위자료

[대구지법 2014. 2. 13. 2012나9865]

【판시사항】

[1] 정보통신서비스 제공자가 부담하는 개인정보보호의무의 내용 및 정보통신서비스 제공자가 개인정보보호에 실패하여 개인정보유출사고가 발생한 경우, 서비스 이용자가 계약상 채무불이행에 따른 손해배상을 청구할 수 있는지 여부(적극)

[2] 인터넷상에서 포털서비스사업을 하는 甲 주식회사가 제공하는 온라인 서비스에 가입한 회원들의 개인정보가 해킹 사고로 유출되었는데, 서비스 이용자인 乙이 甲 회사를 상대로 손해배상을 구한 사안에서, 甲 회사는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제32조에 따른 손해배상책임은 물론 계약상 채무불이행에 따른 손해배상책임도 부담한다고 한 사례

【판결요지】

[1] 정보통신서비스 제공자는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 및 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 등의 규정을 준수함으로써 이용자가 제공한 성명, 주민등록번호, 아이디, 비밀번호 등의 개인정보를 보호할 의무가 있다. 나아가 정보통신서비스 제공자가 서비스 이용약관을 통해 이용자로 하여금 개인정보를 필수적으로 제공하도록 요청하여 이를 수집하는 경우에는 위와 같이 수집한 이용자의 개인정보가 유출되지 않도록 적절한 보안시스템을 구축하고, 개인정보의 취급과정에서 안정성 확보에 필요한 합리적인 수준의 기술적 및 관리적 대책을 수립·운영할 계약상의 의무를 부담한다. 한편 서비스 이용자는 정보통신서비스 제공자 등이 구 정보통신망법상의 규정을 위반한 행위로 손해를 입으면 정보통신서비스 제공자 등에게 손해배상을 청구할 수 있고, 이 경우 해당 정보통신서비스 제공자 등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없으며(구 정보통신망법 제32조), 나아가 서비스 이용자는, 정보통신서비스 제공자가 개인정보보호에 실패하여 개인정보유출사고가 발생했을 경우 계약상 채무불이행에 따른 손해배상을 청구할 수 있고, 이 경우 이용자로서는 정보통신서비스 제공자가 기술적·관리적 보호조치의무를 위반한 사실을 주장·증명하여야 하며, 정보통신서비스 제공자로서는 통상의 채무불이행에 있어서와 마찬가지로 채무불이행에 관하여 자기에게 과실이 없음을 주장·증명하지 못하는 한 책임을 면할 수 없다.

[2] 인터넷상에서 포털서비스사업을 하는 甲 주식회사가 제공하는 온라인 서비스에 가입한 회원들의 개인정보가 해킹 사고로 유출되었는데, 서비스 이용자인 乙이 甲 회사를 상대로 손해배상을 구한 사안에서, 甲 회사는 정보통신서비스 제공자로서 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다) 및 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 등에 따라 이용자인 乙의 개인정보를 보호할 의무가 있으며, 서비스 이용약관에 따라 乙의 개인정보를 보호하기 위한 보안시스템을 구축하고, 개인정보를 취급하면서 안전성 확보에 필요한 합리적인 수준의 기술적 및 관리적 대책을 수립·운영할 계약상 의무가 있음에도 이를 위반하여 해킹 사고를 방지하지 못하고, 그 때문에 乙의 개인정보가 유출되도록 하였으므로 구 정보통신망법 제32조에 따른 손

해배상책임은 물론 계약상 채무불이행에 따른 손해배상책임도 부담한다고 한 사례.

【참조조문】

[1] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제3조 제1항, 제28조 제1항, 제32조, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조, 민법 제390조

[2] 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것) 제3조 제1항, 제28조 제1항, 제32조, 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것) 제15조, 민법 제390조

【전문】

【원고, 항소인 겸 피항소인】

【피고, 피항소인 겸 항소인】 에스케이커뮤니케이션즈 주식회사 (소송대리인 변호사 황영목 외 5인)

【제1심판결】 대구지법 김천지원 구미시법원 2012. 4. 26. 선고 2011가소17384 판결

【변론종결】2014. 1. 23.

【주문】

】

1. 원고와 피고의 항소를 모두 기각한다.
2. 항소비용은 각자 부담한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심 판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심 판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심 판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【청구취지 및 항소취지】 1. 청구취지 피고는 원고에게 3,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 2. 항소취지 가. 원고 제1심판결 중 원고 패소 부분을 취소하고, 피고는 원고에게 2,000,000원 및 이에 대하여 2011. 7. 26.부터 이 사건 소장 부본 송달일까지는 연 5%, 그 다음 날부터 다 갚는 날까지는 연 20%의 각 비율로 계산한 돈을 지급하라. 나. 피고 제1심 판결 중 피고 패소 부분을 취소하고, 그 취소 부분에 해당하는 원고의 청구를 기각한다.

【이유】

】 1. 기초 사실

가. 당사자의 지위

1) 피고는 인터넷상에서 검색, 커뮤니티 등을 기반으로 각종 정보를 제공하는 포털서비스사업을 하는 회사로, 네이트(NATE), 네이트온(NateON), 싸이월드(CYWORLD)와 같은 온라인 서비스를 제공하고 있다.

2) 원고는 구미에서 법률사무소를 운영하고 있는 변호사로서 뒤에서 살펴볼 이 사건 해킹사고가 발생하기 전 피고가 제공하는 네이트와 싸이월드의 양쪽 서비스에 가입한 사람으로, 가입 당시 피고에게 자신의 개인정보인 성명, 주민등록번호, 아이디(ID), 비밀번호, 이메일 주소, 주소, 전화번호 등을 제공하였는데, 당시 피고는 원고를 비롯하여 네이트나 싸이월드의 서비스에 가입하려는 사람들에 대하여 위와 같은 개인정보를 필수적으로 제공하도록 하였고, 이에 원고는 피고에게 위와 같은 개인정보를 제공하여야 했다.

3) 주식회사 이스트소프트(이하 '이스트소프트'라 한다)는 소프트웨어 개발 및 제조 공급업 등을 하는 회사로, 저장 용량을 줄이기 위해 파일을 압축하는 프로그램인 알집, 컴퓨터 바이러스나 악성 코드 등을 예방하거나 탐지하여 제거하는 보안 프로그램인 알약 등을 개발하여 무료 또는 유료로 제공하고 있다.

나. 해킹 사고의 발생

1) 중국에 거주하는 것으로 추정되는 인적사항을 알 수 없는 해커(이하 '이 사건 해커'라 한다)는 2011. 7. 21. 00:40경 피고의 DB 기술팀 직원인 소외 1의 컴퓨터에 윈도우 예약작업을 이용하여, 자신이 미리 설정해놓은 임의의 도메인인 'nateon.duamlive.com'에 역 접속을 시도하는 기능을 가진 악성프로그램인 'nateon.exe'를 유포하고, 2011. 7. 26.부터 2011. 7. 27.까지 중국 내 불상지에서 자신의 컴퓨터로 소외 1의 컴퓨터에 원격접속하여 피고 정보통신망에 침입하였으며, 네이트 회원정보가 저장된 데이터베이스 서버, 싸이월드 회원정보가 저장된 데이터베이스 서버, 네이트와 싸이월드에 모두 가입한 중복 회원정보가 저장된 데이터베이스 서버에 침입하여 위 각 서버에서 처리·보관하고 있는 개인정보를 아이피 주소 '(생략)'이 할당된 컴퓨터인 에듀티에스 서버(www.eduts.co.kr)로 전송하였다(이하 '이 사건 해킹사고'라 한다).

2) 이 사건 해킹사고로 말미암아 네이트 또는 싸이월드의 회원 중 34,954,887명의 개인정보가 유출되었는데, 유출된 개인정보에는 성명, 주민등록번호, 아이디(ID), 비밀번호, 이메일 주소, 주소, 전화번호 등이 포함되어 있다.

3) 피고는 2011. 7. 28. 이 사건 해킹사고를 경찰과 방송통신위원회에 신고하였고, 같은 날 네이트와 싸이월드 홈페이지를 통해 위 해킹으로 회원들의 개인정보가 유출되었다는 사실을 공지하였다.

다.

이 사건 해킹사고의 경위

1) 경찰은 2011. 7. 28. 이 사건 해킹사고에 대한 수사에 착수하였는데, 경찰의 수사 결과에 의하면, 이 사건 해커는 다음과 같은 경로로 네이트와 싸이월드 회원들의 개인정보를 유출한 것으로 파악된다.

가) 이스트소프트는 파일 압축 프로그램인 알집을 국내 공개용, 국내 기업용, 공공기관용, 교육기관용, PC방용, 해외용 등으로 구분하여 공급하고 있는데, 그중 공개용 알집은 기업용 등 다른 알집과 달리 무료로 배포하는 대신 공개용 알집을 실행할 경우 프로그램 창의 상단에 광고가 게시되도록 하여 이를 통해 이익을 얻고 있고, 공개용 알집에는 위와 같이 광고가 게시될 수 있도록 광고 콘텐츠 서버로부터 광고 내용을 불러와서 이를 실행하는 역할을 하는 'ALAD.dll'이라는 파일이 포함되어 있어서, 공개용 알집을 최초로 설치하거나 업데이트하는 경우 위 ALAD.dll 파일이 이스트소프트의 알집 업데이트 서버로부터 사용자의 컴퓨터에 내려진다.

나) 이 사건 해커는 정상적인 ALAD.dll 파일이 아닌, 같은 이름의 악성 프로그램인 ALAD.dll 파일을 만들었고, 이를 공개용 알집의 사용자 컴퓨터에 설치하기 위해 다음과 같이 이스트소프트의 알집 업데이트 서버를 이용하였다.

다) 이 사건 해커는 중국 내에 소재한 컴퓨터에 경유지를 설정하기 위한 목적으로 자신의 'Y' 드라이브를 공유한 채, 원격데스크톱 연결을 하였고, 'Y' 드라이브에 저장되어 있던 ' \ Y \ myxxx \ sb \ dangqian \ stmpxml.dll' 파일을 알집 업데이트 서버 중 하나에 최초 복사하여 알집 업데이트 웹사이트의 ISAPI 필터에 stmpxml.dll 파일을 등록시켰으며, 이를 다시 알집 업데이트 서버 중 다른 4개의 서버에 복사하여 같은 방법으로 ISAPI 필터에 stmpxml.dll 파일을 등록하였다.

라) stmpxml.dll 파일이 ISAPI 필터에 등록되면, 피고, 엔에이치엔(NHN) 주식회사(포털사이트인 네이버 등을 운영하는 회사다) 등 선별된 IP 주소에서 사용되는 컴퓨터가 알집 업데이트를 요청하는 경우, 이스트소프트가 설정한 본래의 내려받기(다운로드) 경로인 'http://aldn.altools.co.kr'이 아닌, 이 사건 해커가 설정한 악성 프로그램 유포지인 'http://inexon.softsforum.org'에서 악성 ALAD.dll 파일을 내려받게 된다.

악성 ALAD.dll 파일이 내려지면, 위 파일은 ALAD2.exe 파일을 생성·실행시키고, 이는 키로깅(keylogging) 프로그램인 Nateon.dll 파일을 실행시켜 키보드 입력값이 컴퓨터에 파일로 저장되게 한다.

마) 2011. 7. 18. 08:58:27경 피고의 컴퓨터가 알집 업데이트 과정에서 'http://inexon.softforum.org'에서 악성 ALAD.dll 파일을 최초로 내려받았고, 같은 달 20일 14:59경 피고 직원 소외 1의 컴퓨터(PC)에 nateon.exe 파일이 생성되어 같은 달 21일 02:02경 소외 1의 컴퓨터가 nateon.exe에 감염되었으며, 같은 달 23일 13:09경 소외 1의 컴퓨터에서 update.exe 파일과 windowsrpc.dll 파일이 실행되었다.

바) 이 사건 해커는 2011. 7. 26. 02:07경 소외 1의 컴퓨터를 거쳐 피고의 DB 관리자인 소외 2의 아이디로 게이트웨이에 접속하였다.

사) 이 사건 해커는 피고의 DB 서버에 침입하여 개인정보를 덤프(dump) 파일로 생성하여 압축한 다음, 이를 게이트웨이에 내려받고, 파일을 송수신하는 통신규약인 FTP(File Transfer Protocol)를 이용하여 위 개인정보 파일을 게이트웨이에서 소외 1 또는 소외 2의 컴퓨터로 내려받은 후 대한민국 내 경유지인 에듀티에스 사이트를 거쳐 중국으로 전송하였다.

그 자세한 유출 경로는 다음과 같다.

① 네이트 회원의 개인정보 유출 경로

이 사건 해커는 2011. 7. 26. 03:42경 custdb2 컴퓨터에서 DB 백업 명령어인 exp(export) 명령으로 네이트 회원 개인정보 DB를 '/data/cust.dmp'라는 덤프 포맷 파일로 저장하였고, 04:18경 pinfodb 컴퓨터에서 서로 다른 컴퓨터 사이에 파일을 복사하는 명령어인 scp(Secure Copy) 명령으로 custdb2에 저장된 '/data/cust.dmp' 파일을 /BACKUP 경로에 내려받았으며, 04:25경 pinfodb 컴퓨터에서 위 파일을 '/BACKUP/cust.dmp.bz2' 파일로 압축하였고, 05:36경 위 파일을 SFTP(Secure File Transfer Protocol, 보안 FTP) 방식으로 게이트웨이 서버의 C:₩temp에 내려받았으며, 06:22경 게이트웨이 서버에 저장된 'C:₩temp₩cust.dmp.bz2' 파일을 FTP 방식으로 소외 1의 컴퓨터에서 내려받았고, 06:33경 소외 1의 컴퓨터에 저장된 위 파일을 다시 FTP 방식으로 에듀티에스 사이트로 전송하였으며, 10:03경 에듀티에스 사이트에서 중국으로 위 파일을 전송하였다.

② 싸이월드 회원의 개인정보 유출 경로

이 사건 해커는, 2011. 7. 26. 04:37경 custdb1 컴퓨터에서 exp 명령으로 싸이월드 회원 개인정보 DB를 '/data/cymem.dmp'라는 덤프 포맷 파일로 저장하였고, 05:08경 pinfodb 컴퓨터에서 scp 명령으로 custdb1에 저장된 '/data/cymem.dmp' 파일을 /BACKUP 경로에 내려받았으며, 05:15경 pinfodb 컴퓨터에서 위 파일을 '/BACKUP/cymem.dmp.bz2' 파일로 압축하였고, 05:36경 위 파일을 SFTP 방식으로 게이트웨이 서버의 C:₩temp에 내려받았으며, 06:21경 게이트웨이 서버에 저장된 'C:₩temp₩cymem.dmp.bz2' 파일을 FTP 방식으로 소외 1의 컴퓨터에서 내려받았고, 06:32경 소외 1의 컴퓨터에 저장된 위 파일을 다시 FTP 방식으로 에듀티에스 사이트로 전송하였으며, 09:44경 에듀티에스 사이트에서 중국으로 위 파일을 전송하였다.

③ 중복 회원정보의 유출 경로

이 사건 해커는, 2011. 7. 26. 04:08경 custdb1 컴퓨터에서 exp 명령으로 네이트와 싸이월드에 중복으로 가입한 회원 개인정보 DB를 '/tmp/pits.dmp'라는 덤프 포맷 파일로 저장하였고, 04:24경 pinfodb 컴퓨터에서 위 파일을 '/tmp/pits.dmp.bz2' 파일로 압축하였으며, 05:41경 pinfodb에 저장된 '/BACKUP/pits.dmp.bz2' 파일을 SFTP 방식으로 게이트웨이 서버의 C:₩temp에 내려받았고, 같은 달 27일 01:13경 게이트웨이 서버에 저장된 'C:₩temp₩pits.dmp.bz2' 파일을 FTP 방식으로 소외 2의 컴퓨터에서 내려받았고, 01:30경 소외 2의 컴퓨터에 저장된 위 파일을 다시 FTP 방식으로 에듀티에스 사이트로 전송하였으며, 06:30경 에듀티에스 사이트에서 중국으로 위 파

일을 전송하였다.

2) 경찰은 2012. 6. 20. 이 사건 해커에 대해 기소중지 의견으로 서울중앙지방검찰청에 사건을 송치하였다.

라. 관련 법령

구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '정보통신망법'이라 한다), 구 정보통신망법 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것, 이하 '정보통신망법 시행령'이라 한다), 정보통신망법 제28조 제1항 및 같은 법 시행령 제15조 제6항에 따라 제정된 개인정보의 기술적·관리적 보호조치 기준(2011. 1. 5.자 방송통신위원회 고시 제2011-1호, 이하 '이 사건 고시'라 한다) 중 이 사건과 관련된 규정은 별지 관련 법령 기재와 같다.

[인정 근거] 다툼 없는 사실, 갑 제1, 2, 3, 11, 18, 23, 24호증, 을 제31, 32호증의 각 기재, 변론 전체의 취지

2. 당사자의 주장

가. 원고 주장 요지

피고는 대규모의 개인정보를 관리하는 인터넷 사업자로서 다음과 같이 서비스이용계약(약관)과 정보통신망법 등 관련 법령에서 정한 기술적·관리적 보호조치 및 보안조치의무 등을 제대로 이행하지 아니한 과실이 있고 이 때문에 원고의 개인정보가 유출되는 이 사건 해킹사고가 발생하였으므로, 원고에게 개인정보 유출로 원고가 입은 정신적 손해에 대한 위자료로 300만 원과 이에 대한 지연손해금을 지급할 의무가 있다.

1) 피고는 싸이월드, 네이트 등의 회원가입자들로부터 주민등록번호, 주소 등의 개인정보를 수집하지 않더라도 정보통신서비스 제공에 아무런 지장이 없음에도, 원고의 주민등록번호, 주소 등의 개인정보를 수집하여 보관하였는바, 피고는 정보통신망법상 개인정보 최소수집의무를 위반하였다.

2) 피고는 그 직원들이 유료로 제공되는 국내 기업용 알집 프로그램을 사용하도록 관리할 의무가 있음에도, 보안에 취약한 국내 공개용 알집 프로그램을 사용하도록 내버려두어 이 사건 해킹사고의 원인을 제공하였다.

3) 피고는 개인정보가 보관된 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 감시하고, 통상적으로 수행되는 업무와 다른 형태의 업무가 수행되거나 비정상적인 트래픽이 발생할 경우 이를 탐지하여 조처할 수 있도록 적절한 침입차단시스템과 침입방지시스템을 갖출 의무가 있는데, 이 사건 해커가 약 3,500만 명에 이르는 회원의 개인정보를 유출하는 동안 대규모 데이터 전송이 발생하였음에도, 이를 탐지하거나 차단하지 못함으로써 기술적·관리적 보호조치의무를 위반하였다.

4) FTP(File Transfer Protocol)는 파일 전송을 위한 프로토콜로서 대량의 파일을 쉽게 송수신하는 역할을 하므로 개인정보를 보관하는 DB 서버와 관련된 곳에서는 사용되어서는 안 된다.

또한, FTP 방식 프로토콜이 설정된 곳에서는 해커가 아주 빨리 대량의 정보를 빼내가는 것이 가능하고, 해킹에 걸리는 시간이 짧아질수록 해킹의 탐지 및 적발이 어려워, 해킹 사고 발생의 위험이 커진다.

이러한 FTP 방식 프로토콜의 취약점 때문에 피고 또한 내부적으로 정한 '개인정보보호 업무지침서' 제26조 제4항에서 DB 서버 관리자의 PC에 FTP 방식의 프로토콜 서비스 등 보안상 취약한 서비스는 제공하지 못하도록 규정하고 있다.

나아가 정보통신망법 제45조에 따라 방송통신위원회가 2010. 2. 3. 고시한 정보보호조치 및 안전진단 방법·절차·수수료에 관한 지침 [별표1]의 2.2.8.에 따르면, 피고는 정보통신망의 안정성 등을 확보하기 위하여 게이트웨이 서버에서 불필요한 FTP를 제거할 의무가 있음에도, 게이트웨이 서버와 DB 서버 관리자의 PC에 FTP 방식의 프로토콜을 설정

하였다.

이로써 이 사건 해커는 게이트웨이 서버와 DB 서버 관리자인 소외 1, 2의 각 컴퓨터에 설정되어 있던 FTP 방식의 프로토콜을 이용하여 DB 서버로부터 개인정보를 유출해 갈 수 있었다.

5) 이 사건 해킹 사고가 발생하기 전날인 2011. 7. 25. 16:48경부터 17:29경까지 DB 서버 관리자인 소외 1이 자신의 컴퓨터로 DB 서버에 로그인하고 업무를 수행하였는데, 작업이 종료된 이후에도 로그아웃하지 아니하였다.

더구나 피고는 그 직원이 작업을 수행한 후 로그아웃하지 않더라도, 일정 시간 동안 아무런 작업도 수행하지 않으면 자동으로 로그아웃되어 다시 로그인해야 하는 방식 또는 작업이 지나치게 긴 시간 동안 이어질 경우 자동으로 로그아웃되어 다시 로그인해야 하는 방식의 로그인 시간제한설정 등의 기술적 보안조치를 두지 않았다.

이로써 이 사건 해커는 DB 서버에 접속하기 위한 두 번째 단계의 인증, 즉 DB 서버 관리자의 이메일로 전송된 일회용 비밀번호(OTP, One Time Password)를 입력하지 않고 DB 서버에 접속하여 개인정보를 유출해 갈 수 있었다.

나아가 설령 피고 주장과 같이, 피고의 DB 관리자가 내부에서 DB 접속 시 아이디와 비밀번호만 입력하면 되도록 하였을 뿐 OTP 등 추가적인 인증수단을 거치도록 하지 않았다면, 그 자체로 안전한 인증수단 적용의무를 위반한 과실이 있다.

6) 이 사건 해커가 데이터베이스 서버의 관리자 아이디와 비밀번호를 습득하였고, 직원의 컴퓨터로 데이터베이스 서버에 접속하여 개인정보를 유출하였다는 것은 피고가 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하는 방법으로 인가받지 않은 접근을 제한하지 않았던 것으로 볼 수 있는바, 피고는 불법 접근을 탐지하거나 방지하기 위한 시스템을 설치하거나 운영하지 않은 잘못이 있다.

7) 피고는 MD5 방식을 사용하여 비밀번호를 암호화하였는데, MD5 방식은 보안상 취약점이 지적되는 암호화 방식으로, 위 방식만으로는 안전한 보호조치가 이루어진 것으로 보기 어렵고, 피고가 여기에 개별 이용자별로 별개의 값을 추가해서 해시함수를 적용하여 변형된 암호화 방식을 사용하였다 하더라도, 피고가 사용한 해시함수는 이용자의 비밀번호에 이용자의 아이디를 붙인 것에 불과하여, 이 사건 해킹 사고로 이용자의 아이디가 유출된 이상 피고가 암호화한 개인정보는 쉽게 해독 가능하므로, 피고는 개인정보가 안전하게 저장·전송될 수 있는 암호화 기술을 사용할 의무를 위반하였다.

나. 피고의 주장

이에 대하여 피고는 다음과 같은 이유에서 원고의 청구에 응할 수 없다고 주장한다.

① 피고는 관련 법령에서 정한 기술적·관리적 보호조치를 모두 준수하였다.

따라서 원고의 개인정보가 유출되었다는 이유만으로 피고에 책임을 묻는 것은 결과책임을 묻는 것과 마찬가지이다.

② 원고의 개인정보가 유출되었다는 사실만으로 원고에게 실질적인 손해가 발생한 것으로 볼 수 없으며, 가사 원고에게 손해가 발생하였다 하더라도, 지적재산권을 보호하는 저작권법의 보호법익을 고려하면, 피고의 국내용 알집 사용에 따른 저작권법 위반행위와 원고의 손해 발생 사이에는 상당인과관계가 없다.

나아가 국내 기업용 알집 프로그램에도 ALAD.dll 파일이 존재하고, 그 업데이트 방식도 국내 공개용 알집 프로그램의 업데이트 방식과 똑같은 이상 피고가 국내 기업용 알집 프로그램을 사용하였다 하더라도, 이 사건 해커의 침입이 가능하였다고 할 것이므로, 피고의 국내 공개용 알집 프로그램 사용이 이 사건 해킹사고의 발생과 인과관계가 있다고 볼 수 없다.

3. 판단

가. 정보통신서비스 제공자의 개인정보보호의무 및 이용자의 손해배상청구권

1) 정보통신서비스 제공자는 정보통신망법 및 같은 법 시행령 등의 규정을 준수함으로써 이용자가 제공한 성명, 주민등록번호, 아이디, 비밀번호 등의 개인정보를 보호할 의무가 있다.

나아가 정보통신서비스 제공자가 그 서비스 이용약관을 통해 이용자로 하여금 개인정보를 필수적으로 제공하도록 요청하여 이를 수집하는 경우에는 위와 같이 수집한 이용자의 개인정보가 유출되지 않도록 적절한 보안시스템을 구축하고, 개인정보의 취급과정에서 안정성 확보에 필요한 합리적인 수준의 기술적 및 관리적 대책을 수립·운영할 계약상의 의무를 부담한다.

2) 한편 서비스 이용자는 정보통신서비스 제공자 등이 정보통신망법상의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자 등에게 손해배상을 청구할 수 있고, 이 경우 해당 정보통신서비스 제공자 등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없으며(정보통신망법 제32조), 나아가 서비스 이용자는, 정보통신서비스 제공자가 개인정보보호에 실패하여 개인정보유출사고가 발생했을 경우 계약상의 채무불이행에 따른 손해배상을 청구할 수 있고, 이 경우 이용자로서는 정보통신서비스 제공자가 기술적·관리적 보호조치의무를 위반한 사실을 주장·입증하여야 하며, 정보통신서비스 제공자로서는 통상의 채무불이행에 있어서와 마찬가지로 그 채무불이행에 관하여 자기에게 과실이 없음을 주장·입증하지 못하는 한 책임을 면할 수 없다.

나. 손해배상책임의 발생

1) 피고는 정보통신서비스 제공자로서 앞서 본 바와 같이 정보통신망법 및 같은 법 시행령 등에 따라 그 이용자인 원고의 개인정보를 보호할 의무가 있으며, 네이트와 싸이월드의 서비스 이용약관에 따라 원고의 개인정보를 보호하기 위한 보안시스템을 구축하고, 개인정보를 취급함에 있어 안전성 확보에 필요한 합리적인 수준의 기술적 및 관리적 대책을 수립·운영할 계약상 의무가 있음에도 다음과 같이 이러한 의무를 위반하여 이 사건 해킹사고를 방지하지 못하고, 그 때문에 원고의 개인정보가 유출되도록 하였으므로 정보통신망법 제32조에 따른 손해배상책임은 물론 계약상 채무불이행에 따른 손해배상책임 또한 부담한다.

가) 대용량 개인정보의 유출 탐지와 방지를 위한 기술적·관리적 보호조치의무 위반

갑 제12호증의 1, 2, 3, 5, 갑 제18, 22, 24, 27, 28호증, 을 제13호증의 5, 6, 을 제20호증의 3에서 14, 을 제31호증의 각 기재에 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정에 비추어 보면, 피고는 정보통신망법 제28조 제1항, 같은 법 시행령 제15조, 이 사건 고시 제8조 및 이용자의 개인정보보호를 위한 적절한 보안시스템의 구축과 기술적·관리적 보호조치를 취할 계약상의 의무를 위반하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입탐지시스템을 적절히 운영하지 못하고, 개인정보의 출력·복사 시 필요한 보호조치를 갖추지 못한 잘못으로 이 사건 해커가 개인정보 DB에 접속하여 원고를 포함한 34,954,887명의 개인정보를 덤프 파일로 생성하고(이는 이 사건 고시 제8조의 '출력'에 해당한다), 이를 게이트웨이, 소외 1 또는 소외 2의 컴퓨터, 에듀티에스 사이트 등을 거쳐서 중국으로 유출하는 것을 탐지하지 못하였다고 봄이 타당하다.

① 피고는 개인정보에 대한 불법적인 접근 및 유출을 차단하기 위하여 개인정보가 보관된 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 감시하고(모니터링), 통상적으로 수행되는 업무와 다른 형태의 업무가 수행되거나 비정상적인 트래픽(특정 전송로 상에서 일정 시간 내에 흐르는 데이터의 양)이 발생할 경우 이를 탐지하여 보안관리자에게 즉시 경고함으로써 보안관리자가 이에 대해 조처를 할 수 있도록 하는 침입탐지시스템을 갖출 의무가 있

다.

이에 대하여 피고는 당시 정보통신망법 등의 관련 법령상 피고가 개인정보에 대한 불법적인 접근을 차단하기 위해 취했어야 할 기술적·관리적 보호조치에 위와 같은 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역 등을 감시해야 할 의무가 포함되지 않는다고 주장하나, 정보통신망법 제28조 제1항, 같은 법 시행령 제15조, 이 사건 고시 제8조의 규정은 피고와 같은 정보통신서비스 제공자에게 개인정보에 대한 불법적인 접근을 차단하기 위한 침입탐지시스템을 적절하게 설치 및 운영하고, 개인정보의 출력·복사 시 필요한 보호조치를 갖추어야 할 의무를 규정하고 있는 점, 외부에서의 권한 없는 자의 접근은 물론 이 사건 해킹 사고와 같이 권한 없는 자가 권한 있는 자의 아이디와 비밀번호를 도용하여 접근하는 경우 또한 '불법적인 접근'에 해당하는 점, 따라서 위와 같은 불법적인 접근을 차단하기 위한 적절한 침입탐지시스템을 설치하고 이를 운영할 의무에는 그 접근이 피고의 정보통신망 외부에서 이루어졌든 내부에서 이루어졌든 통상적으로 수행되는 업무와 다른 형태의 업무가 수행되거나 비정상적인 트래픽이 발생할 경우 이를 탐지하여 보안관리자에게 이에 대해 조처를 할 수 있도록 하는 감시활동을 수행할 의무가 포함된다고 봄이 타당한 점(뒤에서 보는 바와 같이, 피고는 DB 관리자의 컴퓨터를 통해 내부에서 피고의 개인정보시스템에 접근하는 경우 아이디와 비밀번호를 입력하는 것 외에 추가적인 인증수단을 적용하지 않았던 점에서 내부관리자에 의해서 또는 내부관리자의 아이디와 비밀번호를 도용한 해킹 등을 통해서 언제든지 이용자의 개인정보가 한꺼번에 유출될 수 있는 위험이 있었고, 뒤에서 보는 바와 같이 당시 피고로선 그와 같은 위험을 충분히 예측할 수 있었다고 보이므로, 이를 방지하기 위한 기술적·관리적 보호조치로서 위와 같은 감시활동이 수반되는 침입탐지시스템을 갖출 의무가 있었다 할 것이다)에서 피고의 위 주장은 이유 없고, 나아가 피고는 앞서 본 바와 같이 원고를 포함하여 34,954,887명에 이르는 대규모의 개인정보를 수집하고 있던 정보통신서비스 제공자로서 그 이용자들에 대하여 이 사건 해킹사고와 같이 접근권한 없는 해커가 DB 관리자의 아이디와 비밀번호를 도용하여 불법적으로 접근(해커 등 접근권한 없는 자가 내부관리자 등 접근권한 있는 자의 아이디와 비밀번호를 도용하여 이루어지는 접근은 그것이 정보통신망 외부에서의 접근이든 또는 내부망을 통한 접근이든 모두 권한 없는 자의 불법적인 접근이라고 보아야 할 것이다)하는 경우에 대비하여 개인정보가 보관된 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 실시간으로 감시하고, 비정상적이거나 수상한 업무내역이 탐지되는 경우 이를 보안관리자에게 즉시 경고함으로써 보안관리자가 이에 대해 조처를 할 수 있도록 하는 침입탐지시스템을 갖출 계약상 의무를 부담한다고 봄이 타당하므로[이 사건 해킹사고 이전에 피고와 같은 정보통신서비스 제공자가 보관하는 대량의 개인정보가 유출되는 사고가 있었던 점, 더구나 피고는 이 사건 해킹사고 이전에 국내에서 발생한 해커나 내부자를 통한 개인정보 유출 사례와 그 원인 등을 잘 알고 있었던 점(갑 제13호증의 5, 6), 피고 자신도 여러 차례 해커로부터 공격을 받은 전력이 있었던 것으로 보이는 점 등에 비추어 보면, 당시 대규모 개인정보를 수집하고 있던 피고로서는 이 같은 사고가 발생할 수 있음을 충분히 예측할 수 있었다고 할 것이고, 따라서 이에 대비한 합리적 수준의 기술적·관리적 보호조치를 취했어야 할 의무가 있다], 이 점에서도 피고의 위 주장은 받아들이기 어렵다.

② 다만 개인정보 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 실시간으로 감시하면서 어떠한 업무 형태가 나타나거나 어느 정도의 트래픽이 발생했을 때 이를 이상 징후라고 판단하여 DB 관리자에게 경고하도록 할 것인지는 일률적으로 정할 수 없고, 해당 DB를 보유한 정보통신서비스 제공자가 수행하는 업무의 특성이나 서비스 이용자의 수, 정상적인 업무수행 과정에서 평균적으로 발생하는 트래픽 및 그 양상 등에 비추어, 필요한 업무를 수행하는 것에 지나치게 방해가 되지 않으면서도 개인정보 보호에 소홀하지 않은 적절한 수준으로 설정할 수밖에 없

다.

③ 이와 관련하여 피고가 침입차단 및 탐지의 목적으로 주식회사 안철수연구소, 인포섹 주식회사 등과 개인정보시스템에 대한 침입차단시스템 또는 침입탐지시스템 설치, 유지보수, 증설계약 등을 체결하여 침입차단시스템과 침입탐지시스템을 설치·운영하고 있었던 사실은 인정된다.

그러나 이 사건 해킹사고 발생 당시 피고의 침입탐지시스템 등이 DB 관리자나 보안관리자에게 경고하지 않았다는 것은 이 사건 해커가 수행한 업무 내역이나 그 과정에서 발생한 트래픽이 피고가 설정한 경고 발생의 기준에 따를 때 이상 징후로 판단되지 못하였다는 것을 의미하는바, 다음과 같은 사정, 즉 ㉮ 이 사건 해킹사고로 피고의 내부망에서 총 34,954,887명의 개인정보가 2G, 2G, 6G 등 총 10G의 크기로 외부로 유출되었는데, 피고는 당시 기밀 또는 중요 정보에 대한 유출을 차단하기 위한 DLP(Data Loss Prevention) 솔루션을 갖추고 있어서, 위 솔루션을 통해 개인정보 등 특별한 보호가 필요한 정보를 그 밖의 다른 정보와 구별하여 충분히 식별할 수 있었으므로, 위와 같이 유출된 10G의 파일에 개인정보가 들어 있다는 것을 알 수 있었다고 보이는바, 설령 피고의 통상적인 업무수행 과정에서 발생하는 트래픽에 비추어 10G의 크기가 현저한 대용량이라고는 할 수 없더라도, 개인정보는 텍스트 파일이어서 차지하는 용량이 크지 않다는 점에 비추어, 10G의 개인정보가 처리되고 있다는 것은 결국 대다수 회원의 개인정보가 처리되고 있다는 것을 뜻하므로, 피고가 당연히 주의를 기울였어야 할 대용량의 트래픽 발생이라고 볼 수 있으며, 게다가 이 사건 해킹사고가 트래픽이 많이 발생하지 않는 새벽에 원격접속의 방법으로 이루어졌다는 점에서도 이상 징후로 의심할 가능성이 더욱 컸던 점, ㉯ DB 관리자라고 하더라도 개인정보를 파일로 생성하거나 게이트웨이 등으로 내려받을 필요 없이 select 명령어를 통해 조회하는 방법으로 대부분 업무를 처리할 수 있으리라고 보이므로, 이 사건 해커가 exp 명령어를 사용하여 개인정보를 파일로 생성하여 출력하였다는 것은 그 자체로 특이한 업무수행 내역이라고 볼 수 있는데도 피고의 침입탐지시스템 등에서는 이를 이상 징후로 감지하지 못한 점, ㉰ 더구나 앞서 본 바와 같이 이미 이 사건 해킹사고 이전에 피고와 같은 정보통신서비스 제공자가 보관하는 대량의 개인정보가 유출되는 사고가 있었으므로, 피고로서는 고객의 개인정보보호를 위해 해커가 DB 관리자의 아이디 등을 이용하여 정당한 DB 접속권한을 가진 것처럼 DB에 접근하고, 개인정보를 대량으로 그대로 출력하는 비정상적 상황이 발생하는 경우에 대비하여 일정 규모 이상의 개인정보 출력이 있을 경우 침입탐지시스템 등에서 이를 이상 징후로 감지하도록 하여, 실제로 정당한 접속권한을 가진 사람이 업무 수행의 목적으로 이러한 작업을 하는 것인지를 확인할 수 있도록 하는 등의 적절한 보안조치를 취했어야 할 것인데, 이러한 보안조치를 취하고 있지 않았던 점, ㉱ 나아가 이 사건 해커가 이틀에 걸쳐서 대용량의 개인정보 파일을 DB 서버에서 게이트웨이로 내려받고, FTP 방식으로 위 파일을 게이트웨이에서 소외 1 또는 소외 2의 컴퓨터를 거쳐 결국 외부망인 에듀티에스 사이트에까지 전송하는 동안에도 이를 전혀 탐지하지 못했다는 것은 개인정보가 대량으로 전송되는 것을 이상 징후로 감지하는 기준 등이 설정되지 않은 상태였다고 볼 수밖에 없는 점(특히 개인정보가 내부망을 벗어나 외부로 전송되는 것은 더욱 철저히 탐지했어야 한다고 보인다) 등을 종합하면, 피고가 설정한 침입탐지시스템의 수준이 지나치게 완화되어 있어서 개인정보를 보호하기에 매우 부족한 수준이었고, 이 때문에 이 사건 해킹사고를 탐지하지 못하였다고 봄이 타당하다.

나) 게이트웨이 서버와 DB 서버 관리자 PC에 보안상 취약한 FTP 방식의 프로토콜을 설정한 잘못

피고의 DB에서 유출된 개인정보 파일이 FTP 방식으로 게이트웨이에서 소외 1 또는 소외 2의 컴퓨터를 거쳐서 에듀티에스 사이트로 전송된 사실은 앞서 본 바와 같고, 갑 제24, 27, 28호증, 을 제8호증의 각 기재에 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정, 즉 ① FTP는 파일 전송을 위한 프로토콜로 대량의 파일을 쉽게 송수신하는 구

실을 하는 만큼 일반적으로 보안상 취약하다고 여겨지고 있는 점, ② 피고 또한 FTP의 이러한 취약점을 인지하고 내부적으로 만든 개인정보보호 업무지침 제26조에서 "개인정보 접근권한이 있는 컴퓨터에 FTP 서비스 등 보안상 취약한 서비스는 제공하지 않도록 한다"고 규정하고 있는 점(피고는, 위 규정은 개인정보에 접근권한이 있는 컴퓨터가 FTP 서버로 사용되는 것을 제한하는 의미일 뿐, FTP 클라이언트로 사용되는 것을 제한하는 의미는 아니라고 주장하나, 위 규정의 문언 자체에 비추어 볼 때, 피고가 주장하는 바와 같이 FTP 서버로 제공되는 경우만 제한하여 규정하고 있다고 보기 어렵고, FTP 클라이언트로 사용되는 컴퓨터에서도 파일의 대량 수신뿐만 아니라 송신도 가능하므로, 보안상 문제가 발생할 수 있는 것은 마찬가지이다), ③ 위와 같이 피고 스스로 보안상 취약한 서비스로 인지하여 개인정보 접근권한이 있는 컴퓨터에 FTP 서비스를 제공하지 않도록 업무지침을 내렸던 점에서 피고의 게이트웨이 서버의 FTP 프로토콜과 DB 서버 관리자 PC의 FTP 클라이언트 기능이 피고의 평소 업무에 반드시 필요하였다고 보이지도 않는 점 등을 종합하면, 피고는 보안상 취약한 FTP가 게이트웨이 및 개인정보 접근권한이 있는 컴퓨터에서 기능하도록 함으로써, 이 사건 해커가 FTP 방식으로 개인정보가 대량으로 외부에 유출되도록 하는 데에 기여하였다고 봄이 타당하다.

다) 피고 직원 컴퓨터에서 기업용이 아닌 국내 공개용 알집을 사용하는 것을 방지하지 않은 잘못

법령에 위배된 행위와 제3자의 손해 사이에 상당인과관계의 유무를 판단함에 있어서는 해당 법령의 입법 목적과 보호법익, 위 법령 위배행위의 태양 및 피침해이익의 성질 등을 종합적으로 고려하여 판단하여야 한다(대법원 1995. 1. 12. 선고 94다21320 판결 참조).

이 사건에 관하여 보건대, 이스트소프트의 라이센스 정책에 의하면 공개용 알집은 개인이 가정에서 사용하는 용도로만 무료로 제공되며, 피고와 같은 기업에서는 기업용 알집을 유료로 구매 또는 대여하여 사용하여야 함에도, 이 사건 해킹사고 당시 피고의 직원들이 공개용 알집을 사용한 사실은 당사자 사이에 다툼이 없으므로, 피고는 직원들이 위와 같이 공개용 알집을 사용하는 것을 방지하지 않은 잘못으로 이스트소프트의 알집 저작권을 침해하였다고 볼 수 있고, 나아가 갑 제11, 18, 23, 24, 27, 28호증, 을 제31, 47호증의 각 기재에 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정을 종합하면, 피고가 직원들의 공개용 알집을 사용하는 것을 방지하지 않은 잘못과 이 사건 해킹사고 발생 사이에 상당인과관계를 인정할 수 있다.

① ALDA.dll 파일은 알집의 주요 기능인 파일 압축 및 압축된 파일 해제와 무관하게 광고를 게시하는 역할을 하는데, 이 사건 해커는 위 파일과 같은 이름의 악성 파일을 만들고, 피고를 포함한 선별된 IP 주소를 사용하는 컴퓨터가 공개용 알집 업데이트를 하기 위해 이스트소프트의 알집 업데이트 서버에 접근하는 경우 악성 ALAD.dll 파일을 내려받도록 이스트소프트의 ISAPI 필터를 변조하는 등 공개용 알집을 이 사건 해킹사고의 도구로 이용하였다.

② 비록 국내 기업용 알집 프로그램도 업데이트 시 업데이트 서버로부터 국내 공개용 알집 프로그램과 동일한 ALAD.dll 파일이 포함된 업데이트 파일을 전송받고, 공개용 알집과 기업용 알집의 업데이트서버가 같다고 보이지만, 다음과 같은 사정, 즉 ㉮ 기업용 알집 프로그램은 국내용 알집 프로그램과는 달리 ALAD.dll 파일을 사용하지 않도록 프로그램되어 있어, 업데이트 시 업데이트 서버로부터 국내 공개용 알집 프로그램과 동일한 ALAD.dll 파일이 포함된 업데이트 파일을 전송받더라도 실제로 위 ALAD.dll 파일이 로드되거나 실행된 기회는 없는 점(을 제47호증), ㉯ 공개용 알집을 실행하면 사용자 컴퓨터와 알집 서버가 인터넷으로 연결되어 실시간으로 상호 통신이 이루어지면서 다량의 패킷(네트워크 전송 데이터의 최소 단위)이 발생하는 반면, 사용자 컴퓨터와 알집 서버의 경우 사용자 컴퓨터에 현재 설치된 알집의 최신 버전 여부를 확인하기 위하여 미리 설정한 기간마다 주기적으로 알집 서버에 접속할 뿐이어

서, 실시간으로 상호통신이 이루어지거나 다량의 패킷이 발생하지 않으므로, 공개용 알집과 같이 실시간으로 외부 서버와 연결된 프로그램을 이용하는 것이 일반적으로 외부 서버와 연결이 끊어져 있는 프로그램을 이용하는 것보다 더 쉽게 해킹의 대상이 되리라고 보이는 점, ㉰ 공개용 알집이 실시간으로 알집 서버에 연결된 이유는 광고 컨텐츠 서버로부터 광고 내용을 받기 위해서여서 이 사건 해킹사고에 이용된 알집 업데이트 서버와 직접적인 관련은 없다고 하더라도, 공개용 알집이 위와 같이 외부와의 연결이 더 자주 이루어진다는 것은 공개용 알집을 이용하여 사용자 컴퓨터의 방화벽 내부로 더 쉽고 빠르게 진입할 수 있다는 것을 의미한다고 볼 수 있으므로, 보안상의 취약점이 발생할 여지가 크다고 볼 수 있는 점(이에 반하여 기업용 알집을 사용한 경우에도 이 사건 해킹사고와 같은 수준의 해킹사고가 발생했을 것이라는 피고의 주장은 받아들이지 아니한다), ㉱ 피고가 기업용 알집을 구매하여 이를 직원들의 컴퓨터에 설치하였다면, 기업용 알집의 설치 현황이나 최신 버전 여부 등을 파악함으로써 기업용 알집의 업데이트 과정에서 변조된 파일이 위 피고의 내부망에 침입하지 않도록 더욱 쉽게 관리할 수 있었을 것인데, 직원들이 개별적으로 공개용 알집을 이용하였기 때문에, 피고로서는 그 업데이트 과정을 일일이 관리할 수가 없었으리라고 보이는 점 등에 비추어 보면, 공개용 알집이 기업용 알집보다 보안이 취약하다고 보이는바, 피고와 같은 개인정보를 취급하는 회사에서 기업용 알집이 아닌 공개용 알집을 사용한 것은 단순히 이스트소프트의 저작권을 침해한 것에 그치는 것이 아니라 나아가 위 피고가 보관하고 있는 원고를 포함한 고객들의 개인정보 유출 가능성을 한층 크게 한 것이라고 봄이 타당하다.

라) 보안강도가 낮은 개인정보 암호화 방식을 사용한 잘못

피고는 정보통신망법 제28조 제1항 제4호, 같은 법 시행령 제15조 제4항 제1호, 이 사건 고시 제6조에 따라 개인정보를 안전한 방법으로 암호화하여 저장하여야 하고, 특히 비밀번호의 경우 원래의 자료에 함수를 적용하여 얻은 결과(이러한 결과를 '해시 값'이라고 한다)를 구하는 것은 간단하지만, 해시 값에서 원래의 자료를 구하는 것은 어려운 특성이 있는 일방향 해시함수를 통해 암호화하여 안전하게 저장할 의무가 있다.

그러므로 살피건대, 갑 제4, 7, 8, 21, 24, 27, 28호증의 각 기재에 변론 전체의 취지를 종합하면, 피고는 이 사건 해킹사고 발생 당시 MD5 방식의 해시함수를 이용하여 회원들의 비밀번호를 암호화하여 저장하고 있었다.

그런데 MD5는 그 보안 강도가 다른 해시함수에 비해 낮아서 일반적으로 권고되지 않는 암호화 방법인 사실을 인정할 수 있으므로, 피고는 비밀번호 등 개인정보를 안전한 방법으로 저장할 의무를 위반하였다고 봄이 타당하다.

한편 피고의 위와 같은 의무 위반에 따른 손해배상책임의 범위와 관련하여 보건대, 설령 피고가 비밀번호를 MD5가 아닌 다른 해시함수를 이용하여 암호화하였다고 하더라도, 암호화 방식에 따라 암호를 해독하는 데 걸리는 시간이 다를 뿐 어떠한 암호화 방식을 사용했더라도 암호화된 자료를 원래의 자료대로 만드는 것이 결국에는 가능하고, 이 사건 해킹사고를 통해 암호화된 상태로 유출된 원고의 개인정보는 원래의 자료대로 노출될 가능성이 상당하다고 보이므로, 피고에게 원고의 개인정보 유출에 대한 손해배상책임을 인정하는 이상, 위 해킹사고로 유출된 원고의 개인정보가 어떠한 방식으로 암호화되어 있는지는 피고의 손해배상책임의 범위를 산정함에 있어서 크게 고려할 요소는 아니라고 보아야 할 것이다.

2) 앞서 인정한 것 외에 원고가 주장하고 있는 나머지 점들은 아래에서 보는 바와 같이 그 위반 사실을 인정하기 어렵거나 이 사건 해킹 사고와 사이의 상당인과관계를 인정하기 어려우므로 이유 없다.

가) 최소수집의무를 위반하였다는 주장에 관하여

현행 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정된 것) 제23조의2 제1항은 원칙적으로 주민등록번호의 수집·이용을 금지하고, 예외적인 경우에만 이를 수집·이용할 수 있는 것으로 개정되었는데, 이 사건 해킹 사고 당시 시행되던 정보통신망법 제23조의2 제1항에서는 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다고 규정하고 있었고, 제2항에서는 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다고 규정하고 있었다.

여기에 원고가 이 사건 해킹 사고 이전에 네이트 또는 싸이월드에 가입한 회원인 점을 더하여 보면, 적어도 이 사건 해킹 사고 이전에는 정보통신망법에 따라 회원들로부터 주민등록번호를 수집하는 것이 가능하였던 것으로 볼 수 있어, 피고가 당시 주민등록번호 없이 서비스를 제공하고 실명제를 운용하는 것이 가능하였다 하더라도, 이러한 사정만으로는 피고가 이 사건 해킹 사고 이전에 회원들로부터 주민등록번호를 수집한 것이 최소수집의무를 위반한 것이라는 원고의 주장사실을 인정하기에 부족하고, 달리 이를 인정할 증거가 없다.

나아가 피고가 원고로부터 주민등록번호 외에 전화번호, 주소, 이메일 주소 등의 개인정보를 수집하였다 하더라도, 피고가 당시 정보통신망법에 따른 개인정보 수집에 관한 의무를 위반하였다고 보기 어렵고, 달리 이를 인정할 증거가 없으므로 원고의 위 주장은 이유 없다.

나) DB 서버 관리자가 작업종료 후 로그아웃하지 않았고, 자동로그아웃 시간을 설정하지 않은 잘못으로 이 사건 해킹사고가 발생하였다는 주장에 관하여

이 사건 해킹 사고 발생 전날인 2011. 7. 25. 16:48경부터 17:29경까지 소외 1의 컴퓨터로 서버에 접속하여 업무를 수행하였는데, 작업이 종료된 이후에도 로그아웃하지 아니하였던 사실은 인정된다.

그러나 갑 제18호증, 을 제31호증, 제32호증의 각 기재만으로는 당시 피고의 DB 관리자가 내부에서 DB 서버에 접속하는 경우 두 번째 단계의 인증으로 DB 관리자의 이메일로 전송된 일회용 비밀번호(OTP)를 입력하는 구간이 존재하였다는 원고의 주장사실을 인정하기에 부족하고 달리 이를 인정할 만한 증거가 없다.

오히려 같은 증거 및 을 제48호증의 1에서 4의 각 기재에 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정, 즉 DB 서버에 접속하는 경우 이메일로 전송된 일회용 비밀번호(OTP) 입력을 통한 인증은 피고의 '외부 고객센터 소속 종사자'가 외부에서 DB 서버에 접속하는 경우에 관한 것이고, 이 사건 해커와 같이 'DB 서버 관리자 컴퓨터'를 통하여 내부에서 DB 서버에 접속하는 경우 일회용 비밀번호(OTP)를 입력하는 구간은 존재하지 않았던 점, 이 사건 해커는 2011. 7. 26. 오전 시간 동안 수차례 관리자의 아이디와 비밀번호를 새로 입력하고 로그인하였던 점 등을 종합하여 볼 때, 이 사건 해커가 관리자의 아이디와 비밀번호를 이미 파악하였던 이상, DB 서버 관리자의 로그아웃 여부와 무관하게 DB 서버에 접속할 수 있었을 것으로 보인다.

따라서 앞서 인정한 사실만으로는 이 사건 해킹 사고 발생 전날 DB 서버 관리자가 작업종료 후 로그아웃하지 않았고 이 사건 해킹 사고 발생 당시 피고가 자동로그아웃 시간을 설정하지 않았던 행위와 원고 주장과 같은 손해 발생 사이에 상당인과관계가 있는 것으로 보기에 부족하고, 달리 이를 인정할 증거가 없으므로 원고의 위 주장은 이유 없다.

다) 안전한 인증수단 적용의무를 위반하였다는 주장에 관하여

이 사건 해커는 외부에서 직접 개인정보처리시스템에 접속한 것이 아니라, 피고의 내부로 침입한 후 피고 직원 소외 1의 컴퓨터에서 개인정보처리시스템에 접속하였고, 앞서 본 바와 같이 이 사건 해킹 사고 당시 피고는 그 DB 관리자가 내부에서 개인정보처리시스템에 접속하는 경우 추가적인 인증수단을 적용하지 아니하였던 사실은 인정된다.

그러나 이 사건 고시 제4조 제4항은 "정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다"고 규정하고 있었을 뿐, 내부에서 개인정보처리시스템에 접속하는 경우 추가적인 인증수단을 적용할 의무를 규정하고 있지 않았던 점에 비추어 보면, 위 인정 사실만으로 피고가 개인정보 보호를 위한 기술적·관리적 보호조치의무를 위반하였다고 단정하기 어렵다.

라) 피고가 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하지 않음으로써 보호조치의무를 위반하였다는 주장에 관하여

살피건대, 이 사건 해커가 소외 1의 컴퓨터를 이용하여 소외 2의 아이디로 DB의 게이트웨이에 접속한 사실은 앞서 보았으나, 소외 1에게 피고의 DB 서버에 접속할 권한이 없었다고 인정할 만한 증거가 없으며, 오히려 갑 제18호증, 을 제31, 32, 제42에서 44호증의 각 기재에 변론 전체의 취지를 보태어 보면, 소외 1은 DB 기술팀 소속으로 DB 접속권한이 있었고, DB 기술팀의 직원들이 DB 서버에 접속하기 위해서는 가상 사설 네트워크인 VPN(Virtual Private Network)을 통해 먼저 게이트웨이에 접속하는데, 피고는 게이트웨이에 접속할 수 있는 IP 주소를 DB 서버에 접속할 권한이 있는 직원들이 사용하는 컴퓨터의 IP 주소로 한정시키고, DB 서버에 접속 가능한 IP 주소는 게이트웨이의 IP 주소로 한정시키는 방법으로, 허용되지 않은 IP 주소를 통해 게이트웨이나 DB 서버에 접근할 수 없도록 조처를 한 사실을 인정할 수 있으므로, 피고가 이러한 조처를 하지 않았음을 전제로 한 원고의 위 주장 또한 이유 없다.

나. 손해배상책임의 범위

1) 개인정보 유출로 그 정보주체에 위자료로 배상할 만한 정신적 손해가 발생하였는지 여부 및 그 범위는, 유출된 개인정보의 종류와 성격, 개인정보의 유출로 정보주체를 식별할 가능성이 발생하였는지, 제3자가 유출된 개인정보를 열람하였거나 열람할 가능성이 있는지, 유출된 개인정보가 어느 범위까지 확산되었는지, 개인정보의 유출로 추가적인 법익침해의 가능성이 발생하였는지, 개인정보를 처리하는 자가 개인정보를 관리해온 실태와 개인정보가 유출된 구체적인 경위는 어떠한지, 개인정보의 유출로 피해의 발생 및 확산을 방지하기 위하여 어떠한 조치가 취하여졌는지 등 여러 사정을 종합적으로 고려하여 구체적 사건에 따라 개별적으로 판단하여야 한다(대법원 2012. 12. 26. 선고 2011다60797, 60803, 60810, 60827, 60834 판결 참조).

2) 이 사건에 관하여 보건대, 앞서 인정한 사실에다가 갑 제3, 13에서 17호증, 을 제13호증의 5, 6의 각 기재에 변론 전체의 취지를 종합하여 알 수 있는 다음과 같은 사정, 즉 ① 이 사건 해킹사고로 유출된 원고의 개인정보는 성명, 주민등록번호, 아이디, 비밀번호, 주소, 전화번호 등 가장 기본적이면서 보호가 필요한 성격의 정보이고, 정보주체의 식별과 직접적으로 연결된 정보인 점, ② 특히 주민등록번호는 정부, 공공기관, 금융기관에서의 업무처리는 물론 사회적·경제적 생활과 관련된 모든 분야에서 개개인을 식별하는 가장 중요한 정보로 사용되고 있는 민감한 정보인데, 더구나 정보주체가 이를 변경할 수도 없는 영구적 정보인 점, ③ 비록 중국에 거주하는 것으로 추정되는 이 사건 해커가 원고를 비롯한 피고 회원들의 개인정보를 유출한 목적은 불분명하지만, 이 사건 해킹사고 당시는 물론 현재까지 개인정보가 상업적인 목적으로 광범위하게 수집 및 활용되고 있으며, 이를 이용한 보이스피싱(전화금융사기), 이메일을 통한 피싱, 스미싱(문자 사기), 신분 도용에 의한 금융사기 등의 범죄 목적으로도 음성적으로 거래되고 있는

점에 비추어 보면, 이 사건 해커가 위와 같이 유출한 개인정보를 제3자에게 판매하여 이익을 얻고자 하였을 가능성이 상당하고, 따라서 유출된 원고의 개인정보가 이미 광범위하게 확산·전파되었거나, 앞으로도 계속적으로 확산 및 전파될 가능성 또한 상당한 점, ④ 유출된 원고의 개인정보를 이용하여 앞서 본 바와 같은 각종 범죄가 발생할 수 있어 원고의 추가적인 법익침해의 가능성을 배제하기 어려운 점, ⑤ 피고는 원고를 포함하여 무려 34,954,887명에 이르는 대규모 개인정보를 수집하고 있었음에도, 앞서 본 바와 같이 침입탐지시스템 등을 제대로 갖추지 아니하여 대용량의 개인정보가 파일로 생성되고 외부로 유출되는 것을 탐지하지 못하고, 개인정보 접근권한이 있는 컴퓨터에서 보안상 취약한 공개용 알집을 사용하고 FTP 서비스를 제공하는 것을 방치하는 등 여러 면에서 개인정보를 보호할 의무를 소홀히 하여 이 사건 해킹사고를 방지하지 못한 점, ⑥ 나아가 피고는 위에서 본 바와 같이 이 사건 해킹사고가 발생하고 이틀이 지난 2011. 7. 28. 비로소 이 사건 해킹 사고로 유출된 자료가 회원들의 개인정보임을 확인하였고, 이를 확인한 후에도 단지 네이트와 싸이월드 홈페이지를 통해 회원들의 개인정보가 유출된 사실을 공지하였을 뿐, 원고를 비롯한 회원 개개인에게 직접 사고발생 사실과 사고의 내용 및 어떤 정보가 유출된 것인지 정확하게 알리거나 회원들이 이를 바로 확인할 수 있도록 하는 충분한 조처를 하였다고 보이지 않는 점, ⑦ 이 사건 해킹사고 이후 원고는 유출된 자신의 개인정보가 거래되거나 전파되고 있을 수 있다는 불쾌감은 물론 주민등록번호를 대체할 다른 개인식별 수단이 마련되지 않는 이상, 앞으로도 계속적으로 신분도용 등에 따른 추가 피해 발생에 대한 불안감 등의 심리적·정신적 고통을 겪어야 하는 점 등에다가 피고가 개인정보를 수집한 목적, 이를 수집한 방법 및 경위, 피고의 경제적 지위, 대규모 개인정보를 수집 및 보유하고 있던 정보통신서비스 제공자로서의 피고의 사회적 책임, 원고의 나이, 직업 등 이 사건 변론에 나타나 제반 사정을 종합적으로 고려해보면, 피고는 이 사건 해킹사고로 원고가 입은 정신적 손해를 배상할 의무가 있고, 위자료의 액수는 1,000,000원으로 정함이 타당하다.

4. 결론

그렇다면 피고는 원고에게 1,000,000원 및 이에 대하여 이 사건 해킹사고가 발생한 2011. 7. 26.부터 피고가 이행의무의 존재 여부나 범위에 관하여 항쟁하는 것이 타당하다고 인정되는 제1심판결 선고일인 2012. 4. 26.까지는 민법이 정한 연 5%, 그 다음 날부터 다 갚는 날까지는 소송촉진 등에 관한 특례법이 정한 연 20%의 각 비율로 계산한 지연손해금을 지급할 의무가 있다 할 것인바, 원고의 청구는 위 인정 범위 내에서 이유 있어 인용하고 나머지는 이유 없어 이를 기각할 것인데, 제1심판결은 이와 결론을 같이하여 정당하므로 원고와 피고의 항소는 이유 없어 이를 모두 기각하기로 하여 주문과 같이 판결한다.

[[별 지] 관련 법령: 생략]

판사 김현환(재판장) 이성 전명환