보증 지원 근거 마련(안 제 19조).
- 중소기업 또는 소상공인의 사이버재해보험료에 대한 정부의 보험료 일부 지원에 대한 법적 근거를 마련함(안 제 20조).

(2) 제정안 조문

제19조(보험가입의 촉진 등) 정부는 정보통신서비스 제공자의 사이버재해보험의 가입을 촉진하기 위하여 교육·홍보 및 보험가입자에 대한 정책자금 지원, 신용보증 지원 등을 할 수 있다.

제20조(보험료 지원) ① 정부는 「중소기업기본법」 제2조에 따른 중소기업 또는 「소상공인기본법」 제2조에 따른 소상공인이 사이버재해보험에 가입하는 경우 예산의 범위에서 보험료의 일부를 지원할 수 있다.

② 제1항에 따른 지원대상, 지원범위 및 지원절차 등에 필요한 사항은 대통령령으로 정한다.

(3) 검토사항

- 안 제19조 및 제20조는 정보통신서비스 제공자의 사이버재해보험 가입을 촉진하기 위하여 교육·홍보, 정책자금·신용보증 지원 및 보험료 일부 지원을 가능하게 하는 규정으로, 사이버재해의

사회·경제적 파급효과를 고려할 때 사전적 위험관리 및 사후적 피해 구제 기반을 확충하려는 정책수단으로써 입법 취지의 정당성이 인정됨.

- 특히 중소기업·소상공인은 사이버재해에 상대적으로 취약하고³³⁾, 침해사고 발생 시 재무적 충격을 자체적으로 흡수할 여력이 제한적이므로, 보험료 지원 등을 통해 보험 접근성을 제고하여 사이버재해보험시장의 초기 형성 단계에서 가입 장벽을 낮추는 효과를 기대할 수 있음.
- 다만 보험료 지원이 보안 투자를 대체하는 방식으로 작동할 경우, 기업이 법적 책무인 정보보호 조치를 강화하기보다 보험에 의존하게 되는 도덕적 해이가 발생할 우려가 있음.
- 따라서 보험료 지원이 기업의 정보보호 의무 이행 유인을 약화하지 않도록, 지원요건을 보안 수준과 연동하고 지원 수준을 차등적으로 규율하는 방안을 고려할 필요가 있음.
- 과학기술정보통신부는 정부의 사이버재해보험료 일부 지원은, 법적 책무인 정보보호에 대한 기업의 자발적인 노력을 저해할 수 있으므로 신중한 검토가 필요하다는 의견을 제시함.

33) 권순일·한진현, 「사이버 리스크 실태와 과제」, 보험연구원, 2025.5.26

5. 사이버재해보험사업의 지원(제3장)

가. 보험계약 체결 전 실사(안 제21조)

(1) 제정안 요지

- 보험사업자가 보험계약 체결 전에 보험목적물의 보안 수준을 조사할 수 있도록 하며, 조사결과를 보험료율 산정에 반영할 수 있도록 함 (안 제 21조).

(2) 제정안 조문

제21조(보험계약 체결 전 실사) ① 보험사업자는 보험계약 체결 전에 보험 목적물의 보안 수준을 조사할 수 있다.

② 제1항에 따른 조사를 받는 자는 정당한 사유가 없으면 이에 협조하여야 한다.

③ 보험사업자는 제1항에 따른 조사결과를 보험료율 산정에 반영할 수 있다.

(3) 검토사항

- 사이버재해는 사고 발생 가능성과 손해 규모가 보험목적물의 보안 수준, 운영 환경, 관리체계에 따라 유의미하게 달라지는 특성을 가지므로, 보험계약 체결 시 해당 위험을 사전에 평가할 필요성이 인정됨. 특히 일정 규모 이상의 정보통신서비스 제공자에 대해 보험 가입을 의무화하는 제정안의 특성상, 개별 사업자의 보안 수준 차이가 보험료에 충분히 반영되지 않는 경우

교차 보조(cross-subsidization)³⁴⁾ 문제가 발생할 수 있음³⁵⁾.

- 따라서 안 제21조는 보험사업자가 보험계약 체결 전에 보험목적물의 보안 수준을 조사할 수 있도록 명시적 근거를 두어 위험 기반 보험료 산정(risk-based pricing)이 가능하도록 하는 제도적 장치로 평가됨.
- 아울러, 보험사업자는 사전에 피보험자의 보안 수준을 인지한 상태에서 계약을 체결하게 되고, 피보험자는 계약 당시의 보안 상태와 보험조건 간의 관계를 명확히 인식하게 되어, 사고 발생 후 담보 범위나 면책 여부를 둘러싼 분쟁 가능성을 줄일 수 있음.
- 나아가, 정보통신서비스 제공자의 입장에서는 보안 조치를 강화하는 것이 곧 보험료 부담 감소로 이어지는바, 시장 메커니즘을 통해 자율적인 투자를 유도하여 보안 수준을 향상하는 긍정적 효과를 가져올 수 있음.
- 다만, 보험회사는 보험료율을 조정할 수 있을 뿐, 보험목적물의 보안 수준이 현저히 낮다는 이유만으로 특정 기업의 보험 가입을 거절할 수 없음. 이 경우 보안 수준이 낮은 기업은, ‘보안 개선에 따른 비용 부담’보다, 높은 보험료를 부담하더라도 ‘침해사고 발생 시 수령 가능한 보험금’이 더 크다고 판단할 경우 보안 수준을 높이기보다는 사이버재해보험 가입을 선택할 유인이 발생할 수 있음.

34) 위험이 낮은 집단이 위험이 높은 집단의 비용을 사실상 대신 부담하게 되는 현상. 즉 위험이 낮은 집단이 상대적으로 더 높은 비용을 부담하고, 이는 저위험 기업들의 보험가입 유인을 줄이고, 고위험 기업들의 보험가입 유인을 높이는 ‘역선택’ 현상이 발생하게 됨.

35) Einav, L. & Finkelstein, A. (2011). Selection in Insurance Markets: Theory and Empirics in Pictures. Journal of Economic Perspectives, 25(1), 115-13

- 이와 같은 유형의 기업에서 사이버 침해사고가 발생하는 경우, 보험사업자는 매우 큰 재정적 손실을 보게 되고, 이를 우려하여 보험사업자들이 사이버 재해보험시장에 진입하는 것을 주저하게 될 수 있음. 즉 보험료를 조정만으로는 이러한 선택 구조를 충분히 교정하기 어려워, 역선택 및 도덕적 해이를 효과적으로 예방하기 어려운 측면이 있음.
- 이를 해결하기 위해 보험사업자에게 일정한 요건 하에서의 보험인수를 거절하거나 가입조건을 제한하는 근거를 법률에 명시하는 방안을 고려할 수 있음.
- 손해보험협회는 안 제21조는 보험사업자에게 보험계약 체결 전 보험목적물의 보안 수준을 조사할 수 있는 권한을 부여하고 있으나, 보안 수준이 미흡할 경우의 후속 조치는 보험료를 반영에만 한정되므로, 조사 결과 보안 수준이 미흡한 경우 보험인수를 거절하거나 가입조건을 제한하는 근거를 명시함으로써 역선택을 통한 보험사의 재무건전성 악화를 방지하고, 기업의 자발적 보안 수준 향상을 유도하는 방안을 고려할 수 있다는 의견을 제시함.

나. 사이버위험지표의 작성(안 제22조)

(1) 제정안 요지

- 과학기술정보통신부장관은 과거 침해사고 발생 이력, 발생 위험도 등을 고려한 사이버위험지표³⁶⁾를 작성하고 관련 전산체계를 구축·관리

36) 사이버재해 위험 정도를 업종별·규모별 등의 단위로 표시하는 지표로 과기정통부 장관이 3년마다 타당성을 검토 후 정비

하도록 규정함(안 제22조제1항).

- 위험지표의 작성 방법을 과학기술정보통신부장관이 관계 기관과 협의하여 정하도록 하고(안 제22조제2항), 3년마다 지표의 타당성을 재검토 및 정비할 의무를 규율하며(안 제22조제3항), 보험사업자는 과학기술정보통신부장관에게 사이버위험지표의 이용을 요청할 수 있도록 함(안 제22조제4항).

(2) 제정안 조문

제22조(사이버위험지표의 작성) ① 과학기술정보통신부장관은 침해사고 예방과 사이버재해보험사업의 적절한 운영을 위하여 과거의 침해사고 발생 이력 및 향후 발생 위험 등을 고려하여 사이버재해 위험 정도를 업종별·규모별로 표시하는 지표(이하 “사이버위험지표”라 한다)를 작성하고 이를 통합·관리할 수 있는 전산체계를 구축·관리하여야 한다.

② 사이버위험지표의 작성 단위·내용 등 작성 방법에 관하여 필요한 사항은 과학기술정보통신부장관이 관계 기관과 협의하여 정한다.

③ 과학기술정보통신부장관은 제1항에 따라 작성된 사이버위험지표에 대하여 3년마다 그 타당성을 전반적으로 재검토하여 이를 정비하여야 한다.

④ 보험사업자는 사이버재해보험료율과 보험가입금액의 산정 등을 위하여 과학기술정보통신부장관에게 사이버위험지표의 이용을 요청할 수 있다.

(3) 검토사항

- 안 제22조제1항은 침해사고 예방 및 사이버재해보험사업의 적절한 운영을 위하여, 과거 침해사고 발생 이력 및 향후 발생 위험 등을 고려하여 업종별·규모별 사이버재해 위험 정도를 표시하는

‘사이버위험지표’를 과학기술정보통신부장관이 작성하고 이를 관리하도록 하는 규정임.

- 사이버재해는 업종·규모에 따라 노출되는 위험의 양태와 사고 발생 시 파급효과가 상이하고, 보험의 위험평가 및 요율 산정에 필요한 정보가 민간영역에 분산된 경우가 많아 정보 비대칭이 발생하기 쉬운 영역임.
- 이러한 특성을 고려할 때, 공적 기관이 업종·규모별 위험 수준을 체계적으로 산정·제시함으로써 보험자·피보험자 간 정보 비대칭을 완화하고, 보험료 산정의 객관성과 비교 가능성을 높여 제도의 실효성을 확보할 수 있음.
- 한편, 과학기술정보통신부장관이 위험지표의 작성 방법을 관계 기관과 협의하여 정하도록 하고(제2항), 3년마다 지표의 타당성을 전반적으로 재검토 및 정비하도록 하여(제3항) 산정기준의 합리성과 최신성을 확보할 장치를 두고 있으며, 보험사업자는 지표의 이용을 요청할 수 있도록 규정함(제4항).
- 이는 지표를 보험료율 산정의 유일한 기준으로 규율하기보다는 참고자료로 활용될 여지를 남기고 있는 점에서, 제도의 경직성을 완화하려는 취지로 볼 수 있음.
- 다만, 사이버재해는 비정형적인 형태를 띠고, 사이버위험지표 및 보안 수준 평가는 보험료율 산정 등 제도 운용에 직접 연계될 수 있으므로, 평가 체계가 다양한 IT 환경에서도 합리적으로 작동할 수

있도록 기술 중립성과 설명 가능성을 갖출 필요가 있음.

- 가령 현재 금융권 등에서 통용되는 통제 중심의 전통적 보안 평가 기준은 망분리³⁷⁾, 엄격한 접근 통제 등 물리적·절차적 통제의 이행 여부에 초점을 두는 경향이 있어, 신속한 배포와 유연성을 중시하는 정보통신서비스 제공자의 운영방식과 정합적이지 않을 수 있음.
- 특히 인터넷·모바일 기업 등 정보통신서비스 제공자는 기존의 망분리 같은 경계 기반의 물리적 통제 프레임과 구조가 상이한³⁸⁾ 경우가 많으며, 제로 트러스트³⁹⁾ 등의 다른 방식으로 보안 수준을 달성하기도 함.
- 실제로 망분리 규제는 금융시스템 보호에 기여⁴⁰⁾한 측면이 있으나, 디지털 신기술⁴¹⁾ 채택의 장애 요인으로 작용한다는 문제의식이 제기되어 왔었음⁴²⁾.
- 이처럼 통제 방식이 상이하더라도 결과적으로 유사한 수준의 보안 효과를 달성할 수 있음에도 불구하고, 평가 체계가 특정 수단(망 분리) 충족 여부에 과도하게 의존할 경우 보안 성숙도가 높은 기업이 오히려 보안 수준이 낮은 기업으로 분류되는 일이 발생할 수 있음⁴³⁾.
- 따라서 전통적 통제 위주의 평가 기준을 위험지표 및 보험료 산정에

37) 외부 침입으로부터 내부 전산자원을 보호하기 위해 내부망과 외부망을 분리하는 네트워크 보안기법의 일종

38) SaaS(Software as a Service)·퍼블릭 클라우드 환경에서는 물리적 망분리의 구현이 곤란함.

39) 네트워크와 관계없이 기본적으로 어떠한 것도 '신뢰하지 않는' 방어적 보안 개념

40) 전 세계가 2017년 랜섬웨어 감염사고로 피해를 입었음에도 국내 금융권은 피해가 없었음.

41) 인터넷 연결을 통한 오픈소스 활용이 필수적임.

42) [금융위원회 보도자료] 변화된 IT환경의 망분리 규제 합리화를 위한 「금융부문 망분리 T/F」 1차 회의 개최, 금융안전과, 2024-04-12, <https://www.fsc.go.kr/no010101/82108?utm>

43) 매일 수십 번의 코드 업데이트가 일어나는 애자일 환경에서는 '사전 승인' 중심의 전통적 보안 통제가 불가능함. 대신 자동화된 보안 검사(DevSecOps)를 수행함에도 불구하고, 수동 결재 라인 부재나 문서화된 이력 부족을 이유로 보안 수준이 낮게 평가될 우려가 있음

적용함에 있어 발생할 수 있는 부작용을 충분히 고려하고, 민간의 다양한 IT 환경을 반영할 수 있는 평가체계를 정교하게 설계하는 방안이 필요함.

- 한국인터넷기업협회는 현행 금융권 등에서 주로 통용되는 통제 위주의 전통적 보안 평가 기준은 망 분리, 엄격한 접근 통제 등 물리적·절차적 통제에 집중되어 있는바, 이는 신속한 배포와 유연성을 중시하는 인터넷·모바일 기업의 최신 IT 환경⁴⁴⁾과 근본적으로 배치되며, 이러한 최신 개발 환경의 특수성을 고려하지 않고 획일적인 ‘사이버 위험지표’를 적용할 경우 기술적 혁신을 추구하는 기업들이 오히려 보안 수준이 낮은 것으로 오인되어 부당하게 높은 보험료를 부담하거나 가입을 거절당하는 불이익을 받을 수 있으므로, 민간의 다양한 IT 환경을 반영할 수 있는 평가 체계가 선행되지 않은 상태에서 성급한 입법은 지양되어야 한다는 의견을 제시함.

문 의 처
02)6788-5228

44) Agile, DevOps, MSA 등

※ 참고자료

1. 개인정보 보호법 시행령 [별표 1의4]

■ 개인정보 보호법 시행령 [별표 1의4] <개정 2024. 3. 12.>

손해배상책임의 이행을 위한 최저가입금액(최소적립금액)의 기준(제48조의7제4항 관련)

가입대상개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)
정보주체 수	매출액등	
100만명 이상	800억원 초과	10억원
	50억원 초과 800억원 이하	5억원
	10억원 이상 50억원 이하	2억원
10만명 이상 100만명 미만	800억원 초과	5억원
	50억원 초과 800억원 이하	2억원
	10억원 이상 50억원 이하	1억원
1만명 이상 10만명 미만	800억원 초과	2억원
	50억원 초과 800억원 이하	1억원
	10억원 이상 50억원 이하	5천만원

비고: 이 표에서 “매출액등”이란 제31조의2제1항제1호에 따른 매출액등을 말한다.

2. 과학기술정보통신부 의견

정보보호기획과장 지은경(☎ 044-202-6440)

□ 우리부 입장 : **신중검토**

- 침해사고 발생 시 피해기업과 정보통신망 이용자에게 신속하고 실질적인 손해를 보상하는 사이버재해 보험 활성화에 공감하나, 보험 가입 의무화 등 법제화는 신중 검토 필요

< 총괄 >

- 현행 「보험업법」 체계 하에서도 일부 국내 보험사는 사이버사고 종합보험을 판매*하고 있는 등 별도 법 제정이 필수는 아님

* 삼성사이버종합보험(삼성화재), 사이버종합보험(DB 손해보험), 사이버프로텍션보험(한화손해보험) 등

- 해외의 경우에도 사이버재해보험 관련 입법사례는 부재하며, 막대한 과징금(미국, EU), 집단 소송을 통한 대규모 보상(미국) 등 리스크 관리를 위해 민간에서 자발적으로 사이버재해보험 가입
- 국내 사이버재해보험 활성화를 위해, 보험개발원, 보험사 등이 보험료 산정에 참고할 수 있는 리스크 산출 모델, 비용 추정 모델링 등 연구 용역 추진 중

※ 「사이버 침해사고의 경제·사회적 비용추적 연구」 용역(~'26.上)

< 세부내용 >

- (제4조) 사이버재해보험 가입 의무화는 실효성이 부재하면 기업에게 규제로 작용할 수 있으며, 유사 사례* 감안 시 의무 가입 실효성에 대해서도 신중 검토 필요

* 유사 보험인 개인정보배상책임보험(개보위 소관)은 법률로 가입을 의무화하고 있으나, 최근 5년간 실제 보험금 지급 규모는 2억원(보험료 납부는 약 770억원)에 불과

- (제20조) 정부의 사이버재해 보험료 일부 지원은, 법적 책무인 정보보호에 대한 기업의 자발적인 노력을 저해할 수 있으므로 신중 검토 필요

□ 부처별 의견 (부처 의견조회, '25.12.23.~'26.1.5.)

- (행안부) 제7조 사이버재해보험심의위원회는 「정보통신망법」 개정안들에도 유사한 목적의 위원회 신설 조항이 포함되어 있으므로,
 - 향후 법안 심사 시 신설 추진 위원회 간 통합 또는 분과 및 전문위원회 체계로의 연계를 적극 검토
 - 아울러, 「행정기관위원회법」 제11조에 따라 해당 법령 내 5년 이내의 존속기한 명시 필요

3. 금융위원회 의견

< 검토의견 : 이견 없음 >

□ 정책성 보험은 정책목적을 달성하기 위해 개별 법률에 근거를 두고 해당 법률 소관부처에서 운영 중.

- 정책성 보험의 구체적 운영방식(의무가입 여부 등)은 정책목적을 고려하여 국회 논의 등을 거쳐 소관부처가 자율적으로 정할 사항.

□ 다만, 「보험업법」 제129조에 따라 보험회사는 보험료를 산출할 때 객관적이고 합리적인 통계자료를 기초로 대수(大數)의 법칙 및 통계 신뢰도를 바탕으로 하여야 하므로,

- 제정안 제10조제1항*제2호 내지 제4호가 객관적이고 합리적인 수준의 통계신뢰도 등을 갖춘 경우에만 보험료율에 반영할 수 있음.

* 1. 「보험업법」 제129조에 따른 보험료율 산출원칙의 준수

2. 보험목적물의 위험도에 따른 차등적용

3. 제22조에 따른 사이버위험지표의 반영

4. 피보험자의 보안 수준 및 침해사고 이력

4. 손해보험협회 의견

(☎ 02-3702-8696)

① 사고 통지 의무의 실효성 제고(3일→24시간 이내로 수정 필요)

- 법안 제9조 제1항에 따르면 피보험자는 침해사고 발생 사실을 안 날로부터 3일 이내에 보험사업자에게 통지하게 되어 있으나, 현재 정보통신망법에서 기업은 침해사고 발생시 24시간 이내에 과기부 장관 또는 한국인터넷진흥원에 신고하게 되어 있으므로 이와 신고 기한 등을 일치시킬 필요.

② 보험요율 산정에 대한 자율성 확보 필요

- 법안 제10조 제1항에 따르면 보험사업자는 ‘보험료율을 각호의 기준에 따라 산정해야 한다’고 규정.
- 현행과 같은 강행 규정으로 법안이 제정될 경우 새로운 보험 사고 유형이 계속 발생하고 있는 사이버 보험 특성을 고려할 때 보험 요율 산정의 자율성이 제한될 우려가 존재.
- 요율산정의 자율성 확보를 위해 강행 규정이 아닌 임의 규정으로 완화 필요.

③ 사업 중단 손해(제2조 제1항 제2호 나목)의 법령상 명확한 정의 필요

- 사이버 리스크 특성 상 손해의 경계가 모호하여, 보험사고로 인한 사업중단손해가 어떤 손해까지 의미하는지에 대한 의견 차이 발생 가능.
- 예컨대, 해킹피해로 인해 사이트 운영이 일시 중지된 쇼핑몰의 경우 사업 중단 손해가 직원 인건비 등 고정비용인지, 매출 손실까지 포함하는지 불명확.
- 법령상 사업 중단 손해에 대한 명확한 정의를 신설함으로써 기업이 의무적으로 가입해야 하는 보험에 대한 불확실성 해소 필요.

④ 건전성 제고를 위한 인수 거절권 명시

- 법안 제21조는 보험사업자에게 보험계약 체결 전 보험목적물의 보안 수준을 조사할 수 있는 권한을 부여하고 있으나, 조사 결과가 미흡할 경우의 후속 조치는 보험료를 반영에만 한정.
- 조사 결과 보안 수준이 미흡한 경우 보험인수를 거절하거나 가입 조건을 제한하는 근거를 명시함으로써 역선택을 통한 보험사의 재무 건전성 악화를 방지하고 기업의 자발적 보안 수준 향상을 유도.

5. 한국인터넷기업협회 의견

□ (안 제4조 관련) 보험 가입 의무화에 따른 기업자율성 침해 및 재정 부담이 가중됨.

- 본 법안 제4조 보험가입의무는 매출액 및 이용자 수 등을 기준으로 일정 규모 이상의 정보통신서비스 제공자에게 보험을 강제하고 있으며, 미가입시 제31조에 따라 과태료를 부과하도록 규정하고 있음.
- 사이버 리스크 관리는 기업이 자체적인 준비금 적립, 자율적인 보험 가입, 보안 투자 확대 등 기업의 재무 상황과 리스크 성향에 맞춰 자율적으로 선택해야 할 경영상의 판단으로 보임.
- 그럼에도 불구하고 이를 법률로 일률적으로 강제하는 것은 기업의 경영 자율성을 침해하는 과도한 규제라고 사료됨.
- 특히 이미 높은 수준의 보안 투자를 진행하고 있는 기업에게는 이중 비용 부담으로 작용하여 ‘준조세’ 성격의 비용이 될 우려가 큼으로 의무 가입보다는 기업이 자율적으로 리스크를 관리할 수 있도록 인센티브를 제공하는 방식이 바람직해보임.

□ (안 제5조 관련) 보험 목적물의 광범위성과 불명확성으로 인한 과도한 보험료 산정 우려가 있음.

- 본 법안 제5조는 보험의 대상을 개인정보 처리 시스템, 전자상거래 플랫폼, 클라우드, IoT 기기 등으로 규정하고 있으며, 제6호에서 ‘대통령령으로 정하는 정보자산’ 까지 포함하여 그 범위를 매우 포괄적으로 설정하고 있음.

- 법안이 정의하는 ‘정보자산’의 범위가 광범위하고 모호한데, 사이버 자산(데이터, 소프트웨어 등)은 물리적 자산과 달리 객관적인 가치 평가가 매우 어려워 포괄적으로 보험목적물로 지정할 경우, 리스크 평가가 보수적으로 이루어져 보험료가 과도하게 책정될 가능성이 높음.
- 클라우드, 데이터베이스, IoT 기기 등 성격이 상이한데 포괄적으로 보험목적물로 지정하고 있음.
- 나아가 사고 발생시 보상범위에 대한 해석 차이로 인해 불필요한 분쟁이 발생할 소지가 높기 때문에 보험 목적물의 범위를 더욱 구체적이고 한정적으로 명시해야함.

□ (안 제9조 관련) 침해사고 사실을 안 날로부터 3일 이내 보험사에 통지하도록 의무화하는 것은 현실성이 낮음.

- 안 제9조는 침해사고 사실을 안 날로부터 3일 이내 보험사에 통지하도록 의무화하고 있으며 지연 시 보상 책임을 면제할 수 있게 되어 있으나, 고도화된 사이버 공격(APT 등)의 특성상 사고 발생 초기에는 원인분석과 피해 규모 파악에 상당한 시일이 소요됨.
- 3일이라는 물리적인 시간 제한은 기업에게 과도한 부담이 될 수 있으며 성급한 신고로 인해 오히려 기업의 대외 신뢰도 하락이나 부정확한 정보 전달을 초래할 수 있어 신중한 검토가 필요함.

□ (안 제10조, 제21조, 제22조 관련) 다양한 성격의 IT 환경을 반영할 수 있는 평가 체계의 선행이 필요함.

- 안 제10조 및 제22조에 따르면, 과학기술정보통신부가 관리하는 위험지표와 피보험자의 보안 수준을 반영하여 보험료를 산정하도록 되어 있음. 또한 제21조에 따라 보험 계약전 보안 수준 실사가 가능함.
- 현행 금융권 등에서 주로 통용되는 통제 위주의 전통적 보안 평가 기준은 망분리, 엄격한 접근 통제 등 물리적·절차적 통제에 집중되어 있음. 이는 신속한 배포와 유연성을 중시하는 인터넷·모바일 기업의 최신 IT 환경(Agile, DevOps, MSA 등)과 근본적으로 배치됨.
- 이러한 최신 개발 환경의 특수성을 고려하지 않고 획일적인 ‘사이버위험지표’를 적용할 경우 기술적 혁신을 추구하는 기업들이 오히려 보안 수준이 낮은 것으로 오인되어 부당하게 높은 보험료를 부담하거나 가입을 거절당하는 불이익을 받을 수 있음.
- 따라서 민간의 다양한 IT 환경을 반영할 수 있는 평가 체계가 선행되지 않은 상태에서의 성급한 입법은 지양해야 할 것으로 사료됨.

6. 한국인터넷기업협회 추가 의견

□ (안 제4조) 기업의 자체적인 준비금 적립과, 사이버재해보험 의무가입 간에 차이

- 기업의 자체 준비금 적립과 의무 보험 가입은 자금의 법적 성격과 경제적 활용도 측면에서 근본적인 차이가 있음.
- 자체 준비금은 기업 내부에 적립되어 관리되는 '자산'의 성격을 가짐. 만약 우려하던 침해사고가 발생하지 않는다면, 이 자금은 외부로 유출되거나 소멸하지 않고 그대로 기업의 자본으로 보존됨.
- 따라서 기업은 상황에 따라 이 자금을 보안 시스템 고도화를 위한 투자나 R&D(연구개발) 등 기업 성장을 위한 생산적인 분야에 유연하게 재투자할 수 있는 기회를 갖게 됨.
- 하지만 사이버재해보험료는 지출 즉시 효용이 사라지는 '매몰 비용(Sunk Cost)'에 해당함. 사고가 발생하지 않을 경우 납부된 보험료는 기업에게 어떠한 잔존 가치도 남기지 않은 채 순수한 비용 손실로 귀결됨.
- 특히 본 법안 제4조는 대상 기업에게 보험 가입을 강제하고 매년 계약을 갱신하도록 규정하고 있어, 기업 입장에서는 소멸성 비용을 영구적인 고정 비용으로 떠안아야 하는 과도한 재무적 부담이 발생하게 됨.

□ (안 제5조) 보험목적물의 범위의 구체적/한정적 예시

- 제1항/2항의 경우 목적성과 범위가 명확하다고 볼 수 있으나, 3항/4항 등은 목적성/범위가 명확하지 않아 구체적/한정적으로 명시할 필요가 있음.

- 제3항 클라우드컴퓨팅서비스 및 데이터베이스, 4항 사물인터넷 기기 및 스마트 기기의 경우 기업의 전체 서비스가 대상이 될 수 있음에 반해, 침해사고 발생 시 기업 운영에 영향이 미미한 대상까지 포함될 수 있음.
- 제3항 클라우드컴퓨팅서비스 및 데이터베이스 : 테스트/개발 서버, 단순 아카이빙 및 로그 저장소, 단순 정보성 사내 인트라넷 서비스
- 제4항 사물인터넷 기기 및 스마트기기 : 단순 전시 및 홍보용 디스플레이 장치, 테스트 모바일 및 사물인터넷 기기

□ (안 제9조) 한국인터넷진흥원에 통지와 보험회사에 통지 차이

- 기관 신고와 민간 보험사에 대한 통지는 그 근본적인 목적과 파급 효과에서 명확한 차이가 있음. 이는 단순히 행정 절차가 하나 더 늘어나는 차원을 넘어, 기업 경영에 심각한 리스크로 작용할 우려가 있음.
- 첫번째는 공익적 목적과 사적 계약의 차이임. 정부에 대한 신고가 피해 확산 방지와 원인 분석이라는 공익적 목적을 수행하는 반면, 보험사 통지는 어디까지나 사적 계약 관계에 기반함.
- 그럼에도 불구하고 법안 제9조를 통해 민간 기업인 보험사에 대한 통지를 3일 이내로 강제하는 것은 사적 자치의 원칙을 침해하는 과도한 국가 개입에 해당할 수 있음.
- 또한 사고 수습의 우선순위 왜곡 및 분쟁 가능성임. 해당 조항은 단순한 통지 의무를 넘어, 안 제9조 제3항에서 통지 지연 시 '증가된 손해에 대해 보상책임을 지지 않는다'는 불이익을 명시하고 있음.
- 이는 사고 발생 직후 경황이 없는 기업에게 '3일'이라는 촉박한 데드라인을 강요함으로써, 시급한 사고 수습보다 보험사 보고를 우선순위에 두게 만드는 부작용을 낳음.

- 나아가 보험사가 이 조항을 근거로 향후 보험금 지급을 거절하거나 삭감하려 할 경우, 불필요한 법적 분쟁의 도구로 악용될 소지가 다분함.

□ (안 제10조, 제21조, 제22조) 기술적 혁신을 추구하는 기업들이 오히려 보안수준이 낮은 것으로 오인되는 사례

- (망분리 vs 클라우드 네이티브) 전통적 평가 기준은 내부망과 외부망의 물리적 분리를 고수합니다. 그러나 SaaS나 퍼블릭 클라우드를 적극 활용하는 경우, 물리적 망분리와 다른 방식으로 인정하여 위험도가 높게 측정될 수 있음.
- (Agile/DevOps 환경) 매일 수십 번의 코드 업데이트가 일어나는 애자일 환경에서는 '사전 승인' 중심의 전통적 보안 통제가 불가능함 대신 자동화된 보안 검사(DevSecOps)를 수행함에도 불구하고, 수동 결재 라인 부재나 문서화된 이력 부족을 이유로 보안 수준이 낮게 평가될 우려가 있음.