사이버 위험관리를 위한 보험의 역할 및 과제

출처 : 코리안리재보험㈜ The Risk 2017 No.4 Vol.4
글 : 최우석 사무관 과학기술정보통신부 정보보호기획과

1. 사이버위협 심각성 증가

지난 6월 국내 중소 웹호스팅업체가 해킹을 당해 큰 피해가 발생한 사건이 있었다. 이는 해당 기업의 서버 153대가 렌섬웨어에 감염되면서 서비스 이용 기관 홈페이지 5,496개가 마비되고 데이터가 소실될 위험에 처했던 사건으로, 해당 업체는 해커와 협상을 통해 서버를 복구했으나 13억원 상당의 협상금을 지불한 것으로 알려졌다.

최근 정보기술의 발달로 대부분의 경제·사회 활동이 사이버공간과 연계되면서 우리 삶이 매우 편리해지고 있지만, 한편으로는 '사이버위험'에 노출 범위도 넓어지며 관련 피해가 증가하고 있다.

글로벌 리서치기관의 보고서에 의하면, 전세계 사이버사고 피해액은 연간 5,750억불(약654조원, 딜로이트글로벌, '16)로, 자연재해 피해액의 3배를 넘는 것으로 나타난다.(자연재해피해액은 지난 10년간 연평균 1800억불 규모, Swiss Re., 2015)

사이버사고는 개인정보 등 중요데이터 유출, DDoS공격에 의한 네트워크 마비, 바이러스·악성코드에 의한 데이터·시스템 파괴 등이 포함된다. 흔히 알려져 있는 개인정보유출 사고의 경우 광범위한 피해를 입히는 특성으로 인해 사고가 발생할 때마다 사회적 혼란을 유발해왔으나 경제적인 측면에서는 상대적으로 심각하게 받아들여지지 않았다. 법원은 개인정보유출사고시 사고기업에 대해 건당 위자료 10만원 배상을 판결하는데 그친 바 있다.(피해자들은 건당 50~100만원을 청구)

그러나 최근에는 사이버사고의 양상이 변화하고 있다. 앞서 소개한 웹호스팅업체 해킹 사건과 같이 사이버공간에 연계된 재화·서비스를 볼모로 금전을 갈취하는 신종 사이버범죄(일명 '랜섬웨어')가 증가하여 국민 경제에 심각한 위협이 되고 있다.

다크웹과 가상화폐 등 익명성이 높은 기술의 발전에 따라 범죄자가 사법당국의 추적을 피해 피해자로부터 안정적으로 현금을 확보할 수 있는 수단이 마련되면서,

일각에서는 랜섬웨어가 잠재적 범죄 집단에게 비용 효과적인 수법으로 인식되어 일반화, 대중화 될 것을 우려한다. 장차 랜섬웨어 범죄를 실행하는 집단과 범죄의 툴을 제공하는 집단이 분화·전문화되어 나름대로의 생태계가 구성된다면, 사이버공간을 매개로 한 유사 유형의 범죄가 폭증할 수 있을 것이다.

4차 산업혁명과 함께 사이버공간에 연결되는 재화·서비스의 양은 기하급수적으로 증가할 것으로 전망된다. 사이버위험도 이에 비례하여 증가할 것인 바, 경제·사회의 안정적인 운영을 위해 위험 관리 수단으로서 사이버보험 활성화가 필요하다.

표 1. 최근 5년간 사이버 사고 현황

사고명(월)	해킹유형	사고내용
빗썸정보유출('17.6)	정보유출	빗썸 회원정보 유출사고 발생
인터넷나야나 랜섬웨어 감염 ('17.6)	랜섬웨어감염	인터넷나야나 호스팅서버(153대)가 랜섬웨어에 감염되어 이용기관 홈페이지가 랜섬웨어 협박화면으로 변조
워너크라이 랜섬웨어('17.5)	랜섬웨어감염	워너크라이 랜섬웨어에 감염되어 데이터 암호화 피해발생
여기어때 개인정보유출 ('17.3)	개인정보유출	SQL 인젝션 및 세션 변조 공격 등으로 개인정보 유출. 이를 악용하여 금전요구
인터파크 개인정보유출 ('16.5)	개인정보유출	내부직원의 PC가 악성코드에 감염된 후 사내 확산 및 DB파일 탈취
뽐뿌해킹 ('15.9)	개인정보유출	비정상DB질의에 대한 검증절차가 없는 보안취약점을 이용하여 개인정보유출
한수원해킹 ('14.12, '15.3,7,8)	정보유출	해커그룹(Who am I)이 원전중단을 요구하며 원자력 관련 자료를 인터넷에 공개
SKB DDoS공격 ('14.11)	DDoS	SKB DNS를 대상으로 DDoS 공격이 발생한 사고
KT정보유출 ('14.3)	해킹	KT 홈페이지의 타인여부 인증절차 보안취약점을 악용, KT고객 개인정보 유출 사고
6.25사이버공격 ('13.6)	해킹 DDoS	총 69개 기관.업체등에 대한 DDoS 공격 및 홈페이지 변조 사고 발생
3.20사이버공격 ('13.3)	해킹	방송·금융기관 등 서버·PC 등 악성코드 감염

[사이버보험 개념]

▪(정의) 사이버 침해사고로 발생한 유·무형의 피해에 대해 보상하는 보험

▪(보장범위) 정보시스템 파손, 데이터 멸실 등에 따른 손해, 사고원인 분석 및 복구비용, 정보 유출에 따른 제3자에 대한 배상책임 등 보장

2. 국내·외 사이버보험 도입 현황

1) 해외 동향

사이버보험은 미국·영국 등을 중심으로 점차 활성화 추세를 보이고 있다.

미국은 2000년대 개인정보침해사고 처벌 강화에 따라 사이버보험이 확산 중으로, 다양한 리서치기관의 자료에 따르면 가입률이 20~30%에 이르는 것으로 나타난다. 2005년 이후 사이버보험 시장이 본격적으로 확대되기 시작하여 2017년 기준으로 미국 내 사이버보험 시장규모는 연간 40억달러로 추산되고, 앞으로도 10~25%의 지속적인 성장이 예상된다. 미국은 사이버보험 활성화를 위해 2012년부터 오바마 '행정명령 13636'에 따라 국토안보부가 이해관계자 포럼 운영, 정책연구 등을 추진하고 있다.

영국의 경우 사이버보험 시장 규모는 2014년도 2,000만~2500만 파운드(296억원~369억원)에 이르는 것으로 추정된다(Marsh). 영국은 미국에 비해 사이버보험의 활성화 수준이 낮으나 최근 사이버보험을 금융산업을 이끌 새로운 분야로 인식하고 사이버보험 가이드라인을 마련하는 등 집중 육성하기 시작했다.

그 외에 국제기구에서도 사이버보험에 관심을 가지는 동향이 있는데 OECD는 2016. 4월부터 사이버보험 활성화를 위한 비공식 전문가 그룹을 구성하고 있으며, ISO도 관련 논의를 진행하며 최근 새로운 지침을 발표한 바 있다. 국제기구는 중소기업 보안 수준 제고를 위한 현실적 대안으로 보험을 인식하고 있다.

2) 국내 현황

미국 등의 움직임에 비해 우리나라는 아직 사이버보험 시장이 막 시작되고 있는 단계이다. 한국인터넷진흥원 실태조사 및 손해보험협회 조사 등에 따르면 한국의 사이버보험 가입률은 2016년 1.3%, 시장규모는 322억원에 불과하다.

국내 도입되어 있는 사이버보험 상품은 대부분 제3자에 대한 배상책임보험 위주로, 당사자 손해와 소송비용까지 종합적으로 보장하는 보험 상품은 활성화되지 않은 것으로 보인다.

시장 상황처럼 정책적인 측면에서도 우리나라는 시작단계에 있다. 아직 사이버보험에 대한 정부 정책이 마련되어 있지 않으나 방향 설정 및 구체적 지원방안 마련을 위한 연구/논의가 활발히 진행되고 있다. 금년 8월부터 '사이버보험 활성화 방안'에 대한 정부차원의 정책연구가 진행되고 있으며 이를 바탕으로 지난 11월에는 국회 및 과기정통부가 사이버보험 활성화 방안 토론회를 공동주최하여 보험사, 보안기업, 로펌, 수요기업 및 정부가 함께 사이버보험 시장 문제점 및 개선방안을 논의한 바 있다.

표 2. 국내 주요 사이버보험 상품 현황

구분	판매상품명
삼성	개인정보누출배상책임보험, 개인정보보호배상책임보험 전자금융거래배상책임보험, e-biz배상책임보험 정보 및 네트워크 기술에 대한 전문직 배상책임보험(INT E&O) 컴퓨터전문인배상책임보험, 금융사고보상보험책임보험 Samsung Cyber PKG, 전자기기보험
동부	개인정보누출 배상책임보험, 전자금융거래 배상책임보험 컴퓨터소프트웨어사업자 배상책임보험(CCPI) Cyber Security Policy 정보 및 네트워크 기술에 대한 전문직 배상책임보험(INT E&O)
현대	개인정보보호배상책임보험, 전자금융거래배상책임보험 e-biz배상책임보험, New Cyber Security Insurance
KB	개인정보보호배상책임보험, 전자금융거래배상책임보험 E-biz배상책임보험, Cyber Security
AIG	개인정보유출배상책임보험, Cyber Edge
한화	개인정보보호배상책임보험, 개인정보누출배상책임보험 전자상거래배상책임보험, Cyber Security e-biz배상책임보험, New Cyber Security, Cyber PKG

3. 사이버보험 활성화 장애요인 및 개선과제

1) 장애요인

사이버보험이 활성화되지 않는 이유는 보험사와 수요기업(피보험자)가 모두 만족하는 매력적인 보험상품이 설계되지 않기 때문인데 이는 결국 사이버위험에 대해 양측이 인식하는 정도가 다른 데에 기인한다. 보험사는 수요가 불확실한 상황에 과도한 위험을 감수할 만큼 사이버보험에 대해 투자가치를 느끼지 못하고, 수요기업들은 고정적인 비용과 불편을 감당해야 할 만큼 사고 위험을 느끼지 않는다.

국내 주요 보험사 인터뷰 및 수요기업 설문조사를 통해 파악된 사이버보험 확산의 장애요인은 다음과 같다.

공급측면
① 사이버사고 데이터 부족
② 대규모 재난 발생 가능성
③ 초기시장 확보 애로
수요측면
④ 까다로운 가입절차 및 조건
⑤ 좁은 보장 범위
⑥ 인센티브 부족

① 사고 데이터 부족 : 사이버보험 요율 산정, 위험 평가 기준 마련을 위해서는 사이버사고 통계가 필요하나 현재 국내에서 사이버사고 정보를 축적하는 체계가 미비하다. 현행법상 사이버사고는 신고하도록 되어 있고 이를 한국인터넷진흥원이 수집하고 있으나 보험업 등 영리기관에서의 활용에 대해 법적 근거가 없다. 현 체계 내에서는 보험사가 사이버보험 상품을 운영하며 개별적으로 데이터를 축적해야 한다.

② 대규모 재난 발생 가능성 : 사이버보안 분야는 특성상 신규 취약점에 의한 동시다발적인 피해 발생이 가능하여 대규모 배상책임에 따른 보험사 지급불능 사태가 발생할 수 있다. 이는 보험사들이 사이버보험 분야에 진입하는 것을 꺼리게 하고 보험사가 위험부담 완화를 위해 보험요율을 높여 시장을 위축시키는 요인이 된다.

③ 초기시장 확보 애로 : 보험 상품 설계·운용을 위해 최소한의 가입자 확보가 필요하나 사이버보험은 일부를 제외하고 가입 의무가 없어 초기 수요를 충분히 확보하지 못할 위험이 있다.

④ 까다로운 가입절차 및 조건 : 사이버보안 분야는 매우 전문적인 분야로서 위험이 겉으로 드러나지 않아, 피보험자의 위험수준을 정확히 측정하기 위해 복잡한 가입 절차를 거치게 된다. 이는 곧 보안 전문성이 부족한 피보험자에게 부담으로 작용해 보험 가입을 꺼리는 요인이 된다.

⑤ 좁은 보장 범위 : 국내 사이버보험 상품은 제3자 배상책임에 대한 보험 위주로 출시되어 당사자 손실 혹은 소송비용까지 포괄적으로 보장해주는 보험상품을 찾기 어렵다. 수요기업은 매출 손실 까지는 보장해주지는 않더라도 소송비용 등은 보장해주길 희망한다.

⑥ 인센티브 부족 : 다양한 기술적 보호조치들이 권고 또는 의무화되는데 비해 보험에 대해서는 아직 특별히 인센티브가 부여되고 있는 부분이 없다.

2) 개선 과제

보험사와 수요기업 양측이 가지고 있는 위험 인식의 차를 좁히기 위해서는 사이버위험에 대한 실증 데이터를 확보하고 이를 바탕으로 양측이 활발한 논의를 진행해 나가야 할 것이다. 사이버보험 활성화를 위해 다음과 같은 과제들이 검토되어야 한다.

ㅇ 사고데이터 집적 위한 제도적 기반 마련

사고데이터의 빠른 수집, 축적을 위해서는 한국인터넷진흥원 등 공공기관이 보유하고 있는 데이터를 활용할 필요가 있다. 이를 위해 사고 정보에 포함되어 있는 개인정보를 비식별화하여 활용할 수 있도록 근거법을 마련하고, 보유한 정보를 정제 및 공유할 수 있는 시스템을 구축해야 한다. 효율적 운영을 위해서는 보험개발원과의 긴밀한 협력이 필요하다.

ㅇ 사회적 논의의 장 마련 : 포럼 운영

보험 활성화를 위해서는 사이버위험 평가, 보험요율, 보험금 지급 기준 등에 대해 보험사와 수요기업 간 합의가 필요하다. 이를 위해 관계기업, 기관이 한자리에 모이는 논의의 장이 마련되어야 한다. 현재 국회와 과기정통부가 공동 주최하는 '사이버보험 포럼'이 운영되고 있는데, 보험시장이 충분히 형성될 때까지 안정적으로 운영될 수 있도록 각계의 관심이 필요하다.

포럼은 이외에도 사고 데이터 공유, 협력 방안 마련, 법, 제도 개선사항 도출, 보험 역기능 모니터링 및 대응방안 연구 등을 수행하여 보험 활성화에 기여할 수 있다.

ㅇ 인센티브 제공

사이버보험 가입 기업에 대한 인센티브로는 보안사고시 기업에게 부과되는 과태료, 과징금 경감, 공소 면제, ISMS인증 수수료 할인 등 보안 의무 경감 등이 거론된다.

ㅇ 취약기업 보안 컨설팅 지원

중소기업 등 취약계층은 보안 조치를 취할 여력이 부족해 상대적으로 사이버위험 수준이 높을 수 있다. 국가적 보안 수준을 높이기 위해서는 이런 취약기업이 보험에 보다 많이 가입해야 할 것이다. 그러나 보험사 입장에서는 위험이 큰 만큼 보험료를 높이거나 보험 계약 자체를 체결하지 않으려 할 유인이 있어 간극을 좁히기 위한 정부의 개입이 필요하다. 취약기업에 대해 보안 컨설팅을 지원하여 일정한 보안 수준을 확보하도록 돕는다면 보험사가 인수할 위험이 낮아지고 기업이 부담할 보험료도 낮아질 것이므로 대안이 될 수 있을 것이다.

ㅇ 국가 재보험 도입 검토

국가 재보험은 대규모 사이버 재난상황 발생에 따른 보험사 지급불능 사태에 대한 대응수단으로 고려된다. 이는 결국 정부 재정을 통해 사고 위험을 일부 담보하는 것으로 국가 재정 투입 타당성에 대해 면밀한 검토가 필요하다. 국가재보험이 운영된다면 보험사들의 위험이 크게 완화되므로 보험사들의 시장 진입을 촉진하고 보험료를 낮추는데 크게 기여할 것이다. 정부는 정보통신의 진흥을 위해 '정보통신진흥기금'을 설치, 운용하고 있는 바, 이를 재보험의 재원으로 일부 활용하는 방안을 검토해볼 수 있을 것이다.

4. 결언

1) 보험 확산의 기대효과

필자는 사이버보험 확산에 따른 사회적 효과로 크게 4가지를 기대한다.

① 일반 기업들의 사이버위험 분산을 통한 경영 안정성 확보

② 국민 피해 구제 현실화

③ 보안 산업 선순환 생태계 구축

④ 보안+보험이 일원화된 서비스 제공으로 보안 피로도 절감

①위험 분산과 ②피해구제는 보험의 본래 기능 중 하나로, 효과 발생에 대해 별도의 설명이 필요 없을 것이다. 적절한 보험은 기업의 사이버위험을 분산시켜 사고시 기업의 피해를 최소화하고 빠른 회복을 도와 기업 경영을 안정적으로 유지시키고, 제3자 피해가 발생한 경우 신속하고 현실적인 규모의 피해보상이 이뤄지도록 도울 것이다. 특히 피해구제의 경우 개인정보침해사고시 위자료 배상 결정의 주요 고려요인 중 한 가지가 사고기업의 배상능력인 점을 고려, 기업이 보험을 통해 배상능력을 확보할 경우 현재 건다 10만원 수준으로 유지되고 있는 배상 수준이 보다 현실화될 수 있을 것이다.

③현재 보안 산업은 정부의 지속적인 노력에도 불구하고 민간 투자가 잘 이뤄지지 않고 있어 체질 개선이 시급하다. 보안산업은 보안활동을 최전방에서 수행하는 주체로서 국가 보안 수준 제고를 위해 경쟁력 강화가 절실하다. 그러나 일반 기업들은 보안 투자의 이익이 불확실한 상황에서 높은 투자비용을 선뜻 감수하기 어려워 민간 투자가 위축되고, 이에 따라 국내 보안업계는 공공수요와 규제에 의존해 생존하는 방식을 택하게 되어 산업 전반의 경쟁력이 약화되는 악순환이 이어지고 있다.

그런데 보험이 확산될 경우, 보험업계는 피보험자의 위험수준을 낮추기 위해 보안서비스를 구매할 유인이 분명해 보안업계의 악순환 구조를 개선할 수 있을 것으로 기대된다. 일반기업, 특히 중소기업의 경우 보안서비스는 구매하지 않더라도 위험을 확정적으로 보장해주는 보험은 구매할 수 있다.

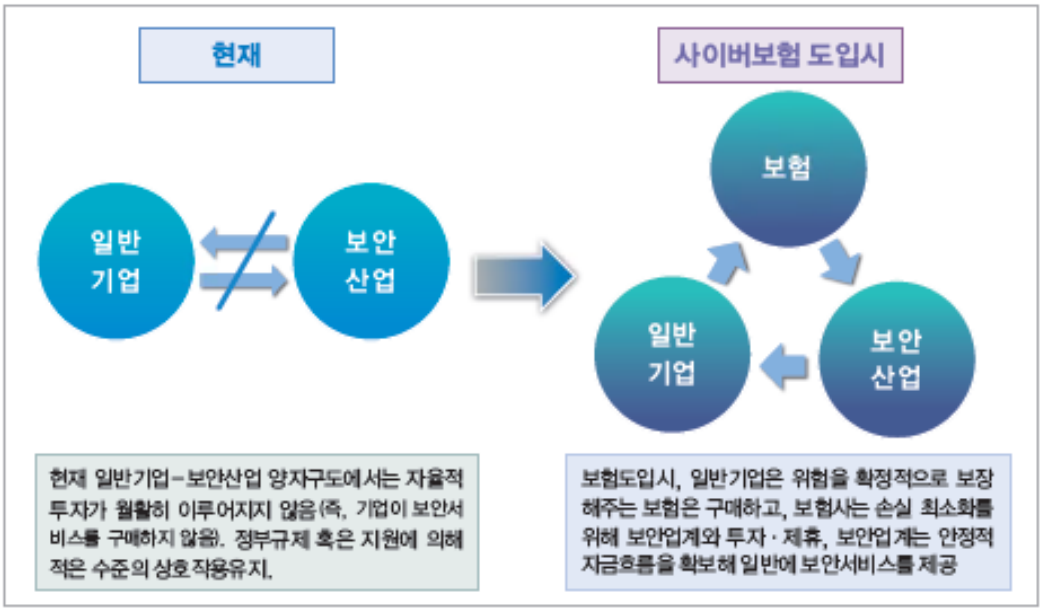
보험사는 피보험자(일반기업)의 보안 수준 강화를 위해 보안서비스에 투자하고 이에 따라 보안업계는 일반기업에 보안서비스를 제공하여 자금 및 서비스의 흐름이 완성될 수 있다.

보험이 확산되어 규모의 경제를 이루게 되면 이 효과는 더욱 극명하게 나타날 것이다. 미시적 수준에서는 혜택을 느끼기 어려우나 거시적 차원에서는 보안 수준 향상에 따른 피해규모 축소가 명백히 나타날 것이므로 보험사는 이익 극대화를 위해 유망 보안기업과 제휴하는 등 보안 산업에 대한 투자를 확대할 가능성이 높다.

실제 미국에서 사이버보험을 가장 먼저 시작한 보험사 중 하나인 AIG는 현재 다양한 보안 기업(Risk Analytics, IBM, K2 Intelligence, BitSight, RSA, Axio Global)과 협력하고 있으며, 이를 통해 피보험자에게 여러 가지 보안 서비스를 제공하고 있다.

보안 산업 경쟁력 강화에 따른 거시적 피해규모 축소와 이에 따른 보험사의 손실 축소는 곧 보험료 인하 여력으로 이어진다. 시장이 잘 관리되어 이 여력이 가격에 반영된다면(보험료가 인하된다면) 보험에 가입하는 기업이 더욱 늘어날 것이며 이는 다시

보험사 매출상승 → 보안투자 확대 → 보안수준 제고 → 피해규모 축소 → 보험료 인하로 이어지며 선순화 체계가 구축될 수 잇다.



④한편, 사이버보안 분야는 일반인의 보안 피로도를 절감하는 것을 또 하나의 큰 숙제로 가지고 있다. 사이버보안은 충분히 교육 받지 않으면 매커니즘을 이해하기 어려운 특수 분야에 속해 일반의 거부감이 크다.

각종 규제 혹은 위기감에 따라 기업들은 일정한 수주의 보호조치를 갖추는데 전문 인력을 고용하기 어려운 기업의 경우에는 보안 체계를 마련하고 운용하는 일이 매우 까다로운 일일 수 있다. 이는 보안조치의 비용 편익 분석이 쉽지 않다는 점도 한 몫을 할 것이다.

이런 가운데 보험이 보안서비스를 연계 제공한다면 기업의 부담은 크게 줄어들게 될 것이다. 보험사는 기업의 사고 가능성을 낮추기 위해 보안 서비스를 제공할 유인이 있으며 비용 최소화를 위해 꼭 필요한 수준의 보안 서비스만을 제공할 것이다.

기업은 불편을 감수하지 않으려 할 것이나 보험료 할인 등의 인센티브가 부여된다면 적정한 수준에서 보안 활동에 참여할 것이다. 즉 보험사가 위험 통계를 바탕으로 적정 보안 서비스 수준을 설정하는 '전문성'을 제공함으로써 기업의 부담을 덜어주는 효과를 내게 되는 것이다.

2) 보험업이 나아갈 방향

이상의 기대효과가 온전히 발휘되기 위해서는 보험업계의 역할이 매우 중요하다. 적정보험료 산정 및 보장범위확대, 보안서비스제공(보안투자), 취약기업까지 대상 범위 확대 등이 모두 보험업계의 실천의지에 의존하며 보험의 빠른 확산은 보험업계가 보안전문성을 얼마나 빨리 쌓느냐(정보 축적 및 위험분석)에 의존한다.

선순환구조가 구축될 수 있도록 보험업계는 보안분야에 대한 전문성을 높이고, 보안산업에 투자하여 기업의 보안수준제고에 기여해야 한다. 또한 보다 많은 기업이 보험시장에 참여하도록 단체보험 혹은 분야별 맞춤형 상품 등을 제공할 필요가 있다.

3) 정부의 역할

정부는 결국 기업 경영 안정성 확보와 이용자 피해 구제를 원활화하는 것이 주요 임무이다. 두 목표가 자연스럽게 달성될 수 있는 시장 구조를 만들고, 시장 실패를 보완하는 역할을 해야 한다.

사이버사고와 관련해서는 위에서 언급한 선순환 구조가 조속히 구축되도록 사이버보험 초기 시장 형성을 지원하고, 순환의 매 과정이 정상적으로 이행되는지 관리·감독하며 부작용이 발생하면 보완해 나가야 할 것이다.

특히, 이용자 피해구제를 위한 현실적인 지원방안 마련이 필요하다. 지난 10년간 주요 개인정보유출사고 47건 중 피해자에게 위자료 배상 판결이 난 경우는 3건, 배상액은 건당 10만원에 불과하다. 위 판결들은 적극적인 가해자가 아닌 사고기업에게 책임을 과중하게 지울 수 없으며 개인정보유출의 직접적인 손해액 확정이 어려워 소정의 위자료를 배상하도록 한 것이다.

개별 사건판결의 논리적 타당성과 별개로, 이런 판례들은 결국 국민들에게 개인정보유출 사고시 지난한 소송과정 끝에 얻게 되는 보상이 최대 10만원에 불과하다는 것을 알려준다. 과연 이 10만원을 위해 사고시 소송을 제기하려는 국민이 얼마나 있을까?

사고기업에게 큰 배상책임을 부여하지 않는 것은 직접적인 가해자를 찾아 처벌하고 피해를 배상하게 하는 일반 법리에 따른 것인데, 사이버사고는 특성상 직접적인 가해자(해커)를 잡기는 어려운 반면 피해는 광범위하여 일반 법리 적용시 결국 피해자만 양산되고 구제는 되지 못하는 결과가 발생한다.

비근한 예로 가해자 식별 및 인과관계 증명이 어려운 환경오염피해의 경우 '환경오염피해구제법'을 통해 '무과실책임', '인과관계 추정'의 법리를 마련해 인과관계와 기업 과실이 입증되지 않는 경우에도 피해와 '상당한 개연성'이 있는 오염물질 배출기업 에게 배상책임을 부여하고 있다.

이 경우 자칫 기업의 책임과중으로 오히려 경제활동을 위축시킬 수 있는데 이에 대해 정부는 보험사와 협력하여 '환경책임보험'을 마련하고 정도이상 이상의 피해는 국가가 부담함으로써 기업-국민을 균형있게 보호하고 있다.

이처럼 국민의 피해구제 현실화를 위해 사이버사고 피해와 관련해서도 분야특수성에 맞는 피해구제법리가 마련되어야 할 것이다. 국회차원의 논의를 통해 결제활성화와 이용자보호의 두가지 목표를 균형있게 달성하는 정교한 정책설계가 필요하다.