전자무역기업이 직면하는 위험과 위험관리
- 전자상거래 보험을 중심으로

신 건 훈
(경상대학교 경영대학 국제통상학전공 조교수)

목 차

Ⅰ. 서언

오늘날 대부분의 기업은 기업운영과 관련하여 인터넷을 활용하거나 전자상거래에 종사하고 있다. 일부 기업의 경우 기업운영과 관련하여 인터넷 또는 전자상거래를 활용하고 있지 않더라도, 일상 업무의 수행을 위하여 컴퓨터에 상당히 의존하고 있다. 기업운영과 관련하여 컴퓨터는 하나의 수단에 불과하지만, 네트워크 또는 인터넷으로 연결되는 컴퓨터는 기업에 대한 무한한 잠재력을 제공한다. 그 반면 오늘날 기업은 컴퓨터 또는 네트워크를 활용하고 있다는 사실만으로도 기업은 과거 경험하지 못하였던 다양하고 강력한 신종 위험에 직면한다. 기업의 입장에서 상황을 더욱 심각하게 만드는 것은 이러한 위험이 현재까지 개발된 보안기술 보다 더 앞서서 발전해 왔고, 지금도 진보 내지 발전하고 있을 뿐만 아니라 미래에도 계속 발전을 계속할 것이라는 점이다.

전자무역기업은 이러한 신종위험으로 인하여 새로운 도전에 직면하고 있다. 과거의 무역상이 인적·물리적 위험에 대처하기 위하여 다양한 관습 및 제도를 고안하였듯이, 전자거래환경 하에서 상거래를 영위하는 오늘날 무역기업의 입장에서는 전자거래환경 하에서 발생하는 다양하고 강력한 신종위험에 대처하기 위하여 새로운 위험관리방법을 모색해야 할 시점에 도달하였다. 전자거래환경이 초래하는 위험은 과거 위험에 비하여 강력하고 다양하기 때문에 이러한 위험에 대처한다는 것은 기업의 입장에서 매우 성가시고 고비용을 요하는 과업이지만, 새로운 위험은 수천만 달러의 가치를 가진 기업을 순식간에 초토화시킬 수 있는 강력한 힘을 가졌기 때문에 기업은 필수적으로 과거와 다른 위험관리수단을 모색해야 한다.

21세기의 전자무역환경에 직면해 있는 무역기업은 여전히 20세기의 위험관리수단으로 기업의 위험에 대처하고 있다. 본 고에서는 전자무역환경 하에서 무역기업이 직면하는 위험에 대한 관리수단으로 전자상거래 보험을 제시한다. 물론 전자상거래 보험은 신종보험으로서 아직까지는 안정성이 결여되어 있고, 또한 많은 문제점을 내포하고 있기 때문에 기업의 입장에서 위험관리를 위하여 보험이라는 제도적인 장치보다는 보안기술이라는 기술적 장치에 비중을 더 많이 두고 있는 상황이다. 하지만 100퍼센트 완벽한 보안기술은 존재하지 않고 새로운 위험이 보안기술 보다 앞서서 발전하고 있기 때문에 전자무역기업의 입장에서 완벽한 위험관리를 위해서는 제도적인 장치로서 반드시 전자상거래 보험을 필요로 하는 시점이다.

본 고에서는 먼저 신종위험의 특성 및 유형을 고찰하고, 이러한 위험에 대한 전자상거래 보험에 대한 담보범위 및 시장현황, 그리고 전자상거래 보험과 관련한 현재의 쟁점을 분석한다. 본 논문의 목적은 전자상거래에 종사하는 기업에 대하여 새로운 전자상거래 위험에 대한 인식 및 위험관리의 필요성을 각인시키고, 보험가입 시 유용한 지침서를 제공하는데 그 목적이 있다.

Ⅱ. 전자무역기업이 직면하는 위험의 분류 및 특성

1. 위험의 분류

오늘날 대부분 기업은 기업운영과 관련하여 인터넷을 활용하거나 전자상거래에 종사하고 있다. 일부 기업의 경우 기업운영과 관련하여 인터넷 또는 전자상거래를 활용하고 있지 않다고 하더라도, 일상 업무의 수행을 위하여 컴퓨터, 컴퓨터 시스템 또는 기업내부의 인터라넷에 상당히 의존하고 있다. 오늘날 기업이 기업운영 또는 업무수행을 위하여 컴퓨터 또는인터넷을 활용하고 있다는 사실만으로 기업은 과거 경험하지 못했던 다양하고 강력한 위험에 노출된다.

전자무역환경 하에서 전자무역기업이 직면하는 위험은 위험의 형태에 따라 다양한 분류가 가능하겠지만, 본 논문에서는 손해발생의 직접당사자를 기준으로 본인위험(또는 본인손해)과 제3자 위험(제3자 손해)으로 분류한다.[2] 즉 전자상거래 행위에 부수하는 위험이 피보험자에 대하여 직접적인 손해를 입히는 경우 이를 본인위험(또는 본인손해)이라고 지칭하고, 피보험자의 과실에 기인하여 제3자가 손해를 입고 차후에 피보험자가 제3자에 대하여 손해배상책임을 부담하게 되는 경우에 이를 제3자에 대한 책임위험(또는 책임손해)이라고 지칭한다.[3]

한편 본인위험은 발생원인에 따라 물리적 위험(화재나 도난 등), 소프트웨어 또는 프

---

2) 손해보험과 관련한 보험이론 상 손해는 일반적으로 직접손해와 간접손해로 분류되고, 간접손해는 다시 비용손해와 책임손해로 분류된다. 여기서 직접손해는 특정 위험으로 인하여 피보험자의 재산이 직접 물리적인 멸실 또는 손상(Physical loss or damage)을 당한 경우에 피보험자가 입는 손해를 의미한다. 간접손해는 피보험자의 재산에 대하여 직접적인 멸실이나 손상이 발생한 것은 아니지만, 피보험자가 보험사고와 관련하여 특정 비용을 부담하는 경우에 그러한 비용손해 및 제3자의 손해에 대하여 손해배상책임을 부담하는 경우에 발생하는 책임손해를 의미한다. 한편 전자상거래 또는 인터넷 활동과 관련하여 기업이 입는 손해는 전통적인 손해보험이론 상 구분되는 직접손해와는 거의 무관하다. 물론 후술하는 화재나 도난의 경우에 직접손해가 발생할 수 있으나, 이러한 위험으로 인하여 발생하는 손해는 본 논문의 주요 분석대상인 전자상거래 관련 손해가 아니라, 주로 전통적인 손해보험, 즉 화재보험, 도난보험 또는 기업종합보험에서 커버되는 손해의 형태라고 할 수 있다. 또한 현재 보험시장에서 판매되는 전자상거래 관련 위험에 대한 보험상품은 담보부문을 크게 본인손해담보(재물손해담보로서 업무장애로 인한 간접손해담보를 포함) 및 배상책임담보로 구분하고 있기 때문에 본 논문에서는 전통적 위험(또는 손해) 분류방식과 다소 상이한 위험분류방식을 채택한다.

3) H. Wesley Sunu, Rober Paul Norman, Katherine S. Kamen, Larry P. Schiffer and Adam B. Perri, "Recent Development in E-Commerce", *Tort Trial & Insurance Practice Law Journal*, Vol.37, No.2, Winter 2002, p.347.

로그래밍의 결함, 외부자의 공격(해킹이나 바이러스 등)으로 분류되고, 이에 기인한 기업의 업무중단은 간접위험으로 분류한다. 또한 본인손해는 궁극적으로 기업 컴퓨터 시스템의 기능상실 또는 기능저하에 직접 기인하는 기업의 재산손해로서, 이는 컴퓨터 시스템의 기능상실에 직접 기인하는 비용손해와 그러한 기능상실의 결과 필연적으로 초래되는 업무중단에 기인하여 간접적으로 발생하는 비용손해로 구분된다. 직접비용손해는 주로 컴퓨터 또는 시스템의 복구 및 교체에 소요되는 비용을 의미하고, 간접비용손해는 업무중단기간동안에 발생한 기업의 영업기회상실에 부수하는 손해를 의미한다.

한편 제3자에 대한 책임위험은 피보험자의 과실이나 태만에 기인하여 발생하는 제3자의 지적재산권 침해, 명예훼손, 프라이버시 침해 및 시스템 에러에 대한 책임을 의미하고, 제3자에 대한 손해배상책임의 결과, 피보험자에게 발생하는 손해를 책임손해라고 정의한다.

2. 위험의 특성

전자상거래에 종사하는 기업이 직면하는 다수의 위험은 전통적 기업이 직면하는 기업위험(예를 들면, 명예훼손 또는 지적재산권 침해)과 유사한 반면, 그 위험의 성격은 전통적 위험과 구분되는 독특한 성격을 내포하고 있다. 즉 해킹이나 바이러스로 대표되는 사이버위험의 경우, 지리적 영향, 위험의 심도, 발생요인의 다양성 및 위험발생의 인식가능성 면에서 전통적인 위험과 구분되는 독특한 성격을 갖는다.[4] 즉, 첫째, 해킹이나 바이러스와 같은 사이버위험이 인터넷을 통하여 발생하는 경우, 정보도난이나 재산손상을 초래하는 위험이 발생장소로부터 물리적으로 수천 마일 떨어진 장소에 있는 디지털재산에 대해서도 손해를 초래할 수 있다. 즉, 해커의 경우 범행장소의 물리적 이동 없이 인터넷으로 연결되는 전세계를 상대로 해킹을 성공적으로 수행할 수 있다.

둘째, 해킹이나 바이러스에 기인한 손해는 바이러스 유포자가 처음에 목표한 기업의 범위를 초월하여 불특정·다수의 재산에 대해서도 손해를 초래함으로써, 일단 당해 손해가 발생하면 그 손해의 규모는 상상을 초월하여 발생한다. 예를 들면, 미국의 '컴퓨터 보안과 관련한 긴급대책센터'(Computer Emergency Response Team Coordination

4) Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail, "A Fraimwork for Using Insurance for Cyber-Risk Management", Communications of the ACM, Vol.46, No.3, 2003. 3, p.81.

Center)에서 발표한 자료에 의하면,[5] 2001년 한 해동안 해커에 의한 악의적인 코드 공격으로 인한 경제적 손실은 전세계적으로 약 131억 달러를 기록하였다.

셋째, 시간이 경과함에 따라 위험을 생성하는 당사자에 대한 정보는 상대적으로 감소되는 반면, 그러한 당사자의 수 및 공격기법은 증가 및 다양해지고 있고, 한편으로는 강력해지고 있다. 1980년대 공격자는 주로 시스템 전문가였으나, 오늘날 습득이 용이한 공격기술을 갖고서 누구라도 성공적인 공격을 감행한다. 해킹의 툴은 급속하게 증가하는 반면, 그러한 툴의 사용방법에 대한 지식의 습득은 점차 용이해짐으로써, 컴퓨터에 관한 평범한 지식을 가진 불특정다수도 그러한 툴을 이해하고 사용하는 것이 점차 더 용이해졌다.[6] 이러한 이유로 인하여 기업재산에 대한 사이버공격의 가능성도 점차 증가할 뿐 아니라, 공격의 기법도 다양·강력해졌다.

넷째, 위험발생의 인식가능성과 관련한 문제로서, 특히 인터넷 상 정보가 상품인 기업의 경우에 기업의 경영전략 상 민감한 정보유출과 보안상 문제점은 종종 인식되지 않는다는 점이다. 즉, 전자상거래 관련 위험은 기술적인 면에서 점차 은밀하게 자행되기 때문에 정보가 유출되었다는 사실을 발견하기가 힘들 뿐만 아니라, 발견하더라도 위험의 생성자 및 발생경로에 대한 식별이 어렵다.

---

5) Bruce Schneier, "Hacking Insurance", http://www.andrew.cmu.edu/user/hchong.

6) 초창기 사이버범죄는 컴퓨터 전문교육을 받은 고학력자에 의하여 자행되었으나, 요즘에는 10대 청소년에 의한 사이버범죄가 큰 폭으로 증가하고 있다. 경찰청 사이버테러대응센터에서 발표한 통계자료에 의하면 10대에 의한 사이버범죄는 2000년 675명, 2001년 2,193명, 2002년 8,250명으로 해마다 급증하고 있으며, 특히 2003년에는 10,187명으로 2000년에 비하여 무려 15배나 증가하였다(인터넷한겨레, 2004년 1월 14일자 보도기사 참조).

Ⅲ. 전자무역기업이 직면하는 위험의 유형

1. 컴퓨터 시스템의 기능장애

기업에서 업무용으로 사용되는 개인 컴퓨터의 손상이나 파괴는 개인 사용자에게 단지 어느 정도 불편함을 초래하지만, 그 자체로서 전체 기업의 운영에 심각한 영향을 미치지는 않는다. 반면 네트워크 서버의 손상이나 파괴는 전체 기업에 심각한 영향을 미친다. 왜냐하면 명칭에서 알 수 있듯이 네트워크 서버는 전체 네트워크에 서비스를 제공하고, 이러한 서비스는 기업내부 또는 내·외부의 컴퓨터 사용자간 의사소통을 의미하기 때문이다.[7]

서버의 기능장애로 인하여 기업 컴퓨터 시스템의 작동이 중단되거나 기능저하가 초래되는 경우, 기업의 대부분 업무는 중단상태에 돌입하게 된다. 기업의 컴퓨터 시스템이 정확하게 작동되기 위해서는 하드웨어가 의도대로 작동되어야 하고, 관련 기능을 운용·관리하는 소프트웨어가 적절하게 운용되어야 하며, 또한 소프트웨어 운용의 기초가 되는 데이터가 완전하고 정확해야 한다. 결국 기업의 컴퓨터 시스템은 다양한 운영요소로 구성되어 있고, 따라서 기업 컴퓨터 시스템의 기능장애를 초래하는 위험요소는 다음과 같이 다양하다.

첫째, 전통적·물리적 위험으로서 화재나 도난위험이 존재한다. 컴퓨터 네트워크가 설치된 건물이 화재나 누수[8]로 손상되거나, 호스트 역할을 하는 컴퓨터가 도난[9]되는 경우에 기업 컴퓨터 시스템의 작동은 중단되고, 결국 기업은 막대한 손해를 입게 된다. 이러한 물리적 위험은 기업에 대하여 컴퓨터, 컴퓨터 시스템 및 네트워크 장비에 대한

---

7) 서버는 컴퓨터네트워크에 연결되어 있는 개별 컴퓨터에 IP 어드레스를 제공하고, 상이한 하부 네트워크 사이 또는 네트워크와 인터넷 사이의 통신을 위한 연결장치 역할을 한다. 결국 기업에서 서버의 기능이 손상되거나 상실되면 네트워크에 연결되어 있는 개별 컴퓨터들은 외부세계와의 상호교신뿐만 아니라 내부 컴퓨터 상호간에도 교신이 불가능해진다.

8) 2000년 9월 28일 발생하였던 D증권사의 전산사고는 대표적인 예를 제공한다. 즉 이 회사의 경우에 당시 일일 약정규모 3000억원의 75-80%가 사이버거래로 이루어지고 있었으나, 전산실의 누수에 의한 전산시스템의 파괴로 이 회사의 사이버거래는 이틀 동안 완전히 중단되었다.

9) 영국의 경우 영국 보험자협회(Association of British Insurers)의 추산에 의하면 매년 약 100,000대의 컴퓨터가 도난되고, 또한 컴퓨터 칩의 도난으로 인하여 매년 약 10억파운드의 경제적 손실이 발생한다(C.C. Nicoll, "Insurance of e-commerce risks", International Journal of Insurance Law, 1999. 10, p.295).

물리적 손해를 초래할 뿐만 아니라, 컴퓨터에 저장되어 있는 기업경영관련 기본 데이터[10] 및 고객정보의 상실로 인한 손해를 초래하게 된다.

둘째, 컴퓨터 시스템을 운용하는 소프트웨어의 결함 또는 프로그래밍 상 오류 또한 컴퓨터 시스템에 치명적인 영향을 초래한다. 기업 컴퓨터 시스템의 구성요소 중 하드웨어에 해당하는 컴퓨터에 대한 물리적 위험도 전체 시스템의 붕괴를 초래하지만, 소프트웨어에 해당하는 소프트웨어의 결함 또는 프로그래밍 상의 오류도 전체 시스템에 치명적인 영향을 미친다. 하드웨어에 해당하는 부분은 상대적으로 신속하게 수선이나 교체가 가능하지만, 기본적인 데이터나 소프트웨어는 재수집 및 복구에 상당한 시간을 요한다. 물론 복구에 소요되는 시간은 당연히 백업 시스템의 존재, 백업 시스템의 가동성 여부, 안전성 및 백업 시스템 간 상호작용에 요구되는 시간에 절대적으로 의존하게 된다.

셋째, 해킹이나 바이러스 등 외부자의 공격은 주로 기업운영에 필수적인 프로그램 또는 시스템운용과 관계되는 데이터의 삭제, 변경 또는 파괴함으로써 기업 컴퓨터 시스템에 치명적인 영향을 미친다. 도난이나 화재와 같은 물리적 위험의 경우 도난경보기나 연기탐지기의 설치로 인하여 어느 정도 위험을 통제하는 것이 가능하나, 해킹[11]이나 바이러스[12] 등 외부자의 공격은 시스템 관리자의 입장에서 볼 때 가장 방어하기 어려운 위험이다. 왜냐하면 이 형태의 위험은 IT 기술 또는 전자상거래의 발전보다 더 급속하게 발전하여 왔으며, 현재도 진화하고 있기 때문이다.[13] 물론 시스템 관리자가

---

10) 예를 들면 기업의 회계기록, 재고상황 및 고객정보 등에 관한 자료이다.

11) 해킹의 대상은 일차적으로 컴퓨터 네트워크에 연결된 시스템이라고 할 수 있으나, 궁극적으로는 시스템에 저장된 데이터가 그 대상이 되며, 오늘날에는 네트워크의 관리 자체에 위험을 가하는 유형의 해킹도 발생하고 있다.

12) 우리 나라의 경우 2000년 상반기에 신종 바이러스가 346종 발견되었고, 이 수치는 1999년 상반기(127종) 대비 172.4% 증가한 수치로써 하루에 약 2종 정도의 신종 바이러스가 제작 및 유포된 셈이다(형사정책연구원, 인터넷범죄의 규제법규에 관한 연구, http://www.kic.re.tr/search/data/00-16k.txt, 2001. 7. 30, p.1).

13) 최근 인터넷 사용자는 스파이웨어, 바이러스, 웜, 피싱 사기, 서비스거부 공격 등으로 곤란을 겪고 있는데, 최근에는 신종 공격수법인 '랜섬웨어'까지 등장하여 사용자를 더욱 곤란에 빠뜨리고 있다. '랜섬웨어'는 어린이를 납치(kidnap)한 후 보상금(ransom)을 요구하는 전통적인 범죄수법을 모방하고 있다. 즉 랜섬웨어는 기존의 해킹이나 바이러스처럼 사용자 컴퓨터의 파일을 삭제·파괴하거나, 사용자의 ID를 도용하는 것이 아니라, 사용자의 중요한 파일을 열지 못하도록 만들고(kidnap), 이를 인질로 삼아 보상금(ransom)을 요구하는 신종 사이버범죄수법이다. 즉 사용자가 악성 코드가 포함된 웹 사이트에 접속하는 경우, 악성 코드는 사용자 컴퓨터에 담긴 약 15종의 데이터 파일을 암호화하고, 특정 주소로 전자메일을 보내야만 암호를 풀 수 있다는 메시지를 남긴다. 사용자가 전자메일을 발송하면, 특정 은행구좌로 소정의 금액을 송금하면 암호를 풀어 준다는 답장이 반송된다(야후 ITnews, 2005. 5. 25, http://kr.blog.yahoo.com/everitnews).

컴퓨터 시스템에 바이러스를 탐지하는 안티-바이러스 프로그램을 설치하고 정기적으로 운용 및 업데이트하거나, 전문 보안업체에 의뢰하여 방화벽을 설치한다면 기술적으로는 어느 정도 외부자의 공격위험을 회피할 수 있으나, 외부공격의 기법은 지금까지 개발된 시스템 보안기술 보다 항상 한발 앞서 발전해왔다.

인터넷 사용의 급증과 더불어 급증하는 수의 컴퓨터 바이러스가 컴퓨터 시스템을 통하여 확산되고 있다. 바이러스는 일종의 컴퓨터 프로그램으로서, 컴퓨터 파일의 감염에 의하여 다양한 유형의 손해, 즉 컴퓨터 프로그램의 변경, 데이터의 변경·삭제, 컴퓨터 시스템의 부당접속을 위한 ID정보 도용 및 시스템 에러를 초래한다. 바이러스는 보통 인터넷이나 이메일을 통하여 전송되는 감염된 파일에 의하여 확산되고, 생물학적인 바이러스와 마찬가지로 자가복제기능을 갖고 있다.

최근 미국 FBI의 도움을 얻어 컴퓨터보안연구소(Computer Security Institute)가 미국 일부 단체를 대상[14]으로 실시한 보안관련 조사의 결과(CSI/FBI Computer Crime and Security Survey)에 의하면, 바이러스 및 해킹에 의한 독점정보의 도난으로 인한 손해액이 최근 상위권을 차지하고 있고, 그 손해액 또한 막대하다([표-2 참조]). 단적인 예로 지금까지 발견된 가장 치명적인 바이러스의 일종인 소위 Love Bug의 경우, 2000년 5월에 발생된 지 한 달도 지나지 않아 전세계에 확산되었다. 이 바이러스는 이메일 사용자로 하여금 "ILOVEYOU"라는 주제 하의 첨부 파일을 오픈하도록 함으로써 전세계 컴퓨터 시스템으로 확산되었고, 전세계 이메일 시스템을 파괴하였으며, 사용자의 패스워드를 도난하고, 사용자의 컴퓨터에 내장된 가치 있는 파일을 삭제하였다. 이 바이러스는 확산된 지 24시간도 채 지나지 않아 10억 달러의 경제적 손해를 초래한 것으로 추산되었다.[15]

---

14) 조사대상단체는 총 494개였고, 첨단기술업체(13%), 연방정부 및 지방정부를 포함한 공공기관(4%), 금융기관(19%), 제조업체(12%), 의료기관(6%), 교육기관(7%) 등으로 구성되어 있다. 한편 전체 단체 중 손해를 경험한 것으로 보고한 단체는 269개(약 55%)였다(2004년 CSI/FBI Computer Crime and Security Survey, pp.1-2 참조).

15) Love Bug는 하루에 US $10억 - 15억의 손해를 초래한 것으로 보도되었고, 총손해액은 US $150억을 상회하는 것으로 추산되었다. 또한 당시 Love Bug의 희생양은 백악관을 비롯하여, 미국 의회, 미국 국방부 및 영국 하원 등이었다(David R. Cohen and Roberta D. Anderson, "Insurance Coverage for Cyber-Losses", Tort & Insurance Law Journal, Vol. 35, No. 4, 2000, pp.891-896).

[표-1] 보안사고에 기인한 경제적 총손해액

단위 : US $

연도	응답자 수	총손해액
1997	249	100,119,555
1998	241	136,822,000
1999	163	123,779,000
2000	273	265,589,940
2001	196	377,828,700
2002	379	455,848,000
2003	530	201,797,340
2004	269	141,496,560

자료 : 2004년 *CSI/FBI Computer Crime and Security Survey*, p.10 및 2003년 *CSI/FBI Computer Crime and Security Survey*, p.20

[표-2] 위험유형별 손해액[16)]

단위 : US $

공격의 유형	2004	2003	2002	2001	2000
서비스 중단	26,064,050	65,643,300	18,370,500	4,283,600	8,247,500
내부자에 의한 무단접속	4,278,205	406,300	4,503,000	6,064,000	22,554,500
바이러스	55,053,900	27,382,340	49,979,000	45,288,150	39,171,700
과도한 네트워크 접속	10,601,055	11,767,200	50,099,000	35,001,650	27,984,740
독점정보 도난	11,460,000	70,195,900	170,827,000	151,230,100	66,708,000
금융사기	7,670,500	10,186,400	115,753,000	92,935,500	55,996,000
네트워크 데이터 파괴	871,000	5,148,500	15,134,000	5,183,100	27,148,000
랩탑의 도난	6,734,500	6,830,500	11,766,500	8,849,000	10,404,300
외부자 침입	901,500	2,754,400	13,055,000	19,066,600	7,104,000

자료 : 2004년 *CSI/FBI Computer Crime and Security Survey*, p.10 및 2003년 *CSI/FBI Computer Crime and Security Survey*, p.20

16) 기타 위험으로서 원격통신에 의한 사기, 내부자의 도청 및 원격도청이 있음.

다른 한편, 해커의 공격은 기업의 컴퓨터 시스템을 마비시킬 수 있는 잠재력을 갖는다. 해킹은 권한 없이 타인의 정보시스템에 무단으로 접속하는 것을 의미한다. 타인의 시스템에 무단으로 접속하는 행위 자체가 위험성을 의미하는 것은 아니지만, 해킹이 무단접속으로 끝나는 것이 아니라 사행활 침해, 정보의 위·변조, 손괴, 시스템 교란 등 정보범죄의 수단이 되고 있다. 최근의 해킹은 과거 호기심이나 도전정신 차원의 해킹이 아니라, 컴퓨터네트워크 소유자에게 수십억 달러의 손해를 입힐 수 있는 대단히 파괴적이고 조직적인 양상을 띄고 있다.[17]

2. 영업장애로 인한 간접손해

기업은 항상 사고나 제3자의 악의에 의하여 기업 자체의 재산손해나 비용손해 또는 타인에 대한 책임손해를 당할 수 있는 위험에 노출되어 있다. 이러한 사실은 기업의 경영층에 의하여 잘 인식되고 있지만, 기업의 상거래활동과 관련하여 종종 간과되기 쉬운 위험은 영업중단에 후속하여 발생되는 간접손해이다.

전술한 위험으로 인하여 기업 컴퓨터 시스템의 기능장애가 발생하는 경우, 시스템의 복구에는 상당한 시간을 요하게 되고, 기업은 일정 기간동안 영업중단상태에 돌입하게 된다. 영리기업에서 시간의 손실은 시장 또는 고객의 상실, 영업기회 또는 영업이익의 상실 및 영업재개를 위하여 지출하는 추가비용의 발생을 의미한다. 특히 기업의 컴퓨터 시스템 상 기능장애로 인하여 영업중단사태가 발생하게 되면 막대한 간접비용손해가 발생할 뿐만 아니라, 특히 전자상거래 기업의 경우 기업의 명성, 신뢰도 또는 이미지에 치명적인 상처를 입게 된다.[18]

3. 불법행위책임

(1) 명예훼손에 대한 불법행위책임

---

17) 형사정책연구원, 전자상거래 관련범죄의 규제에 관한 연구, http://www.kic.re.kr/search/data/00-03k.txt, 2001. 7. 30, pp.3-4.

18) 미국 미네소타 대학의 연구에 의하면 고객의 신뢰가 생명인 금융서비스업종의 경우 전산서비스가 2일 이상 중단되면 25%는 즉시 파산하고 40%는 2년 이내에 파산한다(동아일보 2000년 9월 29일자 경제면 참조).

오늘날 인터넷이란 새로운 매체의 등장으로 인터넷 사용자는 가상공간에서 자기의 주장을 피력하는 기회가 많아지고, 따라서 고의나 과실에 의하여 타인을 비방하거나 허위사실을 유포할 가능성도 확대되었다. 이는 인터넷 사용자가 과거보다 명예훼손으로 인한 민·형사상 불법행위책임에 직면하는 위험에 노출되어 있음을 의미한다. 인터넷의 익명성에 기인하여 기업의 종업원이 채팅 룸이나 뉴스그룹을 통하여 타인을 비방하는 글을 공개하고, 이러한 메시지가 업무시간에 전송되었다면 고용주는 명예훼손에 따른 잠재적 책임에 직면한다. 미국의 한 조사기관의 조사에 따르면, 2000년 1월 한 달 동안 미국 근로자는 업무시간 중 평균 21시간을 업무와 상관없는 인터넷 접속에 소비하였다.[19]

다른 한편, 전자상거래에 종사하는 기업이 웹 사이트를 개설하고 전자게시판을 운영하는 경우에 기업의 고용주는 명예훼손에 의한 불법행위책임에 직면하게 된다. 즉, 웹 사이트의 방문객 또는 종업원이 기업의 전자게시판에 타인 또는 경쟁기업을 비방하는 내용물을 게재하는 경우에 기업 경영자는 당해 게시판의 소유 및 운영자로서 비방의 대상이 된 피당사자에 대하여 명예훼손에 따른 불법행위책임에 직면한다. Western Provident Association v. Norwich Union 사건[20]에서 법원은 피고회사의 일부 직원이 내부 이메일 시스템을 통하여 비영리 건강보험단체인 원고가 재정적으로 파산상태라는 허위사실을 유포함으로써 원고에게 손해를 초래하였다는 사실을 인정함으로써 원고에게 45만 파운드를 배상하라고 판결하였다.[21]

(2) 지적재산권의 침해에 대한 불법행위책임

오늘날 기업이 사용하고 있는 타인의 지적재산권은 매우 가치 있는 자산이다. 한 보고서에 의하면, 미국 기업의 자산가치 중 70%는 지적재산에 내재되어 있을 정도로 오늘날 기업에 있어서 지적재산은 절대적인 가치를 구성한다.[22] 전자상거래는 기업에 대

---

19) Tim Sukel, "The Workplace, Cyberspace and Cyber-Liability"(2000. 9), http://progressivebanks.com/Agents/Safetalk_Sept2000.

20) Stephen York and Ken Chia, E-Commerce-A guide to the law of electronic business, Butterworths, 1999, p.86.

21) 우리나라에서도 사이버 명예훼손에 관한 처벌 법령이 2001년 7월 1일부터 시행되어 인터넷에 허위사실을 유포한 경우에 최고 7년형이나 벌금 5천만원, 비방할 목적으로 사실을 적시하였을 경우에 최고 3년형이나 벌금 2천만원에 처해지고, 이와 더불어 민사소송도 가능하다(매일경제 2001년 6월 30일자 신문, http://find.mk.co.kr/cgi-bin 참조).

하여 인터넷을 통하여 전세계의 잠재고객에 대하여 저렴한 비용으로 거의 실시간에 가까운 제품광고 및 기술적 조언을 할 수 있다는 장점을 갖고 있는 반면, 외부 세계와 손쉽게 정보를 교환할 수 있는 컴퓨터의 의사소통능력으로 인하여 컴퓨터의 소유자 또는 컴퓨터 시스템의 관리자는 뜻하지 않은 법적 책임을 부담하는 경우가 발생한다. 즉 인터넷은 유익한 정보의 강력한 전달수단을 제공할 뿐만 아니라, 특정 정보가 그 정보에 대하여 지적재산권을 보유하고 있지 않은 자의 컴퓨터에 대량으로 정보가 전달되는 導管으로서의 역할을 한다.

① 저작권 침해

저작권(copyright)이라 함은 자기가 창작한 저작물에 관하여 가지는 권리를 말하며, 저작권은 정신적 창작으로 문학, 예술 또는 예술의 범위에 속하는 저작물을 창조한 자가 그 창작물의 이용에 관하여 가지는 배타적 지배권을 의미한다.[23]

저작권은 등록 여부에 상관없이 '저작자의 원저작물'에 대한 보호를 제공한다. 미국의 1976년 저작권법(1976 Copyright Act) 하에서 연방저작권 보호는 문학 창작물, 가사를 포함한 음악 창작물, 음악을 포함한 연극 창작물, 무언극 및 무용 창작물, 사진, 그래픽 및 조각 창작물, 활동사진 및 기타 시청각용 창작물, 음성녹음 및 건축창작물을 대상으로 한다.[24]

저작권자의 일체의 배타적 권리에 대한 침해는 저작권 침해를 구성한다. 저작권 침해는 침해자의 의도 유무에 상관없이 결정된다. 저작권이 있는 창작물의 복제행위는 아이디어가 아닌 보호가 제공되는 표현물의 복제여야만 한다. 또한 복제물의 복제 비중은 미소(de minimis) 기준을 초과해야만 한다.

인터넷 상 디지털 저작물도 저작권에 의한 보호를 받는다. 다만 디지털 매체의 특성상 디지털 저작물은 타인에 의하여 쉽게 침해당할 소지를 많이 안고 있다.[25] 사이버공간에서의 잠재적인 저작권 침해는 타인에게 전송하기 위하여 소프트웨어 응용프로그램

---

22) Near North National Group, "Understanding Cyber Liability", Near North's Insight Online, 2003. Winter, available at http://www.nnng.com/newsletter/winter2003.

23) 이한상·김준학, 지식재산권법, 제일법규, 2001, p.835.

24) 17 U.S.C. §102(a)(1999).

25) 디지털 저작물은 매체의 특성 상 복제의 저렴·용이, 내용수정의 용이, 다양한 멀티미디어, 저작물 분류의 어려움, 저장의 용이 등의 특성을 갖기 때문에 디지털 저작권은 쉽게 침해당할 소지가 많다(이대희, 인터넷과 지적재산권법, 박영사, 2002, pp.337-339 참조).

을 복제하는 것, 저작권이 있는 정보를 인터넷 상에 게시하는 것, 저작권이 있는 문서를 스캐닝하여 디지털 포맷으로 변환하는 것, 저작권이 있는 정보를 이메일을 통하여 전송하는 것, 저작물을 다운로드하여 하드 드라이버에 저장하는 것, 온라인 광고 및 저작권이 있는 기존의 응용 프로그램과 아주 유사한 새로운 응용 프로그램을 생산하는 것 등의 형태로 나타난다.

② 상표권 침해

상표(Trademark)는 제조물을 표시하는 수단으로 시작되었으나, 오늘날의 상표, 즉 브랜드 자체가 하나의 중요한 무형자산으로서 그 용어 자체가 대단히 포괄적이고 종합적인 의미를 내포한다. 즉 상표라 함은 어떠한 사람이 자기의 업무와 연관하여 개성화된 상품에 표시하여 사용함으로써, 자기의 상품과 타인의 상품을 식별시키기 위하여 사용하는 표장이다. 또한 상표는 문자, 도형 등의 수단을 통하여 상품을 표상함으로써, 상품 소유자는 자기 상품을 형상적으로 표시하고 상품의 출처, 품질, 성능 등을 나타낼 뿐만 아니라, 일반 소비자로 하여금 상품을 연상하게 하는 심리적 작용에 따라 상품을 선별하게 하는 기능을 한다.[26]

서비스마크는 제품보다는 서비스의 원천을 식별하고 구분한다는 점을 제외하면 상품과 동일한 개념이다. 상표라는 용어는 보통 상표 및 서비스마크를 포괄하는 개념으로 사용된다.[27] 특정 기업이 여타 기업에 의하여 현재 사용되고 있는 상표와 동일하거나 유사한 상표를 사용함으로써 소비자에게 혼동의 소지를 제공하는 경우에 상표권 침해가 발생한다.[28]

인터넷을 활용하는 전자상거래는 한편으로 수 많은 상표권 침해의 소지를 제공한다. 전자상거래 기업은 대부분 소비자로부터 기억하기 쉬운 웹 사이트의 도메인명을 소유하려고 하기 때문에 도메인명과 관련한 분쟁이 자주 발생한다. 도메인명과 관련하여 특정 기업이 여타 기업에 의하여 현재 사용되고 있는 도메인명과 동일하거나 유사한 도메인명(예를 들면, mirosoft)을 사용함으로써 소비자에게 혼동의 소지를 제공하는 경우에 상표권 침해가 발생한다.

---

26) 이한상·김준학, 전게서, p.487.

27) Robert W. Hammesfahr, @Risk, Internet and E-commerce : Insurance and Reinsurance Legal Issues, Reactions Publishing Ltd., 2000, p.102.

28) Robert W. Hammesfahr, @Risk, Internet and E-commerce : Insurance and Reinsurance Legal Issues, Reactions Publishing Ltd., 2000, pp.103-104 참조.

특히 도메인명과 관련한 분쟁은 현재의 사용과 관계없는 사이버스쿼터(cybersquatter)[29]에 의하여 더욱 가중된다. *Panavision v. Toeppen* 사건[30]에서 제9차 순회법원은 사이버스쿼터가 'panavision.com'이라는 도메인명을 등록함으로써, Panavision이라는 상표를 가진 원고의 상표권을 침해하였다는 판결을 내렸다. 또한 법원은 사이버스쿼터에 대하여 상표권자는 사용금지명령 및 손해배상청구를 추구할 수 있다고 판결하였다. 왜냐하면 이러한 도메인명은 Panavision으로 하여금 새롭고 중요한 사업매체에 자신의 상표를 사용하는 것을 방해하기 때문이다.

한편, 최근 발생하고 있는 인터넷 관련 상표권 침해의 유형은 검색엔진을 통한 키워드 검색과 관계된다. 즉, 기업이 인터넷 검색엔진의 키워드에 자사의 상표 또는 제품과 전혀 무관한 검색어, 예를 들면 나이키와 같은 유명 브랜드 또는 경쟁기업의 상표를 등록함으로써 소비자를 자신의 웹 사이트로 유인하는 경우이다. 최근 미국의 미공개 법정에서는 이러한 행위에 대하여 당사자의 상표를 무단 도용하는 것으로서 상표권의 침해에 해당한다고 판결하였다.[31]

③ 특허권 침해

특허권은 발명이라고 하는 기술적 사상을 객체로 하여 발명에 대하여 부여되는 권리이다.[32] 특허권은 발명자에 대하여 특허출원일로부터 일정 기간동안 당해 발명품을 제조, 사용 및 판매할 수 있는 배타적인 권리를 부여하는 재산권의 일종이다. 미국의 경우 특허청으로부터 특허권을 취득하기 위해서는 기존 기술과 비교해 볼 때, 당해 발명의 발견, 처리과정 또는 디자인이 진정하고(genuine), 새롭고(novel), 유용하며(useful), 또한 고도의(not obvious) 것이어야 한다.[33]

특허의 보호는 법률의 조건 및 요구사항에 의거하여 새롭고 유용한 공정(제조법), 기계, 제품 또는 물질의 합성을 발명하거나 발견한 일체의 자에게 제공된다.[34] 미국 의회

---

29) 사이버스쿼터는 실제 사용하지도 않는 도메인명(본인의 식별과 전혀 상관없는 도메인명)을 선점하고, 이 도메인명과 직접 연관있는 기업에 대하여 당해 도메인명의 사용을 방해하고, 결국 거액의 금전을 받고 판매하려 자를 지칭한다.

30) 141 F.3d 1316, 1326(9th Cir. 1998).

31) http://zdnet.co.kr/news/internet(2004. 9. 3).

32) 이한상·김준학, 전게서, p.94.

33) Robert L. Miller & Gaylord A. Jentz, Law for E-Commerce, West, 2002, p.110.

34) 35 U.S.C. §101 (1999).

는 "태양 아래 존재하는 한 인간이 만든 모든 사물"에 특허보호를 제공하는 목표를 갖고 있다.[35] 미국에서 새로운 특허에 대한 재산권은 특허출원을 위하여 신청서를 제출한 일자로부터 20년동안 보호가 제공된다. 다만 '자연의 법칙'(law of nature), '자연현상'(natural phenomena), '추상적인 아이디어'(abstract ideas) 또는 '수학적 연산방식'(mathematical algorithms)에 대해서는 특허권이 허용되지 않는다. 예를 들면 아인슈타인의 상대성이론이나 뉴튼의 중력법칙은 특허를 취득하는 것이 불가능하다.[36] 특허권의 침해는 피고가 특허권이 적용되는 제품의 범주 내에 있는 제품을 제작, 사용, 판매, 수입 또는 판매를 위한 청약을 하였다는 사실을 제시함으로써 입증된다.[37]

전자상거래와 관련한 쟁점 중 비교적 분쟁을 적게 야기하는 분야가 특허권과 관련한 분야이다. 과거 소프트웨어의 개발자가 특허권을 취득하는 것은 매우 어려웠다. 왜냐하면 다수의 소프트웨어 상품이 단순히 프로그램을 자동화한 것으로서, 이러한 컴퓨터 프로그램은 특허법 하에서 요구되는 '새로운' 및 '고도의' 요건을 충족하지 못한다고 생각하였기 때문이다. 또한 그러한 소프트웨어는 특허의 대상이 되지 못하는 수학적 연산방식에 의하여 산출된다는 이유 때문이었다. 그러나 1991년 미국 대법원은 프로세스 자체의 특허 취득이 가능하다고 판결함으로써,[38] 컴퓨터 프로그램에 내포된 프로세스에 대한 특허권을 인정하였다. 결과적으로 소프트웨어 관련 발명품에 대해서도 특허권이 부여되었다.

한편, 전통적으로 특허권은 새롭고, 유용한 제조과정, 기계, 제조물품, 물질의 혼합에 해당하는 발명품에 부여되었다. 미국 특허청은 보통 컴퓨터 시스템 및 응용 소프트웨어에 대한 특허권을 인정하지 않았다. 왜냐하면 단순히 수학적 알고리즘, 아이디어의 발췌 또는 '업무수행방식'으로 간주하였기 때문이다.[39]

한편 1998년 *State Street Bank & Trust Co. v. Signature Financial Group, Inc.* 사건[40]에서 미국 연방순회항소법원은 3개 범주의 주제, 즉 자연법칙, 자연현상 및 아이디어는 여전히 특허권 부여의 대상이 아니라고 판결함으로써, 그 결과 업무 프로세스

35) Robert W. Hammesfahr, @Risk, Internet and E-commerce : Insurance and Reinsurance Legal Issues, Reactions Publishing Ltd., 2000, p.107.

36) Diamond v. Diehr, 450 U.S. 175, 182(1981).

37) 35 U.S.C. §271(a)(1999).

38) Diamond v. Diehr, 450 U.S. 175, 101 S.Ct. 1048, 67 L.Ed.2d 155(1981).

39) Robert L. Miller & Gaylord A. Jentz, "Law for E-Commerce", West, 2002, p.111.

40) 149 F.3d 1368(Fed. Cir. 1998).

는 특허권의 부여대상에 포함되었다. 이 판결 이후 업무 프로세스에 대한 특허권이 광범위하게 신청되었고, 또한 미국 특허청에 의하여 인정되었다.

예를 들면, 이 사건 이후, Jay Walker가 설립한 Walker Digital은 소비자에 대하여 경매방식으로 항공권을 판매하는 소위 '네덜란드식 경매'(Dutch Auction)방식에 대하여 특허권을 취득하였다. 특허권의 취득 후에 Priceline.com이 탄생되었고, 당해 기업은 얼마 지나지 않아 US $180억의 주식가치를 가진 기업으로 성장하였다. 이와 더불어 기업의 주식을 50%를 보유하였던 Jay Walker는 순식간에 백만장자가 되었다.[41]

한편 웹 사이트 상 데이터베이스에 대해서도 특허권이 인정된다. 따라서 미국 특허청이나 유럽특허사무국(European Patent Office : EPO)이 보유한 특허정보 관련 데이터베이스도 특허권이 인정된다.

(3) 태만 또는 주의의무위반에 대한 불법행위책임

전자상거래와 관련하여 인터넷 사용자의 태만(Negligence) 또는 주의의무의 위반에 대한 책임문제는 다양한 방식으로 초래될 수 있으나, 대표적인 경우는 익명의 자가 악성 바이러스를 개발 및 유포한 경우이다. 보험원칙의 문제로서 피보험자가 고의로 바이러스를 유포함에 따른 법적 책임을 담보하려는 보험자는 없을 것이다. 또한 다수 경우에 악성 바이러스의 개발자 및 고의적인 유포자의 정체는 파악되지 않기 때문에 바이러스 유포에 따른 근원적인 책임주체의 확인 자체가 어렵다.

다른 한편, 컴퓨터 사용자의 고의는 개입되지 않았더라도, 사용자가 정상적인 방법으로 안티-바이러스 프로그램을 설치 또는 실행하지 않은 결과, 바이러스에 감염된 실행 프로그램을 타인에게 전송하고 타인의 컴퓨터를 감염시킨 경우, 그 사용자의 태만 또는 주의의무위반에 대한 불법행위책임의 여지는 남는다.[42] 물론 기존의 안티-바이러스 프로그램으로 탐지 또는 치유할 수 없는 강력한 신종 바이러스의 경우에는 예외지만, 컴퓨터 사용자가 정상적·정기적으로 안티-바이러스 프로그램을 설치·업데이트·실행하지 못함으로써, 바이러스의 감염 및 확산으로부터 제3자를 보호하는 데 실패한 경우

41) 하지만 당해 기업은 기대한 만큼 수익이 발생하지 않았고, 그로부터 얼마 지나지 않아 2001년에 수백만 달러 가치의 기업으로 전락하였다.

42) 바이러스의 유포와 관련한 주의의무의 당위성은 컴퓨터 바이러스가 초래하는 위험의 심각성에 관하여 사회적인 공감대가 형성되어 있고, 기존의 바이러스를 탐지하거나 치유할 수 있는 수많은 프로그램이 개발되어 있다는 사회적 여건에서 찾을 수 있다.

그는 태만이라는 기여과실에 대한 책임을 면하지 못할 것이다.

한편 전자상거래 기업는 기업 컴퓨터 시스템의 유지·관리에 관한 기업의 주의의무를 다하지 못한 경우에 배상책임에 직면한다. 예를 들면, 기업 컴퓨터 시스템의 기능장애로 인하여 기업고객에게 손해를 입히고, 기업이 이에 대하여 배상책임을 부담하는 경우이다. 전자상거래에 종사하는 기업의 경우, 제3장에서 언급한 컴퓨터 시스템의 기능장애는 고객과의 거래중단을 초래한다. 그 결과 기업고객이 막대한 상업손실을 입고, 그러한 컴퓨터 시스템의 기능장애가 기업의 시스템 유지·관리에 관한 주의의무 위반에 기인하였다면, 기업은 고객의 손실에 대하여 배상책임을 부담한다.

다른 한편, 기업 컴퓨터의 보안상 결함도 기업고객에 대하여 손해를 초래한다. 예를 들면, 보안실패로 인하여 기업고객의 신용정보(대표적으로 신용카드정보)가 도난되고, 그로 인하여 고객이 경제적 손해를 입었다면, 기업은 고객의 손해에 대하여 배상책임을 부담한다.

(4) 개인정보보호의무의 위반에 대한 불법행위책임

오늘날 정보통신기술이 발전함에 따라서 방대한 양의 정보가 용이하게 수집·저장·교환되고 있는 반면, 기업이 전자상거래와 관련하여 고객에 대하여 개인정보(예를 들면, 개인 신상, 개인 신용 및 개인의 구매습관 등에 관한 정보)를 제출하도록 요구함으로써, 그러한 정보의 유출·오용·남용·악용에 의한 프라이버시 침해는 심각한 사회문제로 대두되고 있다. 미국의 한 조사에 의하면, 인터넷 이용자 중 81%가 온라인에서 개인 프라이버시에 대한 침해를 우려하고 있고, 우리나라의 경우에도 인터넷을 통한 전자상거래의 기피사유로서 개인 및 신용정보의 유출에 대한 우려가 두 번째 순위를 차지하는 것으로 나타났다.[43]

피보험자가 전자상거래를 수행하는 과정에서 자기의 부주의 또는 시스템보안 상의 문제에 기인하여 법적으로 보호되어야 할 개인정보를 유출하거나 개인 프라이버시를 침해한 경우에는 불법행위에 해당하고, 개인정보의 수집목적이나 이용방법의 사유가 위법인 경우에는 민사상 손해배상청구의 대상이 된다.

---

43) 정영화·남인석, 『전자상거래법』, 다산출판사, 2000, p.212.

(5) 태만한 부실표시에 대한 불법행위책임

월드와이드웹은 개인이나 기업 또는 소기업이나 대기업에 상관없이 전세계 시장에 자기를 소개할 수 있는 동일한 기회를 제공한다. 웹사이트 상의 정보는 다양하고 상이한 목적, 즉 제품의 광고나 소비자에 대한 서비스제공, 전문·유료서비스를 위한 광고 또는 전문가 소개, 자선단체의 목적 설명, 제품사용법이나 제품사용과 관련한 조언 제공 등의 목적을 위하여 제공된다. 정보는 단순히 웹사이트 상에서 수동적으로 열람하는 방식으로 제공될 수도 있고, 실시간 문답식 또는 이메일을 통한 문답식으로 일정기간이 지난 후에 제공되기도 한다.

유사한 이해관계를 가진 참가자들이 포럼의 주제와 관련된 문제를 제시하고 그 문제에 대한 해답을 구하고자 하는 경우에 현재 막대한 양의 정보가 뉴스그룹이나 전자게시판을 통하여 제공되고 있고, 따라서 뉴스그룹이나 전자게시판은 정보취득을 위한 시장역할을 한다.[44] 이러한 매체는 월드와이드웹의 출현 이전, 즉 인터넷이 주로 대학교수들 사이에서 자유로운 정보교환을 촉진하기 위한 목적으로 사용되던 시기에 기원을 두고 있다.[45] 이 경우 정보는 상호협력의 정신 하에서 제공된 것이기 때문에 부정확하거나 오인된 정보의 제공과 관련하여 상대방에 대한 법적 책임이 초래될 여지는 없었다. 이윤동기의 부재가 정보제공자의 주의의무의 존재를 완전히 부정하는 것은 아니지만, 그것이 주의의무 위반에 따른 불법행위책임과 관련하여 가장 중요한 고려사항이라는 사실은 부정할 수 없다.

다른 한편, 소프트웨어의 소유권자가 당해 소프트웨어와 관련되는 문제를 해결하기 위한 수단으로써 인터넷 상의 그룹토의에 참가하는 경우, 부정확한 조언의 제공에 기한 불법행위책임에 직면할 수도 있다. 왜냐하면 그러한 조언이 채팅그룹이나 소프트웨어 판매자의 웹 사이트에서 제공되느냐 여부에 상관없이 또는 정보제공의 대가가 금전이라는 유상의 형식을 채용하였느냐 여부에 상관없이 그러한 정보제공으로 인하여 소프트웨어 판매자의 지명도와 명성이 제고된다는 사실만으로 여전히 상업적인 동기를

---

44) 인터넷 환경 하에서 사람들은 스스로 해결이 불가능한 문제에 봉착하였을 때 타인이 해결방안을 제시해 줄 것이라는 믿음을 갖고서 사이버공간에서 이방인의 문제해결을 위하여 기꺼이 자신의 시간을 할애할 준비를 갖추고 있다.

45) 인터넷(Internet)은 Inter와 Network의 합성어인 Internetwork의 약어로서 전세계에 산재해 있는 네트워크를 연결하는 네트워크이다. 인터넷은 초기에 대학이나 연구소 중심의 학술정보교환용으로 사용되었으나, 점차 상업용목적의 사용이 증대하였고, 특히 1994년 월드와이드웹의 출현 이후 폭발적인 성장을 하고 있다(尹光云 · 張斗彩 · 金喆浩, 『電子商去來論』, 三英社, 1999, p.41).

내포한다고 할 수 있기 때문이다. 더욱이 전문적·기술적 조언제공의 대가가 신용카드에 의한 일시납부방식 또는 연간·월간 회비납부방식을 채택한 경우, 그러한 서비스의 제공자는 태만한 부실표시(Negligent Misrepresentation)에 기인한 책임을 회피할 수 없다.

4. 기타 위험

전술한 위험의 범주에 포함되지 않으나, 특히 전자무역기업의 입장에서 간과할 수 없는 두 가지 형태의 위험이 존재한다. 첫째, 국제 전자상거래에 종사하는 기업에 한정하여 재판관할권 위험(Jurisdictional Risk)이 존재한다. 최근 현실공간에서 국제무역에 종사하고 있는 상인은 재판관할권의 다양성으로 인한 재판관할권 위험을 상당한 수준까지 관리할 수 있다. 왜냐하면 국제상거래에 통일적으로 적용되는 국제상관습 및 국제협약 등이 잘 발달되어 있고, 비록 그 적용이 배제되더라도 국제무역상들은 특정한 거래상대방의 국적을 인지함으로써 필요한 상대국의 법 지식을 습득하거나 법률전문가로부터 법적 조언을 받을 수 있기 때문이다.

인터넷을 통한 전자상거래는 오프라인 거래와는 달리 불특정·다수를 상대로 한 비대면 거래 및 국경 없는 거래라는 특성을 갖는다.[46] 즉 전자상거래 기업은 거래상대방의 다양한 국적 및 문화적 상이성으로 인하여 전자상거래 기업은 재판관할권 위험을 효율적으로 관리할 수 없는 상황에 직면한다. 전자상거래 기업이 불특정·다수인 거래상대방 국가의 전자상거래 관련법률에 대한 법률 지식 또는 조언을 일일이 취득하는 것은 불가능하고, 설령 그것이 가능하더라도 전자상거래 관련 법제가 각국에서 아직 정비되지 않았다는 점을 감안할 때 분쟁이 발생하는 경우 거래상대방 국가의 법률 지식 또는 법적 조언이 각국 법원의 판단을 정확히 예견할 수 있다는 보장은 없기 때문이다.

둘째, 법률서비스 비용발생의 위험이 존재한다. 인터넷을 이용한 전자상거래는 상당히 급속하게 발전되고 있기 때문에 전자상거래와 관련한 법적 불확실성이 존재하고, 이는 전자상거래 기업에 대하여 빈번한 분쟁발생 및 법률서비스 비용발생의 증대를 의미한다. 예를 들면 계약의 성립시기와 관련하여 전자상거래를 격지자간 거래로 볼 것

46) 盧泰嶽, "電子去來에 있어서 契約의 成立을 둘러싼 몇가지 問題", 『法曹』 통권 516호, 1999. 9, pp.54-56.

인가 아니면 대화자간 거래로 볼 것인가의 문제 또는 전자문서의 증거법상 지위에 관한 문제에 대하여 이견의 여지는 남아 있다.[47] 결국 전자상거래와 관련한 법적 불확실성이 완전히 제거될 때까지 전자상거래 기업은 배상청구액을 초과하는 소송비용을 지출할 수 있는 가능성도 배제할 수 없다.

47) 盧泰嶽, "電子去來에 있어서 契約의 成立을 둘러싼 몇가지 問題", 『法曹』 통권 517호, 1999. 10, pp.120-142.

Ⅳ. 전자무역기업의 위험관리

1. 컴퓨터 시스템의 기능상실

제3장에서 언급한 전자상거래의 고유한 성격에 기인하여 발생하는 컴퓨터 시스템의 장애로 인한 전자무역기업의 직접비용손해는 대부분 전자상거래 보험의 본인손해담보 하에서 보상된다. 다만 화재나 도난과 같은 물리적 위험은 전자상거래의 성격에 고유한 위험의 범주에서 벗어나는 전통적인 위험으로서 전통적인 보험에 의하여 커버되어야 한다. 즉 화재나 도난의 경우, 화재보험이나 도난보험에 의하여 커버되거나 또는 기업재산보험에 의하여 커버된다. 한편 기업의 입장에서 물리적 위험에 부수하는 업무장애 위험을 최소화하기 위해서는 기업의 물리적 영업장소 외부의 안전한 장소에 백업 시스템을 구축해 두거나, 위험의 분산을 위하여 중요한 네트워크 구성요소를 물리적으로 상이한 공간에 설치해 두는 것이 바람직하다.

한편 소프트웨어의 결함 또는 컴퓨터 프로그램의 오류에 기인한 기업 컴퓨터 시스템의 기능상실 또는 기능저하에 의한 손해는 일반적으로 본인손해담보 하에서 보상되지 않는다. 본인손해담보 하에서 제외되는 기업의 비용손해를 열거하면 다음과 같다.

· 정부기관 등 공권력의 행사에 의한 보험목적물의 징발, 몰수, 국유화 또는 파괴되어 피보험자에게 직·간접적으로 손해를 유발한 경우

· 컴퓨터 시스템의 일상적인 마모 또는 점진적인 성능저하의 결과 발생한 손해

· 인공위성의 고장으로 인한 손해

· 전기시설, 데이터 송신라인 또는 사회간접자본의 고장으로 인하여 초래되는 전력차단, 불안정한 전력의 흐름 등으로 인하여 초래된 손해

· 소프트웨어 또는 프로그램의 사용불능 또는 성능의 결함으로 인하여 초래된 손해

· 퇴사한 종업원이 컴퓨터 시스템에 대하여 무단으로 접속한 결과 발생한 영업비밀의 노출에 따른 손해

2. 영업장애로 인한 간접비용

기업은 건물이나 기계 등 자산을 보유하고 종업원에 대한 급여 및 영업비용 등을 지

출하는 과정에서 영리활동을 추구한다. 기업의 영리활동은 물적 재산의 직접손해에 기인하여 위축되거나 중단되기도 하지만, 직접손해에 후속하여 발생하는 영업이익의 상실이나 추가경비 등의 간접손해에 의해서도 기업의 영리활동은 상당한 영향을 받는다. 일반적으로 기업의 물적 재산은 재산보험이나 기업종합보험에 의하여 보호되지만, 기업의 영업능력은 이들 보험에 의하여 보호되지 않는다.[48] 예를 들면 화재로 인한 기업의 물적 손해는 화재보험에서 담보되지만, 화재로 인한 영업이익의 상실분이나 추가경비 등 간접손해는 일반적으로 업무장애보험(business interruption insurance)이나 간접손해보험(consequential loss insurance)[49] 하에서 담보된다. 업무장애보험에서 보험금은 업무중단기간동안의 영업이익의 상실분 + 영업비용으로 산정되고,[50] 추가로 피해복구를 위하여 피보험자가 지출한 추가비용도 보험금에 산입된다.

전자상거래 보험 하에서 보상되는 간접비용손해는 컴퓨터 시스템의 손상이나 파괴에 후속하여 발생되는 영업이익의 상실, 복구비용 및 데이터 재수집·재입력에 소요되는 비용이다. 이러한 비용은 배상책임담보 하에서는 담보되지 않고, 종합전자상거래 보험 하에서 피보험자의 선택에 의하여 본인손해에 대한 추가담보로서 본인손해담보와 함께 구매가 가능하다. 영업중단으로 인한 간접손해는 주로 시간요소(time element)에 기인한 유형의 비용에 의하여 산정된다.[51] 따라서 손해산정 시에 시스템의 교체기간 중 발생한 수익의 상실, 시스템의 재설정 시간, 상실된 데이터의 복구 시간, 데이터의 재수집·재입력 시간, 사고조사 시간이 중요한 요인으로 고려된다. 결국 당해 담보주제 하에서 영업중단기간 중 피보험자에 대하여 발생하는 무형의 손해, 즉 영업중단으로 인한 기업의 명성이나 신뢰도의 하락으로 인한 손해, 기업의 이미지를 제고하기 위하여 지출하는 이미지광고비용 등은 담보되지 않는다.

---

48) Why Business Interruption Insurance, http://www.axa-insurance.co.uk/guides, 2001. 2. 12.

49) 일체의 간접손해, 즉 시장상실이나 계약체결기회의 상실로 인한 손해도 담보가능하지만, 영업이익의 상실분이나 추가경비가 표준적인 담보영역이므로 이 보험을 이익상실보험(loss of profit insurance)이라고도 한다(Nicholas Legal-Jones(ed.), MacGillivray on Insurance Law, 9th ed., Sweet & Maxwell, 1997, p.856 ; D.S. Hansell, Introduction to Insurance(2nd ed.), LLP, 1999, p.57 참조).

50) 예를 들면, 손해발생전 회계연도에 순이익+영업비용이 총매출액 £80,000의 40%를 점하였고, 화재발생 후 총매출액이 £30,000으로 감소하였다면, 보험금은 총매출액의 감소분(£50,000)의 40%에 해당하는 £20,000이 된다.

51) Dan Geer, "Solution to Problems", http://www.andrew.cmu.edu/user/hchong.

3. 불법행위책임

전자상거래에 종사하는 기업 또는 컴퓨터 시스템의 관리자는 본인의 고의나 과실에 기인하여 타인 또는 여타 기업에 대하여 손해를 초래하는 경우, 민·형사상 법적 책임을 면할 수 없게 된다. 전자상거래 보험에서 담보되는 법적 책임은 민사상 불법행위에 기하여 초래된 타인에 대한 손해배상책임으로서, 피보험자가 현행 법률을 위반함으로써 초래되는 형사상 징벌적 성격의 형사처벌, 벌금 또는 피보험자가 피해자에게 위로금 성격으로 제공하는 금전 등은 보험보호의 대상이 되지 못한다.

한편 전자상거래 또는 인터넷활동과 관련하여 기업이 민사상 불법행위책임, 즉 피해당사자에 대하여 손해배상책임을 부담하는 경우, 그러한 책임은 일반적으로 전자상거래종합보험의 제3자에 대한 책임담보(Third-Party Liability Coverage) 또는 별도의 사이버배상책임보험(Cyber Liability Insurance) 하에서 담보된다. 다만 보험원칙의 문제로서 불법행위책임의 유형에 상관없이 당해 불법행위가 피보험자의 과실, 즉 실수, 착오, 오류 등에 의하여 행하여진 경우에 한하여 담보가 제공된다. 따라서 당해 불법행위가 피보험자의 고의적 또는 악의적 의사에 의하여 행하여진 경우, 보험자는 면책이다.

예를 들면, 피보험자가 원한이나 악의적인 감정을 갖고서 타인이나 타기업을 비방하거나 허위사실을 유포함으로써 타인의 명예훼손에 대한 배상책임을 부담하는 경우, 피보험자의 고의, 악의 부정직 또는 무모함에 의하여 타인의 지적재산권을 침해함으로써 배상책임을 부담하는 경우, 피보험자가 개발한 바이러스를 타인에게 전송함으로써 그로 인한 배상책임을 부담하는 경우에는 보험자 면책이다. 여기서 피보험자는 피보험기업의 대표이사, 피보험자의 이사·임원 및 피고용인을 포함하는 개념이다.

한편 이 담보주제와 관련하여 유의할 사항은 다음과 같다. 첫째, 태만 또는 주의의무위반과 관련하여 담보범위는 피보험자와 '거래하는 자' 또는 '거래를 위하여' 피보험자가 구축한 웹 사이트에 접속하는 자에 한정한다는 점이다. 여기서 피보험자와 '거래하는(doing business) 자'의 개념이 문제가 될 수 있다. 만약 소비자가 거래에 관련된 문의를 하고 이에 대한 회신목적으로 전송된 이메일을 통하여 바이러스가 전송된 경우라면 그러한 문의 자체로서 '거래'라고는 하기 어렵고, 영리추구를 목적으로 하지 않는 자선단체의 활동에 '영업상'이란 개념이 적용될 여지는 없을 것이다.[52]

---

52) C.C. Nicoll, op. cit., p.301.

둘째, 전자상거래 기업, 온라인 중개인 또는 온라인 전문직상담자에 의한 태만한 부실표시에 대한 배상책임은 일반적으로 전통적인 전문직배상책임보험 하에서 담보되는 위험으로서, 전자상거래 보험 하에서는 담보되지 않는다.

셋째, 불법행위책임 담보와 관련하여 가장 중요한 예외로서, 피보험자의 특허권 침해 행위와 관련한 일체의 배상책임은 전자상거래 보험 하에서 커버되지 않는다. 이 면책은 보험증권의 형식 또는 발행국가를 불문하고 명시적으로 면책으로 규정하고 있다. 전자상거래에 종사하는 기업은 특허권 침해에 기여하거나, 단독으로 특허권을 침해할 위험에 직면할 가능성이 상당히 높다. 즉 피보험자는 전형적으로 침해된 제품을 제조하지는 않으나, 침해 제품을 사용, 판매 또는 광고할 가능성은 항상 존재하기 때문에 특허권 침해에 대한 면책은 다소 의외라고 할 수 있다.[53]

한편 배상책임담보 주제 하에서 커버되지 않는 주요 위험 또는 손해를 열거하면 다음과 같다.

- 신체 장해 및 피보험자가 소유하는 재산에 대한 직접적 손해
- 증권거래법, 공정거래법 등 법률위반으로 인하여 피보험자가 부담하는 벌금 및 책임손해
- 특정 계약 하에서 피보험자의 의무위반 또는 계약불이행으로 인하여 부담하는 손해배상금
- 피보험기업의 임원에 의하여 행하여진 사기적·범죄적·악위적 행위에 기인한 손해. 다만 이 경우 피보험자가 임원의 무고함을 입증하기 위하여 변호사 비용을 지출하는 경우에 그러한 법적방어비용은 결과적인 유·무죄 여부에 상관없이 보상한다.
- 피보험자 상호간의 손해배상청구. 여기서 피보험자의 범위는 피보험자, 피보험자를 대리하는 자 또는 피보험자가 직·간접적으로 소유·관리·운영하는 사업체로서 구체적으로는 피보험자의 모회사, 자회사, 피보험기업의 승계 및 양수인 또는 피보험자가 소유 또는 통제하는 일체의 사업체를 포함한다. 다만 여기서 피보험자의 고객은 피보험자의 범주에 포함하지 않는다.
- 인공위성의 고장이나 전력공급중단에 기인한 손해배상책임
- 특허권의 침해에 기인한 손해배상책임
- 제품, 생산물 또는 서비스가격의 부실표시, 또는 광고한 품질 및 내용과 다른 제품, 생산물 또는 서비스에 기인한 손해배상책임

---

53) Michael A. Rossi, "New Stand-Alone E-Commerce Liability Insurance for Third-Party Liability Claims", Part 2, Insurance Law Group, 2000. 12, http://irmi.com/Expert/Articles/2000/Rossi12a.aspx, p.1.

V. 전자상거래 보험시장의 현황 및 쟁점

1. 전자상거래 보험시장의 현황 및 전망

1990년대 후반에 전자상거래 보험을 도입한 미국의 경우, 현재 다양한 보험회사가 다양한 전자상거래 보험상품을 취급하고 있다([표-3] 참조). 전자상거래 보험을 판매하는 시장 선도자는 ACE, AIG, CNA, Hiscox, Chubb, St. Paul, Sacia, Zurich 등이 있으나, 시장점유율 측면에서 AIG, ACE, Hiscox 순으로 추정된다.[54] 미국 보험시장에서 현재 판매되고 있는 전자상거래 보험의 종류 및 담보범위는 [표-3]과 같다. [표-3]에 나타나는 일부 보험회사의 경우(Gulf, Royal, St. Paul, Tamarak), 중소기업을 대상으로 전자상거래 관련 배상책임보험을 판매하고 있고 최소 보상한도(US $2백만 - 3백만)를 제시하고 있는 반면, 일부 보험사의 경우(AIG, Hiscox, Lloyd's, Marsh), 대기업을 포함한 전체 기업을 대상으로 전자상거래 종합보험을 판매하고 있으며 다소 높은 보상한도(US $2천만 - 3천만)를 제시하고 있다.[55]

[표-3] 미국 보험시장에서 판매되고 있는 전자상거래 보험의 종류 및 담보범위[56]

보 험 자	보험상품명	제3자 범죄	종업원의 부정행위	업무장애 및 추가경비	디지털재산의 강탈	전문직서비스 배상책임	미디어작위·부작위배상책임
AIG	NetAdvantage Pro	×	×	×	×	○	○
AIG	NetAdvantage Security	○	○	○	○	×	○
AIG	ProTech	×	×	×	×	○	○
Chubb	Cyber Security	○	○	○	○	×	×
Chubb	Safety'Net Internet Liability	×	×	×	×	×	○
Hiscox	Hacker Insurance	○	○	○	○	○	○

54) Michael A. Rossi, "Cyber Liability Insurance Issues for Large Companies : Market Status Update for Summer of 2003 and Tips for the Buyer", (2003. 11), http://www.irmi.com/Expert/Articles/2003.

55) Michael A. Rossi, "New Stand-Alone E-Commerce Insurance Policies for First-Party Risks", Insurance Law Group, 2001. 2, http://irmi.com/Expert/Articles/2001/Rossi02.aspx.

56) Michael A. Rossi, "Stand Alone E-Commerce Market Survey", Insurance Law Group, 2001. 7, http://irmi.com/Expert/Articles/2001/Rossi02-1.aspx.

보 험 자	보험상품명	제3자 범죄	종업원의 부정행위	업무장애 및 추가경비	디지털재산의 강탈	전문직서비스 배상책임	미디어작위·부작위배상책임
Legion	INSUREtrust	일부	일부	×	×	○	○
Lloyd's	Computer Informationd and Data Security	○	○	○	○	○	○
Lloyd's (WISP)	Website Crime & Intranet	○	○	○	○	×	×
Lloyd's (Besso)	Technology, Media and Professional Liability	×	×	×	×	○	○
Lloyd's JLT Risk Solutions	E-Comprehensive	○	○	○	○	○	○
Gulf	CyberLiability	×	×	×	×	○	○
Royal	Computer,Telecommunications and Internet Service Liability	×	×	×	×	○	○
St. Paul	Tech.Premier Computer Network Security Protection	○	○	○	○	×	×
St. Paul	Cybertech	×	×	×	×	○	○
Tamarak	Dot.Com E&O Liability	×	×	×	×	○	○
Zurich	E-Risk Protection	○	○	○	○	×	○
Marsh	NetSecure	○	○	○	○	○	○

한편 우리나라에서는 현재 본인손해 및 제3자에 대한 책임손해를 모두 커버하는 Net-Secure종합보험(또는 전자상거래종합보험) 및 배상책임손해만을 커버하는 e-biz@배상책임보험이 판매되고 있다.[57] 1999년 8월 현대해상화재가 보험업계 최초로 금융감독원으로부터 E-Business배상책임보험에 대한 인가를 취득한 이후, 현재는 현대해상화재를 포함한 3개 손해보험사가 Net-Secure종합보험을 취급하고 있고, 나머지 손해보험사가 e-biz@배상책임보험을 취급하고 있다.[58] 한편 손해보험협회에서 수년 전에 발표한 보도자료에 의하면 2002년 9월 현재, 755개 전자상거래 업체 중 Net-Secure종합보험에 가입한 업체는 169개 업체로 가입률은 22.4%에 불과한 것으로 나타났다.[59] 참고로 현재 구입가능한 자료에 의하면, 우리나라 전자상거래 기업의 보험가입현황 및 e-biz@배상책임보험의 실적은 다음과 같다.

---

57) Net-Secure종합보험의 경우, 보험증권의 구성은 SectionⅠ.일반보험조건, SectionⅡ.배상책임담보조항, SectionⅢ.재물손해담보조항, SectionⅣ.컴퓨터범죄담조조항, SectionⅤ.위기관리비용담보조항으로 구성되어 있고, e-biz@배상책임보험의 담보부문은 SectionⅢ.재물손해담보에 해당한다.

58) 조혜원, 개인정보유출 관련 보험제도 활성화방안, 「주간보험이슈」 제72호, 보험개발원, 2005. 5. 11.

59) http://www.kidi.co.kr/instrend/news.

[표-4] 전체 전자상거래 보험의 가입실적

단위 : 천원

보험기간	가입건수	보험료
2000. 4 - 2001. 3	154	4,397,000
2001. 4 - 2002. 3	169	4,590,000
2002. 4 - 2002. 12	140	4,394,000

출처 : 인터넷녹두신문, 2003. 1. 29, http://inp.or.kr/liguard_bbs

[표-5] e-biz@배상책임보험의 보험실적

단위 : 천원

보험연도	원수보험료	원수보험금
2001	528,649	-
2002	1,507,298	150,429
2003	2,568,476	85,728

출처 : 조혜원, 개인정보유출 관련 보험제도 활성화방안,
「주간보험이슈」 제72호, 보험개발원, 2005. 5. 11.

한편, 전자상거래 보험시장의 전망과 관련하여 주요 보험자는 "21세기에 들어와서 보험이 커버해야 할 단일 최대의 위험"이 사이버위험이라고 믿고 있다.[60] 일부 전문가에 의하면 2005년 전세계 전자상거래 보험시장의 규모는 US $1조의 규모에 달할 것으로 전망되고,[61] 2-3년 후인 2007년 내지 2008년에는 시장규모가 US $2조-3조에 달할 것으로 전망하고 있다.[62]

60) H. Wesley Sunu, Rober Paul Norman, Katherine S. Kamen, Larry P. Schiffer and Adam B. Perri, "Recent Development in E-Commerce", Tort Trial & Insurance Practice Law Journal, Vol.37, No.2, Winter 2002, p.346.

61) ISO, "ISO introduces Cyber Risk Program to help cover $7 Trillion E-Commerce Market", http://www.iso.com/press_release/2005.

62) Insurance Information Institute, Press Release(2003. 8. 13), http://iidev.iii.org/media/updates/press.731722.

2. 전자상거래 보험과 관련한 쟁점

(1) 담보위험의 표준화와 관련한 문제

전자상거래에 대한 보험증권은 사이버 위험의 독특한 성격을 반영함으로써, 증권의 내용이 방대하고 복잡한 형식을 취할 뿐만 아니라, 담보범위의 통일성이 부재하고 개별 보험자]에 따라 담보위험의 범위가 다양한 상황이다.[63] 예를 들면 일부 보험사는 업무장애로 인한 간접손해 및 컴퓨터범죄에 대한 담보를 제공하는 반면, 여타 보험사는 불법행위책임에 대한 담보만을 제공하고 있고, 또한 일부 보험사는 태만한 부실표시에 대한 불법행위책임을 담보하고 있다. 물론 인수위험의 다양화는 전자상거래 보험의 위험모델 및 보안모델이 정립되어 있지 않다는 사실에 기인하지만, 그렇다고 하더라도 담보위험의 비표준화는 피보험자로 하여금 보험계약의 내용검토 및 법률적 해석을 위한 변호사비용 등 추가비용의 지출을 초래하게 될 것이다.[64]

(2) 보험료 산정과 관련한 문제

보험료 산정 문제와 관련하여 초래되는 문제는 3가지로 정리할 수 있다. 즉, 첫째, 보험료 산정의 정확성 문제이다. 보험상품의 가격산정은 전통적으로 방대한 역사적 기록을 토대로 작성된 보험통계표에 의존한다. 인터넷은 상대적으로 새로운 것이기 때문에 인터넷 관련 범죄 및 손해액에 관한 방대한 통계자료는 존재하지 않는다. 현존하는 정보보안 문제의 기록보관소(www.cert.org)는 불과 수년의 기록만을 보유하고 있고, 기업이 보안문제에 관하여 상세한 사항을 공개하지 않는다는 사실에 의하여 기록보관의 어려움을 겪고 있다. 이러한 상황에도 불구하고, 보험회사는 사이버위험 보험에 대한 가격을 산정하고 있다. 따라서 보험기업은 계량화할 수 없는 위험을 계량화하고 있다고 말할 수 있다. 결국 보험료 산정과 관련한 사이버위험의 불확실성을 가정한다면, 보험료산정방식의 정확성 여부에 관한 의문이 남는다. Radcliff는 "이 보험상품은 아주 새로운 상품이기 때문에 우리가 위험에 대하여 올바른 보험료를 산정하는가에 대한 의문

---

63) John E. Black Jr., Lorelie S. Masters & David S. Weitzel, "Dangers Lurk in Cyberspace", Business Law, Vol.11, No.6, July/August 2002, http://www.abanet.org/buslaw, p.4.

64) 박석재·신건훈, 전자상거래 보험의 문제점과 해결방안, 무역학회지 제26권 제4호, 2001. 9, p.165.

을 초래한다."[65]고 지적하고 있다.

둘째, 높은 수준의 보험료와 관련한 문제이다.[66] 전자상거래 보험의 경우 고수준의 보험료가 부과된다. 전자상거래 위험과 관련하여 전통적인 보험사들은 아직까지 기존의 보험비용산출기법을 디지털화된 전자자산에 대하여 합리적으로 적용하지 못하고 있고, 위험모델이 정립되지 않은 상태에서 전자상거래 보험의 취급에 따른 위험을 감수하려 하지 않기 때문에 높은 수준의 보험료를 요구하고, 따라서 다수의 소규모 사업자는 보험료를 감당할 수 없는 상황이다.[67]

셋째, 상기 문제와 별개로 보험료의 적용폭(spread)이 너무 크다는 점이다. 보험전문가인 Richard Hunter는 "보상한도 2천 5백만 달러인 사이버 배상책임보험에 대한 보험료는 연간 US $25,000-125,000으로 다양하다. 기존의 보험상품에서 보험료가 500%의 변동폭을 갖는다는 것은 상상할 수 없다. 이 사실은 보험회사들의 위험평가기법이 아직 정착되지 않았음을 의미한다"라고 지적하고 있다.[68] 보험료의 변동폭이 크다는 사실은 보험사의 위험평가기법의 미정착뿐만 아니라 피보험자의 컴퓨터 네트워크에 대한 보안시스템의 안전도, 인증 시스템의 신뢰도 및 전자상거래 분쟁에 관한 법제의 미정비를 반영하는 것이지만, 보험료의 변동폭이 크다는 사실은 결국 피보험자로 하여금 보험자의 보험료산출방법의 정당성 및 합리성에 대한 불신을 초래하는 요인이 되고 있다.

(3) 역선택과 관련한 문제

역선택의 문제가 전자상거래 보험에 고유한 것은 아니지만, 전자상거래 보험은 일반보험과 마찬가지로 역선택(Adverse Selection)의 문제에 직면할 가능성이 크다. 보험거

---

65) D. Radcliff, "Calculating e-risk", Computer World 35, Feb. 12, 2001, p.34.

66) 박석재·신건훈, 전게 논문, p.164.

67) 예를 들면 업무장애담보에 대한 보험료는 전자상거래 사이트의 매출액 및 보안수준에 근거하여 산정되나, 웹매출액이 연간 US $4천만인 기업이 60일간 업무중단을 커버하는 보험계약을 체결하는 경우에 연간 US $50,000-70,000를 지출해야 하고, 이보다 소규모인 기업의 경우 US $100,000의 보상을 받기 위하여 연간 US $1,000-2,000의 보험료를 지출해야 한다. 불법행위책임담보의 경우 US $1백만의 보상한도 하에서 연간 최소 US $2,500의 보험료를 지출해야 하고, 컴퓨터범죄담보에 대한 보험료는 연간 약 US $7,000이다(Susan Breidenbach, "The Policy of Protection", http://nwfusion.com/research/2000, 2000. 10. 23).

68) Susan Breidenbach, "The Policy of Protection", http://nwfusion.com/research/2000, 2000. 10. 23.

래와 관련하여 역선택은 보험가입을 선택한 기업(또는 개인)이 보험계약의 체결 시에 보험회사에게 고지되지 않는 비밀정보를 보유할 가능성이 많기 때문에 발생하는 문제를 언급한다. 예를 들면, 건강이 좋지 않은 사람이 평균적인 사람보다 건강 또는 생명보험을 취득할 가능성이 높다. 건강 및 생명보험에 대한 역선택 문제를 취급하기 위하여 보험자는 보험계약이 체결되기 전에 물리적 신체검사를 요구하고, 라이프 스타일의 특성(예를 들면, 흡연자인가 여부)에 의하여 차별화한다.

전자상거래 보험의 경우, 역선택의 문제는 보안상 문제와 관련하여 명백해진다. 정보보안 상 문제발생의 가능성이 높은 기업이 낮은 기업보다 전자상거래 보험을 구매하는 경향이 클 것이다. 이러한 역선택의 문제는 보험회사의 경영과 관련하여 심각한 문제를 초래할 수도 있다. 보험회사는 이러한 문제를 회피하기 위하여 전자상거래 보험을 제시할 때, 보통 피보험기업의 보안시스템에 관한 감사를 요구한다. 이러한 감사를 통하여 보험회사는 피보험기업의 보안상태 및 위험 정도를 가능한 한 정확하게 측정할 수 있다. 보험회사가 보안감사를 통하여 고수준의 위험을 보유한 기업을 식별하고, 그러한 기업에 대하여 보험료를 차별 적용하면 역선택에 따른 문제를 다소 회피할 수 있을 것이다. 예를 들면, 해킹위험에 대한 보험을 제공하는 보험회사인 J.S. Wurzler는 인터넷 운용상 마이크로 소프트사의 해킹위험이 높은 NT 소프트웨어를 사용하는 기업에 대하여 할증보험료를 부과한다.[69] 즉, 생명보험에서 흡연자나 고혈압 환자를 취급하듯이, J.S. Wurzler는 NT 소프트웨어의 사용에 대하여 할증보험료를 부과하는 방식이다.

(4) 도덕적 해이(Moral Hazard)와 관련한 문제

역선택과 관련한 문제가 보험계약의 체결 전에 피보험자의 은밀한 정보와 관련한 문제를 처리하는 반면, 도덕적 해이와 관련한 문제는 보험계약이 체결된 후에 피보험자가 손해발생의 가능성을 경감하는 조치를 취할 수 있는 유인의 결핍 문제를 취급한다. 예를 들면, 화재보험에 가입한 기업은 그렇지 않은 기업보다 화재예방과 관련한 안전조치에 태만한 경향이 있다.

도덕적 해이 문제와 관련하여 전자상거래 보험은 네트워크 및 인터넷의 보안을 개선하기 보다는 악화시키는 방향으로 작용될 가능성이 높다. 보험회사는 피보험기업에 대하여 해킹보험을 제공하기 전에 방화벽과 같은 특정 수준의 보안기준을 요구하는 반면,

---

69) R. Boyce, "Insurer considers Microsoft NT high-risk", Interactive Week, May 28, 2001, pp.11-12.

당해 기업이 그러한 기준을 충족할 수 있는 능력과 기술을 보유하고 있다고 하더라도 기업의 입장에서는 보안기준을 개선해야 할 유인이 거의 존재하지 않는다. 한편 기업은 자체 네트워크가 담보되었기 때문에 네트워크 보안의 개선을 위하여 추가비용을 지출하지 않으려 할 것이다. 더욱이 기업의 입장에서는 손해발생 시에 일차적으로 그러한 손해를 경감하기 위한 조치를 취하기 보다, 보험회사가 보험금을 지급할 때까지 단지 기다리기만 할 가능성이 존재한다.[70]

다른 한편, 보험회사가 요구하는 보안기술 수준에 따른 보안기술의 표준화는 한편으로 위험을 가중시킬 소지를 내포한다. 이는 보험회사가 전자상거래 보험을 구매하는 기업에 대하여 특정 수준의 방화벽, 암호화 시스템 및 보안시스템 등 일련의 표준화된 보안기술을 요구한다는 사실에 기인한다. 이러한 사실에 기인하여 모든 네트워크가 공통된 위험에 직면하게 되고, 그 중 단일 네트워크의 보안에 문제가 발생하면, 기타 일체의 네트워크도 위험에 직면할 가능성이 높아진다.

한편 보험회사가 도덕적 해이 문제에 대응할 수 있는 한 가지 방법은 보험계약 상 공제액 제도를 운용하는 것이다. 공제액 제도의 운용에 의하여 위험(화재나 보안 상 결함)이 현실화되는 경우 피보험자는 일정한 손해를 당하게 된다. 따라서 공제액 제도는 피보험자로 하여금 손해발생의 가능성을 줄이는 조치에 대하여 보험료 할인을 제시하는 것이다. 예를 들면, 가계보험의 경우, 보험계약 상 화재발생의 가능성을 줄이기 위한 연기 또는 열탐지기(화재경보기의 일종)를 설치한 피보험 가정에 대하여 보험료의 할인혜택을 제공하는 것과 동일하다. 이와 마찬가지로 사이버위험 보험을 제공하는 보험회사는 자체적으로 설정한 특정 보안조치를 위한 기업에 대하여 할인보험료를 적용한다. 예를 들면, AIG는 Invicta Network의 보안장치를 사용하는 기업에 대하여 할인보험료를 적용하고 있고,[71] Lloyd's of London은 트립와이어[72]라는 보안 소프트웨어를 사용하는 기업에 대하여 할인보험료를 적용한다.

전자상거래 보험에서 발견되는 또 다른 특징은 제휴(partnership) 시스템이다. 이 시스템 하에서 제품/서비스의 제공자는 구매자에게 특정 보험을 할인된 가격에 구매할 수 있는 선택권을 제시한다. 예를 들면, HP는 J.S. Wurzler와 제휴하여 HP-UX 시스템

---

70) Andrew Tanner-Smith, "Current Problems with Hacking Insurance", http://www.andrew.cmu.edu/user/hchong.

71) R. Boyce, "Insurer considers Microsoft NT high-risk", Interactive Week, May 28, 2001, pp.11-12.

72) Tripwire는 전자상거래보험에서 사용되는 손해통제수단을 지칭한다.

의 사용자에 대하여 발생한 보안 상 결함으로 인하여 발생한 수입의 상실에 대한 보험을 제시한다.[73] 또한 AT&T는 Marsh와 제휴함으로써 AT&T의 인터넷 데이터 센터 및 웹 호스팅 서비스를 사용하는 기업에 대하여 전자상거래 보험을 제시한다.[74]

73) J. Madden, "HP to offer e-business insurance policies", PC Week, Feb. 16, 2000, pp.15-20.

74) Marsh Company, "Marsh, AT&T unveil innovative e-business risk solution", 2001. 8. 15, www.marshweb.com/home/homepg.nsf.

VI. 결언

최근 인터넷의 급속한 확산은 규모에 상관없이 모든 기업에 대하여 저비용의 새롭고 무한한 영업기회 및 성장기회를 제공하고 있다는 점은 분명한 사실이지만, 이와 더불어 기업은 과거 경험하지 못했던 새롭고 강력한 위험에 노출되고 있다는 사실 또한 간과되어서는 안된다. 무역기업이 전자거래환경 하에서 직면하고 있는 새로운 위험을 효율적으로 관리하기 위해서는 기술적인 측면에서 컴퓨터 시스템에 대한 불법접속을 차단하는 방화벽 설치, 강력한 안티-바이러스 프로그램의 설치 및 운용 또는 전문적인 시스템보안 서비스업체를 이용하는 방법 등이 강구되어야 하겠으나, 결론적으로 강조하고 싶은 점은 기술적으로 100퍼센트 안전한 보안시스템은 존재하지 않는다는 사실이다. 인터넷 환경 하에서 완벽한 보안시스템은 외부와의 단절 및 종업원에 대한 시스템 접근금지를 의미한다. 왜냐하면 인터넷 환경 하에서 기업 컴퓨터 시스템의 보안 정도는 시스템의 개방 정도에 반비례하기 때문이다. 결국 가상공간을 은밀히 배회하는 무수한 위험에 대하여 기업의 재산을 보호하기 위해서는 기술적인 장치는 물론이고 제도적인 장치로서 보험을 이용하는 것이 필수적이다.

한편 본 고에서 위험관리수단으로서 제시한 전자상거래 보험은 아직까지 도입초기단계에 있기 때문에 많은 문제점을 안고 있다. 본론에서 제시한 담보조건의 표준화 및 보험료의 산정 문제는 현재 보험회사들이 신종보험에 대하여 정확한 보험료산출기법 및 보험모델이 정립되지 못한 결과이지만, 어쨌든 소비자의 입장에서는 전자상거래 보험에 대한 불신과 비용을 초래하는 요인으로 작용할 것이다. 또한 역선택 및 도덕적 해이와 관련한 문제는 전자상거래 보험에 고유한 것은 아니기 때문에 보험회사는 이러한 문제를 해결하기 위하여 전통적인 방법, 즉 공제액 제도 또는 보험료의 할인·할증제도의 운용을 통하여 문제를 해결해 나가고 있다. 한편 이러한 문제들을 해결하기 위하여 보험회사는 전자상거래 보험에 독특한 제휴시스템을 이용하고 있다. 이 제도를 통하여 보험회사와 제휴를 맺은 보안전문기업은 피보험기업의 보안시스템에 대한 정기적인 점검을 실시함으로써 보안과 관련한 위험을 경감 및 표준화하고 있다. 향후 이러한 제도가 잘 정착되면, 전자상거래 보험이 최근 7조 달러 규모의 시장을 형성하고 있는 전자상거래 또는 전자무역기업에 대하여 유용한 위험관리수단을 제시할 것으로 전망된다.

마지막으로 강조하고 싶은 점은 오늘날 기업의 경영층은 가상공간이 공상영화나 공

상과학소설의 주제였던 1960년대에 인식된 위험을 커버하는 기업재산보험이나 손해보험이 더 이상 전자거래환경 하에서 발생하는 위험의 관리수단을 제공하지 못한다는 점을 인식할 필요가 있다. 즉 기업은 20세기의 위험관리수단이 21세기의 전자거래환경에 대하여 유용한 관리수단을 제공하지 못한다는 점을 인식할 필요가 있다.

[참고문헌]

盧泰嶽, "電子去來에 있어서 契約의 成立을 둘러싼 몇가지 問題", 『法曹』 통권 516호, 1999. 9

盧泰嶽, "電子去來에 있어서 契約의 成立을 둘러싼 몇가지 問題", 『法曹』 통권 517호, 1999. 10

박석재·신건훈, 전자상거래 보험의 문제점과 해결방안, 무역학회지 제26권 제4호, 2001. 9

尹光云 · 張斗彩 · 金喆浩, 『電子商去來論』, 三英社, 1999

이대희, 인터넷과 지적재산권법, 박영사, 2002

이한상·김준학, 지식재산권법, 제일법규, 2001

정영화·남인석, 『전자상거래법』, 다산출판사, 2000

조혜원, 개인정보유출 관련 보험제도 활성화방안, 「주간보험이슈」 제72호, 보험개발원, 2005. 5. 11.

형사정책연구원, 인터넷범죄의 규제법규에 관한 연구, http://www.kic.re.tr/search/data/00-16k.txt, 2001. 7. 30.

Andrew Tanner-Smith, "Current Problems with Hacking Insurance", http://www.andrew.cmu.edu/user/hchong.

B. Perri, "Recent Development in E-Commerce", *Tort Trial & Insurance Practice Law Journal*, Vol.37, No.2, Winter 2002.

Bruce Schneier, "Hacking Insurance", http://www.andrew.cmu.edu/user/hchong.

Computer Security Institute, 2003년 및 2004년 *CSI/FBI Computer Crime and Security Survey*

C.C. Nicoll, "Insurance of e-commerce risks", *International Journal of Insurance Law*, 1999.

Dan Geer, "Solution to Problems", http://www.andrew.cmu.edu/user/hchong.

David R. Cohen and Roberta D. Anderson, "Insurance Coverage for Cyber-Losses", *Tort & Insurance Law Journal*, Vol. 35, No. 4, 2000

D. Radcliff, "Calculating e-risk", *Computer World* 35, Feb. 12, 2001

D.S. Hansell, *Introduction to Insurance(2nd ed.)*, LLP, 1999.

H. Wesley Sunu, Rober Paul Norman, Katherine S. Kamen, Larry P. Schiffer and Adam Insurance Information Institute, Press Release(2003. 8. 13), http://iiidev.iii.org/media/updates/press.731722.

ISO, "ISO introduces Cyber Risk Program to help cover $7 Trillion E-Commerce Market", http://www.iso.com/press_release/2005.

John E. Black Jr., Lorelie S. Masters & David S. Weitzel, "Dangers Lurk in Cyberspace", Business Law, Vol.11, No.6, July/August 2002, http://www.abanet.org/buslaw

J. Madden, "HP to offer e-business insurance policies", *PC Week*, Feb. 16, 2000

Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail, "A Fraimwork for Using Insurance for Cyber-Risk Management", *Communications of the ACM*, Vol.46, No.3, 2003. 3.

Marsh Company, "Marsh, AT&T unveil innovative e-business risk solution", 2001. 8. 15, www.marshweb.com/home/homepg.nsf.

Michael A. Rossi, "New Stand-Alone E-Commerce Liability Insurance for Third-Party Liability Claims", Part 2, Insurance Law Group, 2000. 12, http://irmi.com/Expert/Articles/2000/Rossi12a.aspx.

Michael A. Rossi, "Cyber Liability Insurance Issues for Large Companies : Market Status Update for Summer of 2003 and Tips for the Buyer", (2003. 11), http://www.irmi.com/Expert/Articles/2003.

Michael A. Rossi, "New Stand-Alone E-Commerce Insurance Policies for First-Party Risks", Insurance Law Group, 2001. 2, http://irmi.com/Expert/Articles/2001/Rossi02.aspx.

Michael A. Rossi, "Stand Alone E-Commerce Market Survey", Insurance Law Group, 2001. 7, http://irmi.com/Expert/Articles/2001/Rossi02-1.aspx.

Nicholas Legal-Jones(ed.), *MacGillivray on Insurance Law*, 9th ed., Sweet & Maxwell, 1997.

Near North National Group, "Understanding Cyber Liability", *Near North's Insight Online*, 2003. Winter, available at http://www.nnng.com/newsletter/winter2003.

Robert L. Miller & Gaylord A. Jentz, *Law for E-Commerce,* West, 2002

Robert W. Hammesfahr, *@Risk, Internet and E-commerce : Insurance and Reinsurance Legal Issues*, Reactions Publishing Ltd., 2000

R. Boyce, "Insurer considers Microsoft NT high-risk", *Interactive Week*, May 28, 2001

Stephen York and Ken Chia, *E-Commerce-A guide to the law of electronic business*, Butterworths, 1999.

Susan Breidenbach, "The Policy of Protection", http://nwfusion.com/research/2000, 2000. 10. 23

Tim Sukel, "The Workplace, Cyberspace and Cyber-Liability", 2000. 9, http://progressivebanks.com/Agents/Safetalk_Sept2000.

Why Business Interruption Insurance, http://www.axa-insurance.co.uk/guides, 2001. 2. 12.