▣ 논 단

개인정보 보호조치의무 위반과 해킹 사이의 인과관계

전 승 재
법무법인(유한) 바른 변호사 / 공학박사

요 약 문

인과관계에 관한 법이론을 정보보호(cyber security) 분야, 특히 해킹을 막지 못한 관리자의 책임을 추궁하는 사례에 적용하는 것이 본고의 목적이다. 우리 법상 개인정보 보호조치의무를 위반(이하 '미조치')한 행위 자체는 과태료 부과 대상이고, 여기에 더해 실제 개인정보 유출(해킹)이라는 결과까지 발생하면 과징금 및 손해배상이라는 실체법상 책임까지 부담해야 하는 구조이다. 여기서 '미조치'라는 원인과 '해킹'이라는 결과 사이에 인과관계가 단절된다면, 즉 당해 미조치로 인해 생긴 취약점이 아니라 다른 제3의 취약점을 해커가 뚫고 들어왔다면, 그러한 결과에 대해서까지 관리자가 책임을 부담해야 하는지 여부가 쟁점이 된다. 본고는 싸이월드 해킹, 인터파크 해킹, 빗썸 해킹, 이상 3개 사례를 통해 이 쟁점에 관하여 검토한다.

싸이월드와 인터파크는 모두 APT(Advanced Persistent Threat) 공격을 당해 사내 PC의 원격제어권한이 탈취된 것으로 시작하여, 이 PC와 DB 서버 사이에 자동 로그아웃이 되지 않고 접속이 유지된 터미널이 남아있었던 것을 기화로 해커가 DB 서버에 침입할 수 있었다. 자동 로그아웃을 설정했을 때 해킹이라는 결과를 회피할 수 있었다고 평가되면 인과관계가 인정될 수 있는 사안이었는데, 싸이월드 사건에서는 이 부분 사실관계가 민사소송에서 심리된 끝에 인과관계가 부정된 반면, 인터파크 사건에서는 인과관계가 공법적·사법적 책임 성립 요건이 아니라는 취지의 행정법원·민사법원 각 하급심의 해석이 내려지면서 이 문제를 회피했다. 그러나 인터파크 판결의 해석은 법치주의의 대원칙인 자기책임의 원리에 위반될 소지가 있으므로 재고되어야 한다. 참고로 2021. 1. 6. 주무부처가 입법예고한 개인정보 보호법 개정안은 과징금 부과 시 인과관계를 고려하도록 명문화하고 있다.

빗썸 해킹 사건의 경우 방통위의 과징금 처분이 내려짐으로써 빗썸의 과실이 드러난 사고와, 해킹 원인이 밝혀지지 않은 다른 사고들이 혼재되어 있었다. 이러한 사안에서 인과관계 요건은, 관리자의 귀책이 입증된 취약점과 그렇지 않은 취약점이 각각 어느 사고에 대응되는지 본건과 별건을 분류해줌으로써 책임부담의 범위를 설정해주는 역할을 한다. 만약 인과관계를 요구하지 않을 경우 엉뚱하게 별건에 대해서까지 책임을 부담시킬

여지가 있고, 관리자로 하여금 피해 내역을 은폐할 유인을 키울 우려가 있다.

따라서 제도적으로는 인과관계 요건을 삭제하는 것보다, 인과관계를 요구하되 그 입증이 원활해지도록 하는 기반을 조성하거나, 인과관계 입증책임을 전환하는 정도로 대응하는 것이 더 바람직하다.

주제어 : 정보보호, 과실, 주의의무, 인과관계, 손해배상, 불법행위, 개인정보 보호법

〈目 次〉

Ⅰ. 문제의 제기

2014년 초 발표된 신용카드 3사 개인정보 유출 사고를 계기로, 정보보호를 소홀히 한 개인정보처리자에게 엄중한 법적 책임을 추궁해야 한다는 목소리가 급격하게 사회적 지지를 얻었다. 이 시기에 여론의 급물살을 타고 입법된 것으로, 개인정보 유출에 관한 300만 원 이하 법정손해배상제,[1] 3배 범위 내 징벌적 손해배상제,[2] 정보통신서비스 제공자에 대한 과징금 상한액 상향[3] 등이 있었다.

---

1) 정보통신망 이용 촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법')(2014. 5. 28. 법률 제12681호로 개정되고 2020. 2. 4. 법률 제16955호로 개정되기 전의 것) 제32조의2, 개인정보 보호법(2015. 7. 24. 법률 제13423호로 개정된 것) 제39조의2.

2) 개인정보 보호법(2015. 7. 24. 법률 제13423호로 개정된 것) 제39조 제3항, 정보통신망법(2016. 3. 22. 법률 제14080호로 개정되고 2020. 2. 4. 법률 제16955호로 개정되기 전의 것) 제32조 제2항.

3) 개인정보 관련 과징금 조항은 2008. 6. 13. 법률 제9119호로 개정된 정보통신망법에서 처음 도입되었는데, 당초에는 개인정보 유출 시에는 1억 원 이하의, 그 외 과징금 부과 대상 개인정보 오남용 행위에 대하여는 관련매출액의

2014년 당시 사회적 주목을 그리 받지 못하였던 개정사항도 있었는데, 개인정보 유출에 관한 과징금 부과 근거규정이 종전 "법률상 조치를 하지 아니하여 이용자 개인정보가 유출된 경우"에서 "유출된 경우로서 법률상 조치를 하지 아니한 경우"로 문언이 변경된 부분이다.[4] 그 개정 의도에 관하여, 방송통신위원회의 입법예고 자료에서 "유출사고 발생 시 법률상 조치 위반과의 '인과관계' 입증이 어려우므로 이를 과징금 부과요건에서 삭제하고자 한다"는 취지의 기재가 있었을 뿐, 국회 의안원문, 검토보고서나 회의록 등에서는 이에 관한 내용을 찾기 어려운 것으로 보아 국회에서는 인과관계 요건 삭제에 관한 찬반논의가 사실상 이루어지지 않은 듯하다.

위 개정된 과징금 부과규정은 2016년 터진 인터파크 해킹 사건에서 최초로 적용되었다. 서울행정법원과 서울고등법원은 개정법이 과징금 부과 구성요건 중 인과관계 요건을 삭제하는 취지가 맞다고 해석했고, 대법원은 심리불속행 기각 판결을 내림으로써 원심을 확정했다.[5]

그러다가 인터파크를 상대로 개인정보 해킹 피해자들이 제기한 민사소송에서도 최근 1심 판결이 선고되었다.[6] 2014년 개정 정보통신망법에 신설된 법정손해배상 규정이 최초로 적용된 사건이었는데, 1심 법원은 이 규정 또한 법정손해배상 요건으로서 인과관계를 요구하지 않는 취지라고 해석했다. 인터파크의 보안 취약점(조치의무 위반)과 해킹 사이의 인과관계가 복잡하게 다투어지던 사건에서 마치 고르디우스의 매듭을 단칼에 끊듯 '인과관계 불문 손해배상하라'는 판결이 선고된 것이다.

인터파크 민사사건에 적용된 정보통신망법상 법정손해배상 규정의 문언은 위 과징금 부과 근거규정과 동일한 구조로 '조치의무 위반'과 '유출'이 병렬적으로 나열되어 있었고,[7] 이에

1% 이하의 각 범위 내에서 과징금이 부과될 수 있었다. 그러다가 2014. 5. 28. 법률 제12681호로 개정된 정보통신망법에서는 개인정보 유출을 비롯하여 모든 과징금 부과 대상 행위유형에 대해 그 상한액이 관련매출액의 3%로 상향되었다.

4) 구 정보통신망법(2014. 5. 28. 법률 제12681호로 개정되고 2020. 2. 4. 법률 제16955호로 개정되기 전의 것) 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
6. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제28조(개인정보의 보호조치) 제1항 제2호부터 제5호까지의 조치를 하지 아니한 경우

5) 서울행정법원 2018. 7. 5. 선고 2017구합53156 판결, 서울고등법원 2019. 11. 1. 선고 2018누56291 판결(심리불속행 확정). 이에 대한 비판 견해로는, 전승재, "해킹과 인과관계 없는 취약점도 과징금 부과 대상인가", 법률신문, 2019. 12. 23.(https://m.lawtimes.co.kr/Content/Article?serial=158301), 전승재, "인터파크 해킹, 대법원 심리불속행 판결에 유감", 보안뉴스, 2020. 3. 23.(https://www.boannews.com/media/view.asp?idx=87127) 참조.

6) 서울중앙지방법원 2020. 10. 29. 선고 2016가합563586 판결(항소심 계류 중).

7) 구 정보통신망법(2020. 2. 4. 법률 제16955호로 개정되기 전의 것) 제32조의2(법정손해배상의 청구) ① 이용자는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

착안하여 위 1심 법원은 인과관계 요건이 삭제된 것이라고 본 것이다. 그런데 이 규정은 2020. 2. 4. 정보통신망법과 개인정보 보호법이 합쳐지면서 개인정보 보호법에 이관되지 않았다. 현행 개인정보 보호법 제39조의2는 고의·과실[8]로 '인하여' 개인정보가 유출된 경우를 법정손해배상 대상으로 규정함으로써 인과관계를 명문으로 요구하고 있다.[9]

현행 개인정보 보호법을 보면 인과관계를 요구하지 않는 법정손해배상 규정은 현재 폐지된 것처럼 보인다. 이것은 자기책임 원칙에 반한다는 반성적 고려로 인해 폐지된 것일까. 만약 그렇다고 하면 인터파크 민사사건에서 그 폐지된 규정이 적용되는 것이 적절한 것인가. 이번 1심 판결처럼 인과관계 불문 손해배상을 시키는 것이 과연 정보보호라는 첨단기술 영역에서 소비자를 두텁게 보호하기 위한 적절한 수단이 될 수 있을까. 한편, 2021. 1. 6. 주무부처가 입법예고한 개인정보 보호법 개정안은 과징금 부과 시 인과관계를 고려하도록 명문화하고 있는데,[10] 그러면 인터파크 행정판결은 이제 입법에 의해 폐기되는 것인가. 이것이 본고에서 답하고자 하는 문제이다.

이하에서는 개인정보 보호조치의무 위반(이는 '과실'에도 해당한다)이라는 원인과 해킹이라는 결과 사이의 인과관계 여부가 문제되었던 역대 사례에 대해 살펴보면서, 이로 인한 법적 책임 유무를 판단하는데 있어 인과관계가 어떤 역할을 하는지 고찰하고, 우리 법제도가 나아가야 할 바람직한 방향을 제시하고자 한다.

Ⅱ. 인과관계가 문제된 해킹 사례

1. 싸이월드 해킹 사건

싸이월드(cyworld.com)를 운영하는 SK커뮤니케이션즈(이하 'SK컴즈')는 2011년 약 3,500만

---

1. 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우
2. 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우

8) 여기서 과실(negligence)은 법률상 개인정보 보호조치의무 위반(negligence per se)을 포함하는 개념이다. 자세한 내용은, 전승재, 「해커 출신 변호사가 해부하는 해킹 판결」, 삼일인포마인, 2020, 29-38면 참조.

9) 개인정보 보호법 제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

10) 개인정보 보호위원회, "개인정보 보호법 일부개정법률(안) 입법예고", 2021. 1. 6.(https://www.moleg.go.kr/lawinfo/makingInfo.mo?lawSeq=62160&lawCd=0&&lawType=TYPE5&mid=a10104010000)
제64조의2(과징금의 부과) ③ 보호위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.
5. 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 정도 및 안전성 확보 조치 등 의무 위반행위와의 인과관계

건의 회원정보가 유출되는 해킹을 당했다. 첫 번째 취약점은, SK컴즈 DB 관리 직원의 업무용 PC가 해커가 심은 악성코드에 감염되었던 부분이다. 이 직원은 이스트소프트에서 무료로 배포하는 '개인용 알집'을 사내 PC에 설치해서 쓰고 있었다. 개인용 알집을 실행하면 배너 광고를 표시하기 위해 이스트소프트가 운영하는 업데이트 서버로부터 배너 광고 이미지 등을 받아오는데, 해커는 그 업데이트 서버에 침입하여 SK컴즈의 IP주소 대역에서 광고 모듈 업데이트를 요청하면 해커가 심은 키로거[11]를 응답하도록 서버 프로그램을 조작하였다. 개인용 알집을 쓰는 SK컴즈 DB 관리 직원의 PC가 해커의 키로거에 감염되자 DB 서버의 ID, 패스워드 등이 해커에게 도청되었다. 참고로 과거 단일한 악성코드나 동종의 침입방식으로 불특정 다수를 노렸던 사이버 공격과 다르게, 싸이월드 사건처럼 해커가 특정한 목표물을 설정해서 지능적 공격을 지속하는 유형을 APT(Advanced Persistent Threat) 공격이라고 한다.

두 번째 취약점은, 위 직원이 퇴근한 후에도 로그아웃이 되지 않고 DB 서버와의 접속이 유지된 터미널이 위 직원의 PC에 방치되어 있었던 부분이다. 해커는 이 터미널을 이용해 DB 서버에 손쉽게 접속할 수 있었고, 여기에서 싸이월드 이용자 개인정보를 대량으로 반출했다.

일단 첫 번째 취약점과 해킹 사이의 인과관계는 부정되었다. SK컴즈 직원이 기업용 알집을 구매하지 않고 가정 등 개인용 PC에서만 무료 사용이 허용된 개인용 알집을 사내 업무용 PC에 설치한 행위는 소프트웨어 라이선스(End-User License Agreement, EULA)를 위반한 것이다. 그런데 이 행위의 저작권 침해 여부는 별론으로 하고, SK컴즈로서는 개인용 알집을 사내에서 사용할 경우 알집 업데이트 서버가 변조되어 알집 업데이트 과정에서 악성 프로그램을 다운로드 받게 됨으로써 해킹 수단으로 악용될 것까지 구체적으로 예견하기 곤란했으며, 설령 기업용 알집을 구매하여 사용했다 하더라도 그 업데이트 서버에 악성코드를 심는 동일한 방식의 해킹을 방어할 수 있었다고 단정하기 어려웠을 것이라고 심리되었다.[12]

두 번째 취약점인 자동 로그아웃(idle timeout) 미설정[13]과 해킹 사이의 인관관계 여부는 치열하게 다투어졌다. SK컴즈의 손해배상책임을 인정한 일부 1심 판결은 인과관계가 있다고 판단했다. SK컴즈가 DB 서버 접속 시 아이디와 비밀번호 이외에도 관리자 이메일로 일회용 비밀번호(OTP)를 전송하여 인증하는 방식을 취하고 있었고 해커가 사내 PC에 키로거를 DB 관리 직원의 PC에 심었다 하더라도 위 OTP를 알아낼 수 없었으리라는 전제 하에, 만약 SK컴즈가

---

11) 키로거(Keylogger)는 PC의 키보드로 입력되는 내용을 별도 파일 등에 저장하는 프로그램이다. 그 별도로 저장된 키보드 입력내용을 PC의 주인 몰래 해커에게 전송할 경우 이는 도청장치처럼 기능한다.

12) 대법원 2018. 6. 28. 선고 2014다20905 판결.

13) 두 번째 취약점의 경우, 싸이월드 해킹 당시에는 자동 로그아웃 설정을 요구하는 행정규칙(「개인정보의 기술적·관리적 보호조치 기준」 고시 조항)이 없었다는 이유로 과실조차 아니라고 판단한 하급심 판결이 주류였다(서울고등법원 2015. 3. 20. 선고 2013나20047 판결 등). 한편, 대법원은 그 행정규칙은 최소한의 기준일 뿐 사회통념상 합리적으로 기대 가능한 보호조치를 하지 아니한 경우에는 과실에 해당할 수 있는 가능성을 열어두었다(대법원 2018. 1. 25. 선고 2015다24904 판결). 자세한 내용은, 전승재·권헌영, "개인정보의 기술적·관리적 보호조치에 대한 공적집행과 사적집행", 경제규제와 법 11권 2호, 2018, 276-278면 참조.

자동 로그아웃을 설정의무(적법한 대체행위)를 이행했더라면 해킹을 막을 수 있었으리라고 그 1심 재판부는 판단한 것이다.[14] 한편, 항소심 및 상고심 판결은 SK컴즈의 손해배상책임을 부정하면서 상당인과관계가 없다는 근거를 들었다. 해커가 DB 서버 관리자의 아이디와 비밀번호를 이미 도청한 상태였기 때문에 터미널의 로그아웃 여부와 무관하게 언제든지 그 아이디와 비밀번호를 가지고 DB 서버에 로그인 할 수 있었다고 보인다는 이유였다.[15] 그런데 여기에는 위 OTP에 관한 언급이 전혀 없어서, 1심 판결이 인정한 사실관계가 항소심에서 제출된 증거에 의해 반증되어서 빠졌는지 어떤지를 알 수가 없다. 자동 로그아웃 미설정과 싸이월드 해킹 간 인과관계 존부는 사실인정의 문제라고 할 수 있다.

2. 인터파크 해킹 사건

인터파크는 2016년 2,500만 건의 회원정보가 유출되는 해킹을 당했다. 해킹 방식은 싸이월드와 유사하게 APT 공격이었다. 해커는 인터파크 전산실 직원 A를 대상으로 삼아 사회공학적 공격(Social Engineering Attack)을 감행했다. 해커는 불상의 방법으로 A의 개인용 네이버 이메일 계정 아이디와 패스워드를 탈취한 후 A의 메일함을 분석하여 A가 친동생과 이메일을 주고받은 것을 보고 A의 동생이 쓰는 말투와 이모티콘 등을 습득했다. 해커는 A에게 스피어 피싱(Spear Phishing) 이메일을 보내면서 마치 A의 동생이 보내는 것처럼 발신 이메일 주소를 변조하고 동생의 어투까지 흉내 냈다. 그 이메일에는 악성코드가 첨부되어 있었는데, 이것은 평소 A가 SNS에 올려 둔 가족사진을 수집하여 만든 화면보호기(SCR 파일)로 위장되어 있었다. 참고로 SCR 파일도 EXE 실행파일과 마찬가지로 악성코드 유포용으로 사용될 수 있다. 감쪽같이 속은 A는 별 의심을 하지 않고 해커가 보낸 첨부파일을 열어보았고, 이리하여 A의 PC가 악성코드에 감염됨으로써 그 제어권한이 해커의 수중에 떨어졌다. 이것이 침입의 시발점이자 해킹의 가장 결정적 원인을 제공한 부분이지만, 이 정도의 지능적 공격은 사회통념상 합리적인 주의의무를 다하더라도 극히 방어하기 어렵기 때문에 이 부분을 가리켜 인터파크의 과실을 물을 수는 없었다.

인터파크의 과실로 지적된 첫 번째 취약점은, 싸이월드와 마찬가지로 자동 로그아웃을 미설정한 행위였다. 이것은 「개인정보의 기술적·관리적 보호조치 기준」(이하 '방통위 고시') 제4조 제10항 위반이자[16] 과징금 부과 처분의 구성요건에 해당한다.[17] 인터파크 전산실 직원 A의

14) 서울서부지방법원 2013. 2. 15. 선고 2011가합11733 판결.
15) 서울고등법원 2015. 3. 20. 선고 2013나20047 판결, 대법원 2018. 1. 25. 선고 2015다24904 판결.
16) 방통위 고시(2015. 5. 19. 방송통신위원회고시 제2015-3호로 개정된 것)
제4조(접근통제) ⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.
참고로 이 조항은 앞서 본 싸이월드 해킹 사건 후 그 재발방지대책으로 신설된 것이다.

PC를 수중에 넣은 해커는 이를 경유하여 사내 네트워크를 통해 DB 관리자(개인정보취급자) 직원 B의 PC에 원격 데스크탑 접속했다. 참고로 해커가 B의 PC의 원격 데스크탑 접속 비밀번호를 어떻게 탈취했는지는 밝혀지지 않았다. 공교롭게도 해커의 접속 당시 B의 PC에는 망분리 프로그램(MirageWorks vDesk) 및 서버 접속 터미널(STG Client)이 그대로 띄워져 DB 서버와의 접속이 유지되어 있었다. 자동 로그아웃 설정이 제대로 안 되어 있었기 때문이다. 이로써 해커는 망분리 프로그램 및 서버 접속 터미널의 아이디 및 패스워드를 추가로 탈취하는 수고를 덜 수 있었고, DB 서버에서 인터파크 회원들의 개인정보 2,500만 건을 유출했다.

두 번째로 지적된 취약점은 사실 해커의 DB 서버 침입 및 개인정보 유출 경로와 직접적인 연관은 없었다. 인터파크 직원들은 사내 수많은 서버들의 접속계정 패스워드를 일일이 외우기 어려워서 이를 엑셀파일에 평문으로 메모한 패스워드 장부를 업무용 파일서버에 올려두고 있었다. 그런데 해커가 A의 PC에서 내부 네트워크를 스캔했더니 그 파일서버가 발견되었고, 위 패스워드 장부가 해커에게 노출된 것이다. 개인정보취급자의 패스워드를 평문으로 방치하는 행위는 방통위 고시 제6조 제1항에 위반된다.[18] 한편, 개인정보가 유출된 DB 서버의 접속 패스워드는 이 장부에 기재되어 있지 않았기 때문에, 이 취약점은 고객정보 해킹의 직접적인 원인을 제공한 것은 아니었다.

방통위는 위 두 취약점을 묶어서 2016. 12. 6. 인터파크에게 44억 8,000만 원의 과징금을 부과했다. 이에 대해 인터파크는 과징금 처분의 취소를 구하는 행정소송을 제기하면서, 특히 위 두 취약점과 개인정보 유출 사이의 인과관계가 없다는 취지로 다투었다.

행정소송의 1심 및 항소심[19]은 인터파크의 청구를 기각하면서, 첫 번째 취약점과 개인정보 유출 사이에 인과관계가 인정된다고 보았다. 인터파크가 자동 로그아웃 설정을 하지 않았기 때문에 해커는 서버 접속 터미널 등의 접속이 종료되지 않은 개인정보취급자 B의 PC를 통하여 비밀번호 입력 없이도 DB 서버에 접속할 수 있었다는 이유였다. 법원은 두 번째 취약점인 패스워드 장부 노출과의 인과관계에 대해서는 판결이유를 적지 않았다. 그 대신에 인터파크 사건에 적용된 개정 법률이 '이용자의 개인정보를 유출한 경우로서 개인정보 보호조치를 하지 아니한 경우'라고 개정됨으로 인해, '유출'과 '미조치' 두 요건이 갖추어지기만 하면 과징금 부과 구성요건이 구비되고 이와 별도로 위 두 요건 간 인과관계는 요구되지 않게 되었다고 해석하면서, 인과관계 여부를 불문하고 과징금 처분이 적법하다고 판결했다. 이 행정판결은 대법원에서 인터파크의 상고가 심리불속행으로 기각되면서 확정되었다.

그 후 개인정보를 유출 당한 이용자들이 인터파크를 상대로 제기한 민사소송에서도 1심

17) 과징금 부과 근거법률의 내용은 각주 4) 참조.

18) 방통위 고시 제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

19) 서울행정법원 2018. 7. 5. 선고 2017구합53156 판결. 서울고등법원 2019. 11. 1. 선고 2018누56291 판결(심리불속행 확정).

판결이 선고되었다.[20] 원고들은 해킹 당시 시행 중이었던 정보통신망법상 법정손해배상 규정[21]을 청구원인으로 개진했는데, 이 규정은 법정손해배상책임의 발생 요건으로 '정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우'와 '개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우'를 병렬적으로 나열하고 있었다. 이는 앞서 본 과징금 부과 근거조항과 동일한 구조였다. 이에 착안하여 민사 1심 법원은 인터파크의 개인정보 보호조치의무 위반이 존재하고 개인정보가 유출되었다는 사정이 발생하기만 하면 양자의 인과관계가 있는지 여부와 상관없이 위 법정손해배상 규정에 의한 책임이 인정된다고 판단했다.

이러한 인터파크 판결로 인해, 마치 개인정보처리자의 보호조치의무 위반이라는 원인과 해킹을 막지 못했다는 결과 사이에 인과관계가 없더라도 법적 책임을 추궁할 수 있는 것처럼 해석될 여지가 생겼다. 그런데 2020. 2. 4. 개정된 현행 개인정보 보호법상 손해배상 규정,[22] 법정손해배상 규정[23] 및 징벌적 손해배상 규정[24]은 모두 보호조치의무 위반과 개인정보 유출 사이의 인과관계를 명문으로 요구하고 있다. 그렇다면 인터파크 민사판결의 법해석은 구 정보통신망법 시절에만 나올 수 있었던 일시적인 것에 불과하고 현행법 하에서는 더 이상 통용될 수 없는 것인가. 또한 현행 개인정보 보호법상 과징금 근거규정은 여전히 인터파크 행정판결 시절과 마찬가지 구조로 '보호조치의무 위반'과 '유출'이 병렬적으로 나열되어 있는데, 정부는 인과관계를 입증할 필요 없이 과징금을 부과할 수 있고[25] 피해자는 인과관계를 입증해야만 손해배상을 받을 수 있다는 뜻인가. 이 부조화를 해결하고자 하는 것이 본고의 핵심 문제의식이다.

3. 빗썸 해킹 사건

빗썸코리아(당시 상호: 비티씨코리아닷컴, 이하 '빗썸')는 거래규모를 기준으로 전 세계에서도 순위권에 들 정도로 대표적인 암호화폐 거래소 중 하나이다. 그러한 빗썸은 2016년경부터 암호화폐가 유출되는 크고 작은 해킹을 수차례 당했는데, 그 가운데에는 빗썸의 과실이 입증된 사고도 있었고 그렇지 않은 사고도 혼재되어 있었다.

---

20) 서울중앙지방법원 2020. 10. 29. 선고 2016가합563586 판결(항소심 계류 중).

21) 구 정보통신망법상 법정손해배상 규정의 내용은 각주 7) 참조.

22) 개인정보 보호법 제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

23) 현행 개인정보 보호법상 법정손해배상 규정의 내용은 각주 9) 참조.

24) 개인정보 보호법 제39조(손해배상책임) ③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.

25) 주무부처 또한 이 문제를 인식하였는지, 2021. 1. 6. 입법예고한 개인정보 보호법 개정안에서 인과관계를 과징금 부과 고려요소로서 규정하는 안을 제안하고 있다. 각주 10) 참조.

대표적인 것은 바로 2017. 4. 1.부터 6. 29.까지 약 3개월간 ID·PW 대입공격(credential stuffing)을 당해 5,000여 개의 이용자 계정이 탈취되고 그 중 266개 계정에서 합계 70억여 원의 암호화폐가 도난당했던 사건이다. 빗썸은 해커의 대규모 로그인 시도 및 이에 따른 로그인 실패 비율 폭증이라는 이상행위를 탐지하지 못함으로써 방통위 고시 제4조 제5항[26] 등[27]을 위반했다고 판단되어 2017. 12. 12. 방통위로부터 과징금 처분을 부과 받았고(행정소송은 따로 제기하지 않았다), 여기에 대한 책임자(빗썸의 창업자이자 최대주주) 및 법인이 고발되어 형사재판 1심에서 벌금형도 선고 받았다.[28] 이러한 행정처분 및 형사판결의 존재 자체로써 빗썸의 보안상 과실은 비교적 명확하게 입증이 되어 있는바, 이 사고를 가리켜 이하에서 '제재 대상 사건'이라 칭한다.

한편, 제재 대상 사건이 아닌 나머지 해킹 사고들에 대하여는 과징금 등 행정처분이 부과 되지 않았다. 추측컨대 위 나머지 해킹 사고들의 경우 대규모 개인정보 유출을 수반하지 않은 특정 이용자 계정에 대한 공격이었다는 이유로 공권력이 개입하지 않은 듯하다. 이에 위 나머지 해킹 사고들에 관하여는 암호화폐를 도난당한 이용자들이 빗썸을 상대로 제기한 민사소송들만 진행되었다. 그런데 손해배상청구가 인용되었다는 소식은 아직까지 언론 등을 통해 들려오지 않는다.[29]

제재 대상 사건이 아닌 나머지 해킹 사고에 관하여 빗썸의 책임을 부정한 민사 판결 두 건이 발견될 뿐인데, [30] 그 두 건의 판결은 위 ID·PW 대입공격 기간 중(2017. 4~6월)이 아닌 다른 시점에 해킹을 당한 사안에 관한 것이다. 첫 번째는 2016. 2.경 해커가 불상의 방법으로 피해자의 빗썸 계정을 탈취하여 시가 약 5,000만 원의 비트코인을 인출한 사건이다.[31] 두 번째는

---

26) 방통위 고시 제4조(접근통제) ⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

27) 아울러 빗썸은 피용자의 업무용 PC 내 엑셀파일에 회원정보를 평문으로 보관하다가 2017. 4. 스피어피싱(spear phishing) 공격을 당해 위 회원정보를 탈취당하기도 했는데, 이는 암호화폐 유출은 수반하지 않았고 오로지 개인정보만 유출된 사고였다. 이 또한 빗썸의 개인정보 보호조치의무 위반행위로 조사되었다.
방통위 고시 제6조(개인정보의 암호화) ④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

28) 서울동부지방법원 2020. 2. 12. 선고 2019고단1838 판결(항소심 계속 중). 제재 대상 사건에 대한 자세한 내용은, 전승재, 앞의 책, 133-139면 참조.

29) 코인원(빗썸이 아닌 다른 암호화폐 거래소)의 일일 암호화폐 출금한도가 2,000만 원으로 설정되어 있었음에도 해커가 탈취한 이용자 계정에서 그 출금한도를 초과하여 인출을 한 사안에서, 그 초과분에 관하여 손해배상을 명한 사례가 발견될 뿐이다(서울남부지방법원 2019. 9. 25. 선고 2019가단201222 판결). 해킹 피해자가 암호화폐 거래소를 상대로 승소한 사례가 언론에 보도된 것으로는 이 사건이 유일하다. KBS, "가상화폐 거래소 해킹 손해배상 책임 첫 인정" 2019. 9. 27.(https://mn.kbs.co.kr/news/view.do?ncd=4291829).

30) 법률신문, "해킹으로 가상화폐 도난… 법원 거래소, 배상책임 없어", 2018. 12. 20.(https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=149446). 법률신문, "해커에 가상화폐 4억 도난…법원 거래소 책임 없어", 2018. 12. 24.(https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=149571).

2017. 11.경 해커가 불상의 방법으로 피해자의 빗썸 계정을 탈취하여 여기에 보관된 4억 원 이상의 예수금을 가지고 이더리움을 매수하여 외부로 유출한 사건이다.[32] 두 사건의 각 원고 모두 제재 대상 사건의 존재를 원용하며 빗썸이 보안을 소홀히 하여 보호조치의무를 위반한바 있었다고 주장했다. 그러나 법원은 그러한 빗썸의 과실과 당해 사건 유출 사이에 인과관계가 없다고 보아 각 원고의 청구를 기각했다. 제재 대상 사건을 통해 빗썸의 과실이 입증되어 있기는 하지만 이것은 2017. 4~6월 ID·PW 대입공격 기간 중 유출의 원인일 뿐이고, 위 두 사건의 각 피해자의 경우 다른 시기에 해킹을 당했고 그 해커의 침입 경로가 밝혀지지 않았으니 당연히 빗썸의 과실도 입증 불가하였으며, 위 두 해킹은 제재 대상 사건에서 드러난 빗썸의 과실과는 다른 원인에 의한 것으로 보이는 이상 이에 관한 책임을 빗썸에게 지울 수 없다는 의미이다.

이상과 같은 일련의 빗썸 해킹 사건들을 놓고 보면, 여러 건의 취약점(관리자의 과실에 의한 취약점도 있을 수 있고 불가항력적인 취약점도 있을 수 있다)에 의하여 여러 건의 해킹 사고가 각각 발생하였을 때, '인과관계'란 어느 취약점이 어느 사고에 대응되는지를 연관시켜 줌으로써 해당 취약점을 막지 못한 관리자의 행위에 귀책이 있다면 이로 인하여 어느 결과에 대해서까지 책임을 부담해야 하는지 그 범위를 설정해주는 역할, 즉 본건과 별건을 분류해주는 역할을 한다고 할 수 있다.

Ⅲ. 해킹 사고에서 인과관계의 의의

1. 과실과 법익침해 간 인과관계 판단기준 일반론

인간의 행위와 결과는 조건적 연쇄에 엮여 있는데, 그 안에서 법적 책임 귀속의 한계를 설정하는 것이 바로 '인과관계'이다.[33] 이는 헌법상 행복추구권, 자기결정권 내지 일반적 행동자유권에서 파생되는 자기책임의 원리에 맞닿아 있다. 사람은 자기의 운명에 대한 결정·선택을 존중받는데 이는 그에 대한 책임을 스스로 부담하는 것을 전제로 한다. 자기책임의 원리는 책임부담의 근거로 기능하는 동시에, 자기가 결정하지 않은 것이나 결정할 수 없는 것에 대하여는 책임을 지지 않고 책임부담의 범위도 스스로 결정한 결과 내지 그와 상관관계가 있는 부분에 국한됨을 의미하는 책임의 한정원리로도 기능한다.[34]

---

31) 서울중앙지방법원 2018. 12. 18. 선고 2017가단5016023 판결(확정).

32) 서울중앙지방법원 2018. 12. 20. 선고 2017가합585293 판결, 서울고등법원 2020. 9. 10. 선고 2019나2004142 판결(확정).

33) 김대휘, "인과관계론", 법률신문, 2014. 11. 20.(https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=88902).

34) 자기책임의 원리는 연좌제 금지를 선언한 헌법 제13조 제3항에서도 표현되어 있다. 이와 관련하여, 담배소비세가

형법에서 인과관계란, 형벌법규가 일정한 행위와 함께 그것과 구별될 수 있는 특정한 외부의 결과발생을 요구하고 있는 경우, 즉 결과범의 경우에 나타난 결과를 행위자의 소행으로 돌리기 위한 전제로서 양자의 관련성을 일컫는다.[35] 인과관계가 부정되면, 결과를 요하는 고의범의 경우 그 결과가 발생하지 않은 것으로 보아 기수책임을 지지 않고, 과실범의 경우 미수를 벌하지 않으므로 불벌이 되며, 결과적 가중범의 경우 기본범죄만 성립하게 되므로, 형사법 분야에서는 인과관계론에 관한 논의가 활발하여 왔다.

가장 기본적인 이론은 조건설이다. 일정한 선행사실(가해행위)이 없었다면 결과(범죄 구성요건)도 발생하지 않았을 것이라는 조건관계가 있으면 인과관계를 인정한다는 내용으로, 라틴어로 CSQN(Conditio Sine Qua Non), 영미권에서는 But-for Test라고 한다. 조건설의 문제점은, 자칫 인과관계가 무한히 확장되어 버릴 수 있다는 것이다.[36] 그러한 인과관계의 연쇄선상에서 행위자가 인식하였거나(고의) 인식할 수 있었던 것(과실)을 표준으로 하여 가벌의 한계선을 긋고자 "어떤 행위라도 죄의 요소되는 위험발생에 연결되지 아니한 때에는 그 결과로 인하여 벌하지 아니한다."는 형법 제17조가 제정되었다.[37] 구체적 판단기준으로는, 일상적인 생활경험을 기준으로 인과관련이 상당한 것으로 평가될 수 있는가 하는 상당인과관계설,[38] 합법칙적인 관점에서 그 행위로 인하여 발생한 결과라고 할 수 있을 때에 인과관계를 인정하는 합법칙적 조건설,[39] 결과를 행위자에게 귀속시키는 것이 규범적으로 정당화될 수 있는지 여부를 위험실현(위험의 창출 또는 증대행위가 위반한 규범의 보호범위 내 속하는지 여부) 및 회피가능성(결과에 대한 객관적 예견가능성 또는 지배가능성이 있는지 여부)의 관점에서 판단하는 객관적 귀속설[40] 등이 활용되고 있다.

본고에서 연구대상으로 하는 '해킹을 막지 못한 관리자의 법적 책임'은 과실책임에 속한다. 과실이란 법익침해라는 결과발생을 예견·회피할 수 있었음에도 불구하고 그렇게 하지 않았다는

면제된 담배를 공급받은 자가 이를 당해 용도에 사용하지 않은 경우 면세담배를 공급한 제조자에게 담배소비세와 이에 대한 가산세의 납부의무를 부담시키는 지방세법 조항이 자기책임의 원리에 반하여 위헌이라고 판단된 사례(헌법재판소 2004. 6. 24. 선고 2002헌가27 결정), 피용자의 범죄행위에 대해 사업주의 관리감독책임 여부를 묻지 않고 자동적으로 사업주를 처벌하는 양벌규정이 위헌이라고 판단된 사례(헌법재판소 2009. 7. 30. 선고 2008헌가14 결정, 헌법재판소 2010. 9. 30. 선고 2009헌가23,31 결정) 등이 있다.

35) 편집대표 박상욱·김대휘, 「주석 형법 총칙 1(제3판)」, 한국사법행정학회, 2020, 430면.

36) 예컨대 A가 땅에 흘린 바나나 껍질을 B가 밟고 미끄러져 뇌진탕으로 사망했다면, '안 흘렸다면 안 죽었을 것이다'는 조건관계가 성립하기 때문에 조건설에 따른 인과관계는 존재한다. 그러나 바나나 껍질로 인해 사람이 사망하리라는 결과까지는 사회통념상 예측하기 곤란하기 때문에 B의 사망에 대한 책임을 A에게 지우는 것은 과도하다. 또 다른 예로, 살인자의 부모가 살인자를 낳고 키운 사실과 살인이라는 결과 사이에 조건설에 따른 인과관계는 존재하지만, 그러한 살인자의 부모를 살인죄로 처벌할 수는 없다.

37) 엄상섭, "책임조건의 정형화", 23면. 이건호, "형법 제17조의 위험발생의 의미와 상당인과관계설", 형사법연구 17권, 2002, 22면에서 재인용.

38) 이건호, 앞의 글, 31면.

39) 하태영, "형법 제17조 인과관계와 객관적 귀속", 동아법학 통권 58호, 2013, 293-294면.

40) 하태영, 앞의 글, 294-301면.

법적 평가이다. 예컨대 특정한 보안조치로써 일정 유형의 해킹을 방어할 수 있음이 당해 업계에 보편화되어 있음에도 불구하고 그 조치를 하지 아니한 경우 과실이 인정될 수 있다. 그러면 과실과 결과 사이의 인과관계 유무는 어떤 기준으로 판단하는가. 교통사고의 예를 들어 보면, 선행차량에 역과되어 부상당한 채 도로에 누워있는 피해자를 후행차량의 운전자가 뒤늦게 발견하고 급제동하였으나 차량을 멈추지 못하고 2차 역과하여 사망케 한 사안에서, 대법원은 후행차량 운전자가 선행차량과의 적절한 안전거리를 유지하는 등 통상의 주의의무를 다하였다면 2차 역과사고를 방지할 수 있었으리라는 전제 하에 그 과실과 사망 사이의 인과관계를 인정한바 있다.[41] 여기서 법원은 주의의무에 합치되는 행위를 했을 때(과실이 없었을 때) 결과를 방지할 수 있었다면 과실과의 인과관계를 인정하고, 반대로 그러한 원인을 제거했음에도 불구하고 마찬가지의 결과가 발생하였을 상황이라면 인과관계를 부정하는 판단기준을 적용한 것이다. 이처럼 '적법한 대체행위에 의한 결과 회피 가능성'은 해킹 사건에서도 주요한 인과관계 판단 기준이 된다.

참고로 과실책임에 관한 사례가 방대하게 축적된 교통사고 분야에서는, 신뢰의 원칙, 즉 '교통규칙을 준수하는 운전자는 다른 교통관여자들도 교통규칙을 준수할 것이라고 신뢰하면 족하고, 다른 교통관여자들이 교통규칙을 위반하는 경우까지 예상하여 이에 대한 방어조치를 취할 의무는 없다'는 원칙이 발달되어 왔다.[42] 이는 사회적 위험부담의 적정분배원리를 배경으로 과실범의 주의의무를 합리적으로 제한하는 역할을 하는데,[43] 판례는 이를 상당인과관계의 문제로 해결하기도 한다. 직진신호에 따라 교차로를 통과한 운전자의 과속행위와 반대편에서 신호를 위반하여 좌회전을 한 차량과의 사고 사이의 상당인과관계를 부정한 사례,[44] 야간에 고속도로를 무단횡단하는 보행자를 충격하여 사망에 이르게 한 운전자의 과실과 사고 사이의 상당인과관계를 부정한 사례[45] 등이 그 예이다.[46]

민사법 분야에서도 인과관계에 대한 논의가 활발하게 이루어져 왔다. 민법 제750조는 불법행위책임의 성립 요건으로서 고의 또는 과실로 인한 위법행위와 손해 사이의 인과관계를 요구한다. 이는 사람은 자신의 고의 또는 과실 있는 행위에 대해서만 책임을 지고, 자신의 행위에 의해 야기되지 아니한 손해, 예컨대 타인의 행위 또는 우연으로 인한 손해에 대하여는 책임을

41) 대법원 2001. 12. 11. 선고 2001도5005 판결. 한편, 이 판결에 대하여는, 과연 동일한 상황에서 후행차량 운전자가 적법한 대체행위를 했을 때 피해자를 발견하고 제동을 할 수 있었을지 여부에 대해 가상의 사실을 재연하는 방법을 통해 보다 더 신중한 심리를 했어야 한다는 지적이 제기된바 있다. 송승현, "과실범에 있어 과실판단과 인과관계판단", 형사정책연구 통권 99호, 2014, 82면.

42) 김현철, "신뢰의 원칙과 그 적용한계에 관한 고찰", 서울법학 28권 1호, 2020, 249면.

43) 김현철, 앞의 글, 247면.

44) 대법원 1998. 9. 22. 선고 98도1854 판결.

45) 대법원 2000. 9. 5. 선고 2000도2671 판결.

46) 신뢰의 원칙을 상당인과관계 판단에 적용하는 판례의 태도에 대하여는, 신뢰의 원칙은 사실판단의 문제가 아니라 규범적 판단의 의무이므로 객관적 귀속의 기준 중 주의의무 위반관련성의 문제로 보아야 한다는 견해도 제기되고 있다. 김현철, 앞의 글, 287면.

지지 않는 것이 원칙이기 때문이다.[47] 그 판단 기준으로는, 객관적으로 보아 어떤 선행사실로부터 통상 일반적으로 발생할 수 있다고 인정되는 후행사실이 있는 경우에 두 사실이 상당인과관계에 있다고 하는 상당인과관계설이 기본이 되고 있다.[48] 특히 과실 불법행위에 있어서 '예견가능성' 요소는 과실 유무뿐만 아니라 인과관계 판단에도 영향을 미친다.[49]

한편, '규범의 보호목적'이 무엇인지에 따라서 인과관계 유무가 서로 다르게 판단된 사례들도 일부 있다. 예컨대 차량이 전신주를 충격하여 특고압 전선이 떨어져 인근 공장에 화재가 발생한 사안에서, 그 화재 피해는 교통사고를 낸 과실과 너무 먼 손해라고 보아 인과관계를 부정한 사례가 있다.[50] 이와 대비하여, 유사한 사고에서 사고차량 내 승객을 구조하기 위해 현장에 접근하던 사람이 넘어진 전신주의 고압선 전류에 감전되어 사망한 사안에서는 그 교통사고와 감전사고 사이의 상당인과관계를 인정한 사례가 있다.[51] 생명·신체와 관련된 손해에 대하여는 책임을 엄격하게 인정하는 반면,[52] 이보다 낮은 평가를 받는 순수한 재산상 손해의 경우 사소한 실수가 피해자의 특수한 상황과 경합되어 손실이 지나치게 과다해진 경우 이를 적절히 제한하기 위해 인과관계가 부정될 수 있다는 것이 근거이다.[53][54]

과실과 손해 사이의 인과관계와 관련하여, "적법한 대체행위를 하였어도 어차피 동일한 손해가 발생했을 것이다"는 가해자의 면책(인과관계 단절) 항변을 허용할 것인지 여부가 쟁점이

---

47) 편집대표 김용담, 「주석 민법 채권각칙 6(제4판)」, 한국사법행정학회, 2016, 130면.

48) 곽윤직, 「채권총론」, 박영사, 2004, 112면.

49) 대법원 2016. 5. 12. 선고 2015다234985 판결. 이는 금융기관이 본인확인절차를 제대로 거치지 않아 타인의 명의를 모용한 계좌가 개설된 후 그 모용계좌를 통해 별도의 사기범죄가 행하여진 사안에 관한 것이었다. 법원은 위 금융기관이 모용계좌를 개설해주었다는 사정만으로는 위 사기범죄에 대한 방조책임을 지우기에 부족하고, 위 모용계좌가 사기행위를 용이하게 한다는 사정을 위 금융기관이 구체적으로 예견하기 어려웠다는 이유로 금융기관의 과실과 사기 피해 사이의 상당인과관계를 부정하였다.

50) 대법원 1997. 10. 10. 선고, 96다52311 판결. 참고로 이 사건 피해자인 공장은 교통사고를 낸 화물차량 운전자의 소속회사 및 충격된 전신주를 관리하던 한국전력공사 모두를 상대로 손해배상을 청구하였다. 법원은, 운전자측을 상대로 한 청구에 대해서는 당해 교통사고로 인해 특고압선으로 인한 화재가 발생할 것까지 예견하기 어려웠다는 이유로 '상당인과관계'를 부정한 반면, 한국전력공사를 상대로 한 청구에 대해서는 차량이 전신주를 충격할 것까지 예견하여 보호시설을 갖출 주의의무가 있다고 보기 어렵다고 하여 '과실'을 부정하였다.

51) 대법원 1994. 10. 25. 선고 94다20655,20662 판결. 이 사례에서 법원은 교통사고귀책자가 그 사고로 발생한 고압선 등 주위의 위험요소에 의하여 감전으로 인한 인명사고가 발생할 수 있음을 충분히 예견할 수 있었다는 이유로 상당인과관계를 긍정하였다.

52) 이는 계란두개골(egg shell skull) 원칙, 즉 '불법행위자는 가해당시 피해자의 상태를 감수하여야 한다'는 영미법상 원칙을 반영한 것으로, 신체의 중요성에 비추어 피해자의 특수한 체질 등 통상 예견하기 어려운 요소라 할지라도 인과관계를 단절하지 못한다는 의미이다. 박희호, "책임법에 있어서 인과관계의 구체적 척도에 관한 연구 - 대법원 판례에서 사용되는 척도를 중심으로", 동아법학 통권 56호, 2012, 312면.

53) 박희호, 앞의 글, 312-314면.

54) 한편, 규범의 보호목적을 비롯하여 법적 평가를 인과관계의 판단기준으로 삼는 견해에 대하여는 반대 견해도 제시되어 있다. 독일은 완전배상주의를 취하기 때문에 책임설정적 인과관계(엄격한 증명)과 책임충족적 인과관계(개연성의 증명)을 구분하여 배상 범위를 제한할 도구로서의 인과관계 역할이 매우 중요하나, 우리나라는 제한배상주의를 취하기 때문에(민법 제393조, 제763조에 의하여 통상의 손해만 배상함이 원칙) 실무상 사실적 인과관계로 충분하며 규범적 인과관계를 구분할 실익이 크지 않다는 것이다. 편집대표 김용담, 앞의 책, 260-261면.

된다. 원고 보험회사의 보험계리인으로 근무한 피고가 그 임무에 위반하여 회사의 책임준비금을 과도 계상한 것을 정당한 것으로 잘못 확인함으로써 결손을 분식하게 한 결과 그 기간 동안 계약자배당에 관한 법적 제한을 회피하여 초과배당이 이루어진 사안에서, 피고가 그러한 항변을 하였다. 피고 본인의 위법한 행위가 없었더라도 어차피 원고 회사가 사옥 등에 대한 자산재평가를 통하여 합법적인 흑자 결산을 하였을 것이고 그 결과 동일한 규모의 계약자배당(자금 유출)이 있었을 것이므로 피고의 불법행위와 원고 회사의 손해 사이에 인과관계가 없다는 취지였다. 이에 대하여 법원은 '적법한 행위에 의한 동일한 손해의 발생 여부가 피해자의 별도의 의사 결정 혹은 행정관청의 허가 등 제3자의 행위에 의존하는 경우에는' 동일한 결과 발생의 가능성이 높아 명백히 예상되는 경우가 아닌 한 가해자측의 주장을 받아들이기 어렵다고 판단하였다.[55] 즉, 위 사안의 피고가 적법한 대체행위(분식회계 적발)를 하였어도 동일한 손해가 발생하였으리라는 사정은 제3의 행위(원고 회사의 자산재평가 및 합법적인 흑자 결산)에 의존하기 때문에 인과관계가 단절되지 않는다는 의미이다.

2. 해킹을 못 막은 관리자의 책임 성립요건으로서 '인과관계'에 관한 검토

가. 싸이월드 해킹 사건의 경우

싸이월드 해킹 사건의 첫 번째 취약점이었던 개인용 알집의 사내 사용 행위의 경우, 인과관계를 논하기에 앞서 과실 해당여부부터 부정되었다. SK컴즈로서는 개인용 알집을 사내에서 사용할 경우 알집 업데이트 서버가 변조되어 알집 업데이트 과정에서 악성 프로그램을 다운로드 받게 됨으로써 해킹 수단으로 악용될 것까지 구체적으로 예견하기 어려웠기 때문에, 이를 회피할 의무를 통상적인 주의의무의 범주에 넣기 곤란하다는 것이다.

나아가, 앞서 본 것처럼 예견가능성의 부존재를 들어 과실뿐만 아니라 인과관계도 부정할 수 있다는 견해가 이 부분에 적용될 수 있다. SK컴즈의 개인용 알집 사용 행위가 설령 과실에 해당한다 하더라도(가령 DB 서버를 관리하는 전산실 내 PC에서는 미리 인가된 소프트웨어만 사용해야 한다는 주의의무 또는 사내 규정을 SK컴즈가 위반했다고 보더라도), 서버 보안과 기능적으로 무관한 압축해제 용도로만 쓰이는 알집을 사용한 것이 원인이 되어 서버 접근 권한이 탈취 당하리라고는 (적어도 그 당시에는) 예견하기 어려웠다는 이유로 상당인과관계를 부정할 수 있을 것이다.

또한 신뢰의 원칙, 즉 다른 교통관여자의 교통준수를 신뢰한 운전자는 스스로 사고를 야기하지 않는 한 보호 받는다는 원칙을 유추적용하여 이 부분 인과관계를 단절시킬 여지도 있다. 알집 업데이트 서버의 해킹은 SK컴즈의 책임범위 밖에 있고, 알집은 장기간 다수의 이용자들에

55) 대법원 2005. 12. 9 선고 2003다9742 판결.

의해 보편적으로 사용되어 오면서 특별한 보안 취약점이 보고되지 않았으며, 개인용 알집과 기업용 알집이 보안기능 측면에서 차이가 나는 것도 아니기 때문에, 그러한 알집으로 인해 생긴 보안 취약점에 대해서까지 책임을 묻기 어렵다는 이론구성도 가능할 여지가 있다.

다음으로 두 번째 취약점이었던 자동 로그아웃 미설정 행위의 경우, 적법행위에 의하더라도 동일한 결과를 회피할 수 없었다 하더라도 그러한 동일한 결과의 발생 여부가 제3의 행위에 의존하는 경우에는 여전히 책임이 인정된다는 앞서 본 법리[56]를 적용해볼 수 있다. 만약 SK컴즈가 DB 서버 접속 시 다른 인증수단 없이 오로지 아이디와 비밀번호만 쓰고 있었다고 하면, 해커가 키로거를 통해 그 아이디와 비밀번호를 이미 도청한 이상 서버에 자동 로그아웃을 설정했다 하더라도 해커의 침입을 막을 수 없었을 것이므로 인과관계가 부정된다. 이와 달리, 만약 SK컴즈가 OTP까지 쓰고 있었다고 가정할 경우, 서버에 자동 로그아웃이 설정되어 있었더라면 해커가 OTP 인증을 뚫기 위해 별도의 해킹까지 성공시켰어야만 침입이 가능하므로, 적법행위에 의할 때 동일한 결과 발생 여부가 OTP 해킹이라는 제3의 행위에 의존하게 되어 여전히 인과관계가 인정될 것이다. 대법원은 전자로 판단한 반면, 후자와 같이 판단한 1심 판결도 있었다. 싸이월드 사건의 경우 행정제재가 내려지지 아니하여 해킹 원인이 낱낱이 정확하게 밝혀지지 아니한 측면이 있었고, 피해자인 원고들은 상당한 입증곤란을 겪었을 것이며, 민사소송에 명확한 증거가 현출되지 아니하여 재판부에 따라서 사실인정을 서로 다르게 한 결과 인과관계 판단이 갈리지 않았나 추측해본다. 사고 원인조사 및 인과관계 입증에 관한 제도개선 방안은 뒤의 IV.절에서 제안한다.

나. 인터파크 해킹 사건의 경우

인터파크 해킹 사건의 첫 번째 취약점인 자동 로그아웃 미설정 행위의 경우에도 적법행위에 의할 때 해킹이라는 결과를 회피할 수 있었는지 여부가 인과관계 판단의 관건이다. DB 관리직원 B의 PC에서 서버 접속 터미널 등이 로그아웃 된 상태였다고 가정할 때, 가령 해커가 B의 PC의 완전한 제어권한 또는 DB 서버 접속에 필요한 아이디 및 패스워드 등 접속권한을 이미 탈취한 상황이었다면 어떨까. 이 경우 인터파크가 자동 로그아웃을 설정했어도 해커의 침입을 막기 어려웠을 것이므로 싸이월드 사건처럼 상당인과관계가 부정될 여지가 있을 것이다. 이와 달리, 만약 해커가 B의 PC 제어권한 또는 DB 서버 접속권한을 완전히 탈취하지 못한 상황이었다면, 즉 해커가 B의 PC에 원격 접속을 해보니 마침 DB 서버와의 접속이 유지된 터미널이 떠있었던 것이 침입의 결정적 계기를 제공했다고 하면 어떨까.[57] 이 가정 하에서 자동 로그아웃이

56) 대법원 2005. 12. 9 선고 2003다9742 판결.

57) 인터파크 사건의 해커는 2016. 5. 4. 22:30 B의 PC에 최초로 원격접속했는데, DB 서버에 접속한 것은 불과 약 4시간 후인 5. 5. 02:10이고, 그 날 12:08부터 다음 날인 5. 6. 02:05까지 고객정보 DB 유출을 끝냈다고 한다. 이렇게 단시간 내 해커가 DB 서버에 침입할 수 있었다는 것은 후자의 가능성, 즉 해커가 B의 PC에

제대로 되었다면 해커가 별도의 해킹까지 성공시켰어야만 침입이 가능하므로, 적법행위에 의한 회피가능성이 그러한 제3의 행위에 의존하게 되어 인과관계가 여전히 인정될 것이다. 이러한 인과관계 여부는 해커의 침입 경로가 정확하게 조사되어야만 판단될 수 있는 사실인정의 문제이다. 그 사실관계가 명확하게 밝혀지지 않았을 때 불이익을 누가 부담하느냐는 입증책임의 문제이다.

두 번째 취약점인 패스워드 장부 노출 행위의 경우 회원정보가 유출된 DB 서버의 패스워드가 그 장부에 메모되어 있지 않았으므로 해커의 침입 원인과 무관하다. 조건설, 상당인과관계설, 적법한 대체행위에 의한 회피가능성 등을 비롯하여 어떤 이론을 적용하더라도 이 행위와 해킹 사이의 인과관계는 부존재하다고 판단된다. 인터파크 임직원들이 평소 패스워드를 평문으로 메모·공유할 정도로 보안 불감증 내지 문화적 취약점이 있었다는 사정이 해킹의 간접적인 원인을 제공했다고 볼 여지도 있으나, 이것을 가리켜 법률적 인과관계가 있다고 평가하기는 다소 곤란할 것이다.

문제는 이처럼 관리자의 과실은 있으나 이것과 인과관계가 없는 결과에 대해서까지 그 관리자의 책임으로 돌릴 수 있느냐는 것이다. 앞서 본 인터파크 행정판결은 과징금 부과 근거조항의 법문에, 민사 1심 판결은 구 정보통신망법상 법정손해배상 조항의 법문에 각각 인과관계 요건이 삭제되어 있다고 해석하면서, 인과관계 유무를 불문하고 인터파크의 공법적·민사적 책임을 인정했다. 그러나 그러한 결론에는 동의하기 어렵다. 인과관계가 부존재하다는 것은 그 행위로 말미암아 그 결과가 발생한 것이 아니라고 평가된다는 뜻이다. 자신의 행위에 의해 야기되지 아니한 결과에 대해서 책임을 지우는 것은 자기책임의 원리와 상충된다. 인터파크 사건의 경우 패스워드 장부가 노출된 것이 인터파크의 과실인 것은 맞지만, 만약 이 행위만 있었다고 가정하면 DB 서버 해킹을 당하지 않았을 것이다. 이 행위의 관점에서 보면 우연히 다른 취약점을 해커가 뚫고 침입하는 바람에 해킹이라는 결과가 터진 것이다. 해킹이라는 결과는 그 침입 원인을 제공한 취약점의 탓으로 돌려야지, 패스워드 장부 노출 행위의 탓으로 돌릴 수는 없다. 재판부로서는 인터파크에게 책임을 지우고자 하였다면 자동 로그아웃 미설정 행위와 해킹 사이의 인과관계를 심리하여 상당인과관계가 있다는 결론을 내렸으면 될 일이다. 법적 책임 요건 가운데 인과관계가 요구되지 않는다고 판결한 것은 자칫 자기책임의 원리에 위반될 수 있다. 다행히 현행 개인정보 보호법의 손해배상 규정은 보호조치의무 위반과 개인정보 유출 사이의 인과관계를 명문으로 요구하고 있고,[58] 2021. 1. 6. 입법예고된 개인정보 보호법 개정안은 과징금 부과 시 인과관계를 고려하도록 규정하고 있으므로,[59] 위와 같은 인터파크 판결의 법해석이 장래 반복되지는 않을 것으로 보인다.

원격접속 했을 때 마침 자동 로그아웃이 안 되고 DB 서버와 연결이 유지된 터미널이 떠 있었던 것이 침입의 결정적 계기를 제공하였을 가능성이 있다고 사회통념상 볼만하다.

58) 각주 22) 내지 24) 각 참조.

59) 각주 10) 참조.

다. 빗썸 해킹 사건의 경우

빗썸의 과실이 입증된 해킹 사고(제재 대상 사건)와 그렇지 않은 다른 사고들이 혼재되어 있었다. 제재 대상 사건의 경우 빗썸이 ID·PW 대입공격 등을 막지 못한 행위가 개인정보 보호조치의무 위반에 해당하고 이것과 해킹 사이의 인과관계도 존재한다는 점은 방통위의 과징금 처분 및 형사 유죄판결을 통해 선명하게 드러나 있다. 문제는, 빗썸 이용자 개인정보뿐만 아니라 266개 계정에서 합계 70억여 원의 암호화폐까지 도난당했는데, 왜 그 피해자가 빗썸을 상대로 민사소송에서 승소했다는 소식이 없느냐는 것이다. 암호화폐 도난 사실은 행정청의 보도자료에 기재된 내용이므로, 행정청은 그 266개 계정이 누구의 것이고 얼마씩이 유출되었는지 피해내역을 특정할 수 있는 접속기록(Log) 등을 분명 확보하고 있었을 것이다. 그 조사 자료가 민사소송에 공유된다면 해당 피해자는 손해배상을 받을 수 있어야 마땅한데, 왜 그러한 승소 사례가 발견되지 않는지 심히 의문이다. 이 현상은 정보통신망법상 행정청의 침해사고 조사자료가 행정처분의 근거로만 사용될 수 있도록 법률상 용도가 제한되어 있기 때문에 민사법원의 문서송부촉탁신청을 받아도 이 자료를 송부할 수 없다는 제도적 문제점에서 기인한다. 이에 대한 해결방안은 뒤의 IV.절 3.항에서 제시한다.

한편, 제재 대상 사건이 아닌 나머지 해킹 사고들의 경우, 그 피해자들이 빗썸을 상대로 제기한 민사소송은 앞서 본 것처럼 모두 청구기각되었다. 그 해킹은 위 ID·PW 대입공격 등이 아니라 원인불상의 다른 사고를 통해 유출된 것이기 때문에 당연히 빗썸의 책임으로 돌릴 근거가 없다. 그런데 만약 인터파크 판결처럼 법정손해배상 요건 가운데 인과관계가 삭제되었다고 해석하면 어떻게 될까. 이 경우 빗썸에게 한 때 ID·PW 대입공격 등을 막지 못한 과실이 존재하였고, 별건 사건이라 할지라도 개인정보가 유출되었다는 사정이 병렬적으로 존재하기만 하면 법정손해배상책임이 성립할 여지가 있는데,[60] 이는 자기책임 원칙에 어긋나는 귀결이다. 위 별건 사건에서의 피해자를 실효적으로 구제하는 제도를 설계하려면, 법적 책임 요건에서 인과관계를 삭제하는 방식으로 접근할 것이 아니라, 인과관계 입증책임을 전환시켜 인과관계 단절을 관리자로 하여금 항변하도록 하는 것이 더 바람직하다. 이에 대한 해결방안은 뒤의 IV.절 1.항에서 제안한다.

60) 물론 개인정보 유출에 관한 법정손해배상책임은 상한액이 300만원으로 규정되어 있기 때문에, 설령 이 책임이 성립하더라도 빗썸이 유출된 암호화폐의 시가에 상당하는 손해 전액을 배상할 의무는 없다. 혹자는 법정손해배상책임이 소액에 그치기 때문에 인과관계 요건을 빼더라도 개인정보처리자의 부담이 그리 가중되지 않을 것이라고 여길 수도 있다. 그러나 개인정보 유출 소송의 대부분은 재산적 손해 없이 정신적 손해만을 10만 원 내지 20만 원 선의 위자료로 청구하는 사건이고 다만 유출 피해자 수가 워낙 많다 보니 배상총액이 커지는 것이 문제라는 현실을 고려할 때, 인당 금액이 소액이라는 사유는 인과관계 요건을 달리 취급할 근거는 되지 않는다.

3. 해킹과의 인과관계는 어떻게 입증하는가

해킹 사고가 인지되면 우선 해커가 어느 경로로 침입해서 어떤 데이터를 유출했는지를 확인해야 한다. 해커의 침입 경로로 의심되는 시스템상 취약점이 드러나면, 그 취약점이 사회통념상 합리적인 주의의무를 기울였다면 막을 수 있었던 것인지(민사상 과실의 기준) 또는 법률상 개인정보 보호조치의무 위반에 의하여 야기된 것인지(공법적 책임 또는 형사처벌[61]의 기준) 여부가 판단된다. 그 다음 단계로서 인과관계 유무를 따지는데, 인과관계란 해킹 피해를 그 취약점의 탓으로 돌릴 수 있는가에 관한 문제이다. 조사된 각 취약점에 대해 관리자의 귀책여부가 가려지면, 그 다음 단계로서 각 취약점이 해커의 침입 원인·경로와 얼마나 연관이 있는지를 따져서 인과관계 여부를 판단한다. 구체적으로는, 해당 취약점이 없었더라면 해킹이 발생하지 않았겠는가(조건설), 해당 취약점이 존재한다면 통상 해커가 침입할 수 있다고 일반적으로 여겨지는가(상당인과관계설), 적법한 대체행위로써 취약점을 예방했더라면 해킹이라는 결과를 회피할 수 있었겠는가(객관적 귀속) 등을 기준으로 법적 인과관계를 판단한다.

인과관계 인정을 위해 얼마나 엄격한 입증을 요구할지에 관하여는, 앞서 본 것처럼 '규범의 보호목적'을 고려할 수도 있을 것이다. 해킹으로 인해 생명·신체 손해가 발생했다면 그 보호법익의 중요성에 비추어 인과관계를 매우 넓게 인정해야 할 것이고, 금융자산이 탈취되는 등 금전적 직접손해가 발생한 경우에도 피해 구제 흠결이 없도록 인과관계를 함부로 단절해서는 안 될 것이다. 반면, 금전손해 등 없이 오로지 개인정보만 유출되어 정신적 손해[62]가 발생한 데 그친 경우라면 관리자의 사소한 실수로 인해 손실이 과다해지는 것을 적절히 제한하기 위하여 조금 더 분명한 인과관계 입증을 요구할 수도 있을 것이다.

그렇다고 해서 형법에서처럼 합리적 의심의 여지가 없을 정도로 엄격한 인과관계 입증을 요구할 일은 아니다. 민사소송이나 행정소송에서 사실의 증명은 추호의 의혹도 없어야 한다는 자연과학적 증명이 아니고, 특별한 사정이 없는 한 경험칙에 비추어 모든 증거를 종합적으로 검토하여 볼 때 어떤 사실이 있었다는 점을 시인할 수 있는 고도의 개연성을 증명하는 것이면 충분하기 때문이다.[63] 예컨대 해커의 침입 경로를 현실적으로 완벽하게 추적하지 못하여 해커가 무슨 취약점을 공격(exploit)하여 침입했는지를 정확하게 재연하기 어렵다 하더라도, 제반 정황으로 보아 특정 취약점이 당해 해킹의 여지를 제공했을 것이라고 개연성을 합리적으로

61) 참고로 2021. 1. 6. 입법예고된 개인정보 보호법 개정안에서는 보호조치의무 위반으로 고객정보를 유출 당한 경우에 대한 형사처벌 규정을 삭제하는 방안을 제안하고 있다. 이 개정안이 통과될 경우 해킹을 당한 관리자는 과징금 등 행정법적 책임 및 민사상 손해배상책임을 부담할 뿐 형사책임을 추궁 당하는 일은 없어질 것으로 보인다.

62) 개인정보 유출로 인한 정신적 손해 쟁점에 관하여는, 전승재·권헌영, "개인정보 유출로 인한 손해배상 제도에 관한 고찰 - 신용카드 개인정보 유출 소송을 통해 드러난 제도적 한계를 중심으로", 경제규제와 법 11권 1호, 2018, 30-43면 참조.

63) 대법원 2018. 4. 12. 선고 2017두74702 판결.

추측 가능한 경우에는 그 취약점을 막지 못한 행위와 해킹 간 상당인과관계를 인정할 수 있을 것이다.[64]

특히 '적법한 대체행위에 의한 결과 회피 가능성'은 해킹 사건에서도 주요한 인과관계 판단 기준이 될 수 있다. 다른 분야, 예컨대 교통사고 분야의 경우, 앞서 본 2차 역과 사례에서처럼 후행 운전자가 그 당시 적법행위(서행 및 안전거리 준수)를 했더라면 2차 역과라는 결과를 피할 수 있었는지 가정적 상황을 재연하여 인과관계를 판단하는 것이 어려운 일이었다. 환경소송 등의 분야에서도, 사업자의 고의·과실에 따른 오염물 배출행위가 밝혀지더라도 오염원과 피해 사이의 자연과학적 인과관계를 입증하기 곤란한 사례가 많다. 이에 비하여 해킹 사안의 경우 사실적 인과관계의 존부 내지 적법행위에 의한 회피가능성을 판단하기가 상대적으로 용이한 편이다. 자주 발생하는 해킹 기법들이 유형화되어 있고 이를 방어하기 위한 보안기술 또한 세분화되어 있기 때문이다. 어떠한 보안조치를 했더라면 당해 해킹을 막을 수 있었을 것이라고 사후적 관점에서 인과관계를 평가하는 것은 그리 어려운 일이 아니다. 다만, 사후적 관점에서 꼽은 그 보안조치를 해킹 사고 발생 전부터 미리 대비했어야 한다고 요구하는 것이 사회통념상 합리적인 주의의무 범주에 포함되는지 여부, 즉 과실 여부의 판단이 진정으로 어려운 일이다.

고객정보를 해킹 당한 관리자를 제재하는 공적집행(公的執行) 사안에서는, 조사권한을 행사하는 공권력이 해커의 침입 경로, 그 원인을 제공한 취약점 및 이것이 법률상 개인정보 보호조치의무 위반에 해당한다는 점을 밝혀야 한다. 피해 고객이 관리자를 상대로 손해배상을 청구하는 사적집행(私的執行) 사안에서는 원칙적으로 피해자가 상대방의 과실 및 손해와의 인과관계를 입증해야 한다. 이 때 관리자가 당해 해킹 사고로 인해 행정처분 등 제재를 받았다면, 그 공적집행의 존재를 피해자가 민사소송에서 원용함으로써 관리자의 당연과실(negligence per se)을 입증할 수 있다. 여기서 공적집행의 근거가 된 조사자료가 민사소송에 공유될 수 있다면 더욱 실효적인 피해자 구제가 가능할 것이다.

한편, 예컨대 앞서 본 방통위의 과징금 처분이 내려지지 않은 빗썸의 별건 해킹 사건처럼 공적집행이 이루어지지 않은 사안에서는, 피해자가 관리자의 과실 및 손해와의 인과관계를 맨손으로 입증해야 한다. 그런데 피해자로서는 전산실 내에서 무슨 일이 일어났는지 알 수 없으니 이것을 입증하기가 현저히 곤란하다. 제도적으로는 특별법에 입증책임 전환규정을 두는 방안이 있다.

---

64) 예컨대 앞서 각주 57)에서는 해커가 상당히 단시간 내 침입할 수 있었다는 사실로부터 자동 로그아웃 미설정 행위가 침입의 결정적 계기를 제공했을 것이라고 추측하였다.

Ⅳ. 개인정보 보호법 개정 제언

1. 손해배상 특칙

본문에서 강조한 것처럼 자기의 행동 탓으로 발생한 것이 아닌 우연한·엉뚱한 결과에 대해서 책임을 지우지 않으려면 '인과관계' 요건은 반드시 필요하다. 한편, 위험원(危險源)을 운영함으로써 수익을 창출하는 특수한 사업자에게는 무과실책임 내지 결과책임을 지움으로써 현저하게 고도의 책임을 요구하는 분야가 있다. 환경정책기본법 제44조에 따른 환경오염 피해에 대한 무과실책임, 원자력 손해배상법 제3조에 따른 원자로 운전으로 인한 원자력손해에 대한 무과실책임 등이 그 예이다. 또한 관리자가 자신의 관리영역 내에서 위험발생원인을 배타적으로 지배하면서 이에 대한 1차적·대외적 책임을 부담하는 지위에 있을 때에도 무과실책임을 부담하는데, 민법 제758조에 따른 공작물 점유자·소유자의 책임, 국가배상법 제5조에 따른 영조물책임 등이 그 예이다. 그러나 다른 대부분의 영역에서는 자기책임의 원리 및 여기에서 파생되는 과실책임의 원리가 지배하며, 본인의 행동에서 일련의 조건적 연쇄를 거쳐 발생한 손해가 본인이 통제할 수 없었던 불가항력적·반사적인 것으로 평가된다면 이에 대한 책임을 부담시킬 수는 없다.

인터파크 사건에 적용된 구 정보통신망법상 법정손해배상 규정은 다행히 현행 개인정보 보호법에 이관되지 않았고, 현행 개인정보 보호법 제39조의2는 고의·과실로 '인하여' 개인정보가 유출된 경우를 법정손해배상 대상으로 규정함으로써 인과관계를 명문으로 요구하고 있다. 한편, 이 조항은 물론 개인정보 보호법상 일반적 손해배상 근거조항의 경우, 인과관계의 입증책임을 손해배상을 청구하는 피해자에게 지우고 있어 그 입증곤란을 제도적으로 구제해줄 필요성이 있다. 참고로 이들 손해배상 조항은 과실의 입증책임도 제대로 전환시키지 못하는 입법미비가 오래 전부터 있었으므로,[65] 이번 기회에 함께 바로잡는 것이 바람직하다.

---

65) 개인정보 보호법 제39조 제1항 본문은 '이 법을 위반한 사실'을 피해자가 입증하도록 규정하고 있는데, 당해 개인정보처리자에게 공법적 제재가 부과되지 않은 이상 그 법위반사실을 피해자가 입증하기는 곤란하다. 참고로 동조항 단서는 '해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다'라고 함으로써 일견 입증책임 전환규정의 형식을 취하고 있으나, 여기서 고의·과실이란 '개인정보 유출에 관한 고의·과실'(주의의무 위반)이 아니라 '이 법을 위반한 행위에 관한 고의·과실'을 가리키는 것인데, 그러한 과실은 행위자가 의무규범의 존재를 인식하기만 하면 저절로 인정되는 것이어서 가해자에게 반증토록 하는 것이 실무상 전혀 의미가 없다. 이동진, "개정 정보통신망법 제32조의2의 법정손해배상 해석론과 입법론", 서울대학교 법학 55권 4호, 2014, 378-379면. 김경환, "개인정보 손해배상제도의 문제점과 개선방향", 보안뉴스, 2013. 5. 22.(http://www.boannews.com/media/news_print.asp?idx=36183) 참조.
나아가 동법 제39조의2 제1항의 경우 '고의·과실' 요건이 본문과 단서에 모두 포함되어 있는데, 이 경우 본문상의 적극적 요건을 피해자가 입증해야 하는 것인지, 단서상의 소극적 요건을 관리자가 항변해야 하는 것인지 여부가 혼란스럽다.

현행 개인정보 보호법	개인정보 보호법 개정(안)
제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.	제39조(손해배상책임) ① 정보주체는 다음 각 호 중 어느 하나에 해당하는 경우에는 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의·과실 또는 인과관계 없음을 입증하지 아니하면 책임을 면할 수 없다. 1. 개인정보처리자가 이 법을 위반한 경우 2. 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우
제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.	제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 ~~개인정보처리자의 고의 또는 과실로 인하여~~ 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의·과실 또는 인과관계 없음을 입증하지 아니하면 책임을 면할 수 없다.

만약 본고의 제안에 따라 과실 및 인과관계의 입증책임을 전환하는 규정이 입법되면 어떻게 될까. 앞서 본 빗썸 사건의 경우 과실이 입증된 해킹(제재 대상 사건)과 그렇지 않은 별건 해킹 각각에 의한 피해가 혼재되어 있었는데, 별건 해킹 사건에서 빗썸이 손해배상책임을 피하려면 제재 대상 사건의 피해내역(266개 계정)을 재판부로 하여금 확인할 수 있도록 함으로써 별건 사건의 피해자가 위 피해내역에 포함되어 있지 않다는 점을 적극적으로 항변하는 쪽으로 양상이 바뀔 것이다. 이렇게 하는 것이 인과관계 요건을 아예 삭제하는 것보다 더 실효적인 피해자 구제를 가능케 한다.

나아가, 해킹의 원인을 전혀 밝혀내지 못한 사례에서는 인과관계 입증책임 전환규정이 어떻게 작용할까. 만약 침입 경로 및 원인된 취약점의 내용이 전혀 현출되어 있지 않다면 관리자가 과실 또는 인과관계의 부존재를 항변할 소지가 없게 되므로 이에 대한 손해배상책임을 떠안을 수밖에 없다. 관리자로서는 입증책임상의 불이익을 피하기 위해서라도 해킹 사고 원인을 은폐하지 못하게 되고, 오히려 행정청의 침해사고 원인조사에 적극 협조할 유인이 생기게 된다. 그래야만 면책의 근거도 함께 찾을 수 있기 때문이다. 이렇게 제도를 운영할 경우, 해킹의 원인을 못 찾은 사건이라면 그야말로 불가항력적인 사고일 수도 있고 이에 대해서까지 법적 책임을 부담시키는 것이 다소 가혹할 여지도 있겠으나, 장기적으로는 침해사고 원인조사에 대한 협조의 정도를 높이고 사회 전체적인 보안수준을 높이는데 기여할 것으로 기대된다.

2. 침해사고 원인조사 실효성 제고방안

'인과관계'가 해킹을 막지 못한 관리자의 법적 책임 성립요건이라면, 법집행주체가 그 인과관계를 실효성 있게 입증할 수 있도록 기반을 조성해주는 것이 필요할 것이다.

해킹 원인을 밝히려면 서버에 남은 접속기록(log)를 분석하는 것이 가장 기본이다. 네트워크 서비스들은 접속이 들어올 때마다 접속일시, 접속지(IP 주소), 요청한 작업내역(request) 등을 텍스트 파일에 순차적으로 기록해두는데 이것이 바로 접속기록이다. 예컨대 작업내역이 비정상적이거나 해외 등 소재탐지가 곤란한 IP 주소에서 이례적으로 잦은 접속시도를 한다면 해킹 시도를 의심해볼 수 있다. 접속기록을 분석함으로써 어느 네트워크 서비스에 취약점이 있었는지, 해커가 어느 PC 또는 서버를 경유하여 침입했는지, 정확히 어떤 데이터를 유출했는지 등도 추적한다. 즉, 해킹 당시의 접속기록을 확보하는 것은 강력범죄 현장에 남겨진 범인의 발자국, 지문, 혈흔 등을 채취하는 것만큼이나 중요하다.

문제는 현행 개인정보 보호조치의무 기준을 정한 행정규칙은 '개인정보취급자의 접속기록'에 대해서만 보존의무를 부여하고 있고,[66] '이용자의 접속기록'에 대해서는 보존의무를 규정하고 있지 않는 점이다.[67] 예컨대 해커가 개인정보취급자(피용자 또는 내부 서버)의 접속권한을 탈취하는 유형의 공격에서는 개인정보취급자의 접속기록만 가지고도 어느 정도 추적이 가능하겠으나, 외부 이용자에게 열려 있는 서버를 공격하여 오작동 시키거나 침입을 시도하는 유형인 SQL injection, parameter 변조, 이용자 계정 credential stuffing 등의 공격은 이용자의 접속기록까지 분석해야만 실효성 있는 원인조사를 할 수 있다. 이상행위 탐지 또한 마찬가지이다.

접속기록은 해커가 추적을 피하기 위해 삭제할 수도 있지만, 때로는 관리자가 법적 책임을 피하기 위해 인멸해버릴 유인도 있으며, 그러한 악의가 없더라도 서버 스토리지 부담 때문에 일상적으로 삭제해버리는 경우도 다반사다. 따라서 접속기록(특히 이용자의 접속기록)에 대해서 법령상 보존의무를 강화하고, 접속기록이 정상적으로 보존된 사례에 비하여 유실된 사례에서 보다 큰 불이익이 가하여지도록 제도를 운영할 필요가 있다.[68]

---

66) 개인정보의 기술적·관리적 보호조치 기준(2020. 8. 11. 개인정보보호위원회 고시 제2020-5호) 제5조(접속기록의 위·변조방지) ① 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.
② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.
③ 정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

67) 이용자의 접속기록 보존의무를 규정한 조항은 개인정보 보호 관련 법령에는 없고, 대신 통신비밀보호법에 있다. 이는 통신사나 인터넷 사업자측에 남은 통신사실확인자료를 범죄수사를 위해 수사기관이 제공 요청할 수 있도록 하는 법률이다. 이에 따르면 컴퓨터 통신의 로그기록 및 IP주소 추적자료는 3개월 동안 보존해야 한다. 한편, 통신비밀보호법은 사이버보안을 위해 제정된 법률이 아니기 때문에, 통신사실확인자료만 가지고는 침해사고 원인을 충실하게 조사하기에 다소 부족하다.

3. 조사자료 민사소송 공유 근거규정

빗썸 해킹 사건에 적용된 구 정보통신망법 제64조의2는, 행정청의 조사자료가 행정처분 근거로만 사용될 수 있고, 다른 용도로 활용되거나 제3자에게 제공될 수 없으며, 행정처분(또는 이에 관한 행정소송) 절차가 끝난 경우에는 즉시 폐기되어야 한다고 규정하고 있었다. 이 규정 때문에, 빗썸에서 암호화폐가 도난당한 이용자 계정 266개가 누구의 것이고 얼마씩의 피해가 발생했는지 조사한 자료가 행정청에 분명히 있는데도, 그 자료가 민사소송에서 피해자 구제를 위해 활용될 길이 막혀 있었다.

현행 개인정보 보호법의 경우 2020. 2. 4. 정보통신망법의 개인정보 보호 규정과 통합되었으나, 위 조사자료 폐기에 관한 규정은 이관되지 않았다. 만약 개인정보 보호법에 이 규정을 신설한다면, 폐기 및 비공개의 예외사유로서 '피해자가 제기한 민사소송으로부터 문서송부촉탁을 받았을 때'를 추가할 필요가 있다.

구 정보통신망법[69]	개인정보 보호법 제정(안)
제64조의2(자료 등의 보호 및 폐기) ① 과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자등으로부터 제64조에 따라 제출되거나 수집된 서류·자료 등에 대한 보호 요구를 받으면 이를 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다. ② 과학기술정보통신부장관 또는 방송통신위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보안조치를 하여야 한다. ③ 과학기술정보통신부장관 또는 방송통신위원회는 다른 법률에 특별한 규정이 있는 경우 외에 다음 각 호의 어느 하나에 해당하는 사유가 발생하면 제64조에 따라 제출되거나 수집된 서류·자료 등을 즉시 폐기하여야 한다. 제65조에 따라 과학기술정보통신부장관 또는 방송통신위원회의 권한의 전부 또는 일부를 위임 또는 위탁받은 자도 또한 같다. 1. 제64조에 따른 자료제출 요구, 출입검사, 시정	제63조의2(자료 등의 보호 및 폐기) ① 보호위원회는 개인정보처리자로부터 제63조에 따라 제출되거나 수집된 서류·자료 등에 대한 보호 요구를 받으면 이를 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다. ② 보호위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보안조치를 하여야 한다. 다만, 당해 법위반행위의 피해자를 특정하기 위한 개인정보로서 피해자의 민사상 구제 등을 위해 필요한 자료는 원문 그대로 보존할 수 있다. ③ 보호위원회는 다른 법률에 특별한 규정이 있는 경우 외에 다음 각 호에 해당하는 사유가 발생하면 제63조에 따라 제출되거나 수집된 서류·자료 등을 즉시 폐기하여야 한다. 제68조에 따라 보호위원회의 권한의 전부 또는 일부를 위임 또는 위탁받은 자도 또한 같다. 1. 제63조에 따른 자료제출 요구, 출입검사, 제64조에

68) 접속기록 보존의무 강화를 위한 행정규칙 개정 제안은, 한국아이티법연구원, 「지능정보사회에 대비한 개인정보 보호 안전조치 합리화방안」, 개인정보 보호위원회 연구보고서, 2019, 86-91면 참조.

구 정보통신망법[69]	개인정보 보호법 제정(안)
명령 등의 목적이 달성된 경우 2. 제64조제4항에 따른 시정조치명령에 불복하여 행정심판이 청구되거나 행정소송이 제기된 경우에는 해당 행정쟁송절차가 끝난 경우	따른 시정조치 등의 목적이 달성된 경우 2. 제64조에 따른 시정조치에 불복하여 행정심판이 청구되거나 행정소송이 제기된 경우에는 해당 행정쟁송절차가 끝난 경우 3. 제64조에 따른 시정조치가 내려진 법위반행위에 의하여 피해자가 생명·신체·재산상 또는 정신적 손해를 입어 개인정보처리자를 상대로 손해배상 등을 청구할 가능성이 있다고 인정되는 경우에는 그 시정조치가 내려진 날로부터 3년이 경과한 경우 [70] ④ 제1항에도 불구하고 보호위원회는 제3항 각 호에 따른 자료의 보존기간 중 당해 법위반행위의 피해자가 정보통신서비스 제공자를 상대로 제기한 소송의 수소법원으로부터 민사소송법에 따른 문서송부촉탁을 받았을 때에는 문서송부촉탁의 입증취지와 관련된 자료를 법원에 송부하여야 하며, 피해자 구제를 위해 필요한 경우 공공기관의 정보공개에 관한 법률 제9조 제1항 단서 제6호 본문 및 제7호 본문[71]에 따른 비공개사유를 적용하지 아니할 수 있다. 해당 자료를 송부 받은 법원은 필요한 경우 당해 소송의 당사자, 대리인, 그 밖에 당해 소송으로 인하여 조사자료의 내용을 알게 된 자에게 그 이를 당해 소송의 계속적인 수행 외의 목적으로 사용하지 아니할 것을 명할 수 있다.

69) 2020. 2. 4. 법률 제16955호로 개정되기 전의 것.

70) 보존기간을 처분일로부터 3년으로 제안하는 이유는, 불법행위에 의한 손해배상청구권은 민법 제766조 제1항에 의하여 손해 및 가해자를 안 날로부터 3년의 소멸시효에 걸리는데, 통상 행정처분이 내려진 날 보도자료가 배포되어 일반 소비자들이 알게 되므로 현실적으로 이 날부터 3년간 소제기 가능성이 있다고 보여지기 때문이다.

71) '개인정보로서 공개될 경우 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보'의 경우 공공기관의 정보공개에 관한 법률(이하 '정보공개법') 제9조 제1항 단서 제6호 본문에 의하여, '법인등의 경영상·영업상 비밀에 관한 사항으로서 공개될 경우 법인등의 정당한 이익을 현저히 해칠 우려가 있다고 인정되는 정보'의 경우 동 조항 제7호 본문에 의하여 각각 원칙적 비공개 대상이다. 그런데 침해사고 조사자료에 그러한 개인정보 또는 영업비밀 등이 포함되어 있다 하더라도 이를 비공개함으로써 얻어지는 이익에 비해 이를 민사소송에 제공하여 침해사고 피해자를 구제함으로써 얻어지는 이익이 더 우월하므로, 이 경우 위 비공개사유를 배제하는 방안을 제안하는 것이다.

Ⅴ. 결 론

인터파크 사건에 적용된 구 정보통신망법은, 과징금 부과 요건으로 '개인정보 보호조치의무 위반'과 '유출'을 병렬적으로 나열하고 있었고, 300만원 이하 법정손해배상의 요건 또한 마찬가지였다. 행정사건 1심 및 항소심 판결은 위 과징금 부과 근거조항이 인과과계 요건을 요구하지 않는 취지라고 해석했고, 그 영향으로 민사사건의 1심 판결은 동일한 구조의 법정손해배상 규정 또한 인과과계를 요구하지 않는 취지라고 해석했다. 그러나 이는 자기의 행위에 의하지 않고 다른 우연한 사정이 개입하여 나타난 결과에 대해서까지 개인정보처리자에게 책임을 지울 수 있다는 점에서 법치주의의 기본원칙인 자기책임의 원리에 위반될 소지가 있다. 인과관계란 조건적 연쇄에 묶인 수많은 결과 가운데 행위자가 어디까지 책임을 져야 하는지 한계를 설정하는 법적 개념으로, 쉽게 삭제해도 될 만한 요건이 아니다. 예컨대 환경오염으로 발생한 피해나 원자력발전소 방사능 유출과 같이 무과실책임을 지움으로써 관리자에게 현저하게 고도의 책임을 요구하는 특수한 분야에서는 인과관계 요건을 삭제할 수 있겠으나, 과실책임의 원리가 지배하는 다른 대부분의 분야에서는 그러하지 않다.

구 정보통신망법상 과징금 부과 조항은 정보통신망법과 개인정보 보호법이 통합되어 2020. 2. 4. 개정된 현행 개인정보 보호법 제39조의15로 이관되어 있으므로, 인터파크 행정판결의 해석이 되풀이될 여지가 있다. 다행히 주무부처가 이 문제점을 인식하였는지 2021. 1. 6. 입법예고한 개인정보 보호법 개정안에서 과징금 부과 시 인과관계를 고려하도록 명문화하고 있다. 따라서 위 개정안이 통과되면 이 문제는 해결될 것으로 보인다.

구 정보통신망법상 법정손해배상 규정은 현행 개인정보 보호법에 이관되지 않았다. 현행 개인정보 보호법 제39조의2는 고의·과실로 '인하여' 개인정보가 유출된 경우를 법정손해배상 대상으로 규정함으로써 인과관계를 명문으로 요구하고 있으며, 이것이 타당하다. 인과관계 요건을 없앤다고 해서 피해자가 폭넓게 보호되는 것이 아니며, 오히려 관리자로 하여금 해킹으로 인한 피해 내역을 은폐할 유인을 키우고, 개별 사건에서 책임소재가 불분명하다는 이유로 손해액이 감액되는 등의 반작용을 낳을 수 있기 때문이다.

해킹 분야에서는 '과실'이 입증되면 '인과관계'는 상대적으로 입증하기 요이한 편이다. 공적집행 분야의 경우 행정청으로 하여금 침해사고 원인조사를 더욱 철저하게 할 수 있도록 제도화함으로써 인과관계 입증을 가능케 하는 기반을 조성하는 것이 충분히 가능하다. 사적집행 분야의 경우 그러한 공적집행 조사자료가 민사소송에 공유될 수 있도록 하거나, 또는 입증책임 전환규정을 둠으로써 피해자 구제의 실효성을 기하는 것이 바람직하다. ▧

(논문접수 : 2020. 12. 15. / 심사개시 : 2020. 12. 30. / 게재확정 : 2021. 1. 15.)

참 고 문 헌

1. 단행본

곽윤직, 「채권총론」, 박영사, 2004.
전승재, 「해커 출신 변호사가 해부하는 해킹 판결」, 삼일인포마인, 2020.
편집대표 김용담, 「주석 민법 채권각칙 6(제4판)」, 한국사법행정학회, 2016.
편집대표 박상욱·김대휘, 「주석 형법 총칙 1(제3판)」, 한국사법행정학회, 2020.
한국아이티법연구원, 「지능정보사회에 대비한 개인정보보호 안전조치 합리화방안」, 개인정보보호위원회 연구보고서, 2019.

2. 논문

김현철, "신뢰의 원칙과 그 적용한계에 관한 고찰", 서울법학 28권 1호, 2020.
박희호, "책임법에 있어서 인과관계의 구체적 척도에 관한 연구 - 대법원 판례에서 사용되는 척도를 중심으로", 동아법학 통권 56호, 2012.
송승현, "과실범에 있어 과실판단과 인과관계판단", 형사정책연구 통권 99호, 2014.
이건호, "형법 제17조의 위험발생의 의미와 상당인과관계설", 형사법연구 17권, 2002.
이동진, "개정 정보통신망법 제32조의2의 법정손해배상 해석론과 입법론", 서울대학교 법학 55권 4호, 2014.
전승재·권헌영, "개인정보 유출로 인한 손해배상 제도에 관한 고찰 - 신용카드 개인정보 유출 소송을 통해 드러난 제도적 한계를 중심으로", 경제규제와 법 11권 1호, 2018.
전승재·권헌영, "개인정보의 기술적·관리적 보호조치에 대한 공적집행과 사적집행", 경제규제와 법 11권 2호, 2018.
하태영, "형법 제17조 인과관계와 객관적 귀속", 동아법학 통권 58호, 2013.

3.인터넷 자료

KBS, "가상화폐 거래소 해킹 손해배상 책임 첫 인정" 2019. 9. 27.(https://mn.kbs.co.kr/news/view.do?ncd=4291829).
개인정보 보호위원회, "개인정보 보호법 일부개정법률(안) 입법예고", 2021. 1. 6.(https://www.moleg.go.kr/lawinfo/makingInfo.mo?lawSeq=62160&lawCd=0&&lawType=TYPE5&mid=a10104010000).

김경환, “개인정보 손해배상제도의 문제점과 개선방향”, 보안뉴스, 2013. 5. 22.(http://www.boannews.com/media/news_print.asp?idx=36183).

김대휘, “인과관계론”, 법률신문, 2014. 11. 20.(https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=88902).

법률신문, “해킹으로 가상화폐 도난… 법원 거래소, 배상책임 없어”, 2018. 12. 20.(https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=149446).

법률신문, “해커에 가상화폐 4억 도난…법원 거래소 책임 없어”, 2018. 12. 24.(https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=149571).

전승재, “해킹과 인과관계 없는 취약점도 과징금 부과 대상인가”, 법률신문, 2019. 12. 23.(https://m.lawtimes.co.kr/Content/Article?serial=158301).

전승재, “인터파크 해킹, 대법원 심리불속행 판결에 유감”, 보안뉴스, 2020. 3. 23.(https://www.boannews.com/media/view.asp?idx=87127).

Abstract

The Causation Between The Violation of Personal Data Protection and Hacking

Jeon, Seung-Jae

The purpose of this paper is to apply the legal causation theory to the field of cyber security, especially to the case of judging the legal responsibility of a administrator who could not prevent hacking. This paper examines how the causation between the violation of personal data protection and hacking has become an issue through these three cases; Cyworld hacking, Interpark hacking, Bithumb hacking. Then this paper considers about the role of causation in determining whether security-neglected administrator bear legal responsibilities, and proposes ways to amend our legal system.

Cyworld and Interpark both encountered an APT (Advanced Persistent Threat) attack; the remote access privilege of the in-house PC was stolen. The hacker was able to invade the DB server because there was no idle timeout setting in the terminal from the PC to the server and the terminal remained connected. If the hacking could be avoided when the idle timeout was set, it could be judged that there was a causation. In Cyworld case, causation was denied after being investigated in the civil lawsuit. On the other hand, in Interpark case, this issue was discarded by a court interpretation; legal responsibility could be imposed regardless of causation. However, this interpretation is not proper because it may violate the principle of self-responsibility.

In Bithumb hacking case, there were a mixture of accidents in which Bithumb's negligence was revealed by a penalty that was imposed by the KCC, and other accidents whose cause of the hacking was unknown. In these cases, the causation plays a role in setting the scope of the burden of responsibility by classifying which incident the vulnerability is attributable to and which vulnerability is not, respectively. If the causation is not requested, there is room for responsibility for extraordinary matters, and it creates an incentive for the manager to conceal the damage.

Therefore, it is not desirable to delete the causation in the legal system. It is necessary to establish a basis for enabling causation to be easily proved, or switch the burden of proof.

Key Words : Cyber Security, Negligence, Duty of Care, Causation, Compensation, Torts, Personal Information Protection Act