서 울 서 부 지 방 법 원

제 12 민 사 부

판 결

사 건	2011가합11733 손해배상(기) 2011가합13234(병합) 손해배상(기) 2011가합14138(병합) 손해배상(기) 2012가합1122(병합) 손해배상(기)
원고(선정당사자)	김** 등 2882명
피 고	1. 에스케이커뮤니케이션즈 주식회사 2. 주식회사 이스트소프트 3. 시만텍코리아 주식회사 4. 주식회사 안랩
변 론 종 결	2013. 1. 23.
판 결 선 고	2013. 2. 15.

주 문

1. 피고 에스케이커뮤니케이션즈 주식회사는 원고(선정당사자)들 및 별지1. 선정자목록 기재 선정자들에게 각 200,000원 및 이에 대한 2011. 7. 26.부터 2013. 2. 15.까지는 연 5%의, 그 다음날부터 다 갚는 날까지는 연 20%의 각 비율에 의한 금원을 지급

하라.

2. 원고(선정당사자)들의 피고 에스케이커뮤니케이션즈 주식회사에 대한 나머지 청구 및 피고 주식회사 이스트소프트, 시만텍코리아 주식회사, 주식회사 안랩에 대한 각 청구를 모두 기각한다.

3. 소송비용 중 원고(선정당사자)들과 피고 에스케이커뮤니케이션즈 주식회사 사이에 생긴 부분의 4/5는 원고(선정당사자)들이, 나머지는 위 피고가 각 부담하고, 원고(선정당사자)들과 피고 주식회사 이스트소프트, 시만텍코리아 주식회사, 주식회사 안랩 사이에 생긴 부분은 원고(선정당사자)들이 부담한다.

4. 제1항은 가집행할 수 있다.

청 구 취 지

피고들은 각자 원고(선정당사자)들 및 별지1. 선정자목록 기재 선정자들{이하 원고(선정당사자)들과 선정자들을 합하여 '원고들'이라고만 한다}에게 각 1,000,000원 및 이에 대한 2011. 7. 26.부터 이 사건 소장 송달일까지는 연 5%의, 그 다음날부터 다 갚는 날까지는 연 20%의 각 비율에 의한 금원을 지급하라.

이 유

1. 기초사실

가. 당사자의 지위

1) 피고 에스케이커뮤니케이션즈 주식회사(이하 '피고 SK컴즈'라 한다)는 인터넷상에서 검색, 커뮤니티 등을 기반으로 각종 정보를 제공하는 포털서비스사업을 하는 회

사로, 네이트(NATE)[1], 네이트온(NateON)[2], 싸이월드(CYWORLD)[3]와 같은 온라인 서비스를 제공하고 있다.

2) 피고 주식회사 이스트소프트(이하 '피고 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.

3) 피고 시만텍코리아 주식회사(이하 '피고 시만텍'이라 한다)는 소프트웨어 개발, 판매 및 기술 지원업 등을 하는 회사로, 피고 SK컴즈에게 컴퓨터 바이러스와 악성 코드 등을 감지하고 제거하는 백신 프로그램인 시만텍 엔드포인트 프로텍션 버전 11(Symantec Endpoint Protection v.11)을 판매하고, 위 백신 프로그램의 업데이트를 제공하고 있다.

4) 피고 주식회사 안랩(이하 '피고 안랩'이라 한다)은 컴퓨터 바이러스의 연구 및 백신프로그램의 제조 및 개발, 보안솔루션 제공업 등을 하는 회사로 피고 SK컴즈와 사이에 보완관제서비스 용역계약을 체결하고, 이에 따라 피고 SK컴즈를 위하여 침입탐지시스템(Intrusion Detection System) 및 침입방지시스템(Intrusion Prevention System)의 운영·관리 등 보완관제 업무를 수행하고 있다.

5) 원고들은 뒤에서 살펴볼 해킹사고가 발생하기 전 피고 SK컴즈가 제공하는 네이트와 싸이월드의 한쪽 또는 양쪽 서비스에 가입한 사람들로, 가입 당시 피고 SK컴즈에 성명, 주민등록번호, 아이디(ID), 비밀번호, 이메일 주소, 주소, 전화번호 등 개인정보를

---

1) 네이트는 검색, 뉴스, 이메일, UCC(User Created Contents) 공유 서비스, 만화 등을 제공하는 포털사이트이다.
2) 네이트에서 제공하는 인스턴트 메신저(Instant Messenger)이다.
3) 싸이월드는 인터넷을 기반으로 한 소셜 네트워크 서비스(Social Network Service)로, 싸이월드의 이용자들은 각자 홈페이지(미니홈피)를 운영하면서 글이나 사진을 게시하고, 배경음악을 설정하며, 방명록 등을 통해 다른 이용자와 소통할 수 있고, 공동의 커뮤니티 홈페이지(싸이월드 클럽)를 통해 서로의 관심사와 개성을 공유할 수 있다.

제공하였다(원고들이 네이트나 싸이월드의 서비스에 가입할 당시 필수적으로 위와 같은 정보를 제공하여야 했고, 그 외에 선택적으로 혈액형과 닉네임 등의 정보를 제공할 수 있었는데, 원고들 중 선택적 정보를 제공한 자가 있음을 인정할 자료가 없으므로, 원고들 모두 필수적 정보만을 제공한 것으로 본다).

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 피고 SK컴즈 DB기술팀 직원인 김차영의 컴퓨터에 윈도우 예약작업을 이용하여, 이 사건 해커가 미리 설정해놓은 임의의 도메인인 'nateon.duamlive.com'에 역접속을 시도하는 기능을 가진 악성프로그램인 'nateon.exe'를 유포하고, 2011. 7. 26.부터 2011. 7. 27.까지 중국 내 불상지에서 자신의 컴퓨터로 김차영의 컴퓨터에 원격접속하여 피고 SK컴즈 정보통신망에 침입하였으며, 네이트 회원정보가 저장되어 있는 데이터베이스 서버, 싸이월드 회원정보가 저장되어 있는 데이터베이스 서버, 네이트와 싸이월드에 모두 가입한 중복 회원정보가 저장되어 있는 데이터베이스 서버에 침입하여 위 각 서버에서 처리, 보관하고 있는 개인정보를 아이피 주소 '211.115.112.36'이 할당된 컴퓨터인 에듀티에스 서버(www.eduts.co.kr)로 전송(이하 '이 사건 해킹사고'라 한다)하였다.

2) 이 사건 해킹사고로 인해 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) 피고 SK컴즈는 2011. 7. 28. 이 사건 해킹사고를 경찰과 방송통신위원회에 신고하였고, 네이트와 싸이월드 회원들에게 위 해킹사고로 인한 개인정보 유출 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) 피고 이스트소프트는 파일 압축 프로그램인 알집을 국내 공개용, 국내 기업용, 공공기관용, 교육기관용, PC방용, 해외용 등으로 구분하여 공급하고 있는데, 그 중 공개용 알집은 기업용 등 다른 알집과 달리 무료로 배포하는 대신 공개용 알집을 실행시 프로그램 창의 상단에 광고가 게시되도록 하여 수익을 얻고 있고, 공개용 알집에는 위와 같이 광고가 게시될 수 있도록 광고 콘텐츠 서버로부터 광고 내용을 불러와서 이를 실행하는 역할을 하는 ALAD.dll이라는 파일이 포함되어 있어서, 공개용 알집을 최초로 설치하거나 업데이트하는 경우 위 ALAD.dll 파일이 피고 이스트소프트의 알집 업데이트 서버로부터 사용자의 컴퓨터에 다운로드된다.

나) 이 사건 해커는 정상적인 ALAD.dll 파일이 아닌, 동일한 이름의 악성 프로그램인 ALAD.dll 파일을 만들었고, 이를 공개용 알집의 사용자 컴퓨터에 설치하기 위해 다음과 같이 피고 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 필터[4]에 stmpxml.dll 파일을

4) ISAPI 필터는 인터넷 정보 서버의 앞단에 위치하면서 인터넷 정보 서버로 들어온 모든 요청에 대해 가장 먼저 처리할 권한과 인터넷 정보 서버가 생성한 응답을 클라이언트에 보내주기 전에 가공할 수 있는 권한을 가진다.

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 SK컴즈, 엔에이치엔 주식회사(포털사이트인 네이버 등을 운영하는 회사, 이하 'NHN'이라 한다) 등 선별된 IP 주소에서 사용되는 컴퓨터가 알집 업데이트를 요청하는 경우, 피고 이스트소프트가 설정한 본래의 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 다운로드 받게 된다. 악성 ALAD.dll 파일이 다운로드되면, 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 피고 SK컴즈의 컴퓨터가 알집 업데이트 과정에서 'http://inexon.softforum.org'에서 악성 ALAD.dll 파일을 다운로드 받았고, 같은 달 20. 14:59경 피고 SK컴즈 직원 김차영의 컴퓨터에 nateon.exe 파일이 생성되어 같은 달 21. 02:02경 nateon.exe에 감염되었으며, 같은 달 23. 13:09경 김차영의 컴퓨터에서 update.exe 파일과 windowsrpc.dll 파일이 실행되었다.

바) 이 사건 해커는 2011. 7. 26. 02:07경 김차영의 컴퓨터를 경유하여 이용석의 DB 관리자 아이디로 게이트웨이[5]에 접속하였다.

사) 이 사건 해커는 피고 SK컴즈의 DB 서버에 침입하여 개인정보를 덤프(dump)[6] 파일로 생성하여 압축한 다음, 이를 게이트웨이에 내려받고, 파일을 송수신하는 통신규

---

5) 게이트웨이란 하나의 네트워크에서 다른 네트워크로 이동하기 위해 거쳐야 하는 관문이다. 두 컴퓨터가 네트워크 상에서 연결되려면 동일한 통신규약, 즉 동일한 프로토콜을 사용해야 하므로, 프로토콜이 다른 네트워크 상의 컴퓨터와 통신하는 경우 게이트웨이가 프로토콜 변환기 역할을 한다.

6) 저장매체로부터 다른 저장매체나 프린터, 화면, 기타 출력장치로 대량의 복사를 수행하는 것을 뜻한다.

약인 FTP(File Transfer Protocol)를 이용하여 위 개인정보 파일을 게이트웨이에서 김차영 또는 이용석의 컴퓨터로 내려받은 후 대한민국 내 경유지인 에듀티에스 사이트를 경유하여 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 김차영의 컴퓨터에서 내려받았고, 06:33경 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 김차영의 컴퓨터에서 내려받았고, 06:32경 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 중복 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 27. 01:13경 게이트웨이 서버에 저장된 'C:₩temp₩pits.dmp.bz2' 파일을 FTP 방식으로 이용석의 컴퓨터에서 내려받았고, 01:30경 위 파일을 다시 FTP 방식으로 에듀티에스 사이트로 전송하였으며, 06:30경 에듀티에스 사이트에서 중국으로 위 파일을 전송하였다.

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

라. 관련 법령

정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것, 이하 '정보통신망법'이라 한다), 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 별지2. 관련 법령 기재와 같다.

[인정근거] 다툼 없는 사실, 갑 제1, 3, 43호증, 을가 제17, 18, 24, 25, 36, 42호증(가지번호 있는 호증은 가지번호를 포함한다, 이하 같다)의 각 기재, 변론 전체의 취지

2. 피고 SK컴즈에 대한 청구에 관한 판단

가. 손해배상책임의 발생

1) 피고 SK컴즈는 정보통신서비스 제공자로서 정보통신망법 및 같은 법 시행령 등에 따라 위 피고가 운영하는 네이트 또는 싸이월드의 회원인 원고들이 회원 가입시 제공한 성명, 주민등록번호, 아이디, 비밀번호 등의 개인정보를 보호할 의무가 있음에도, 다음과 같이 이러한 의무를 위반하여 이 사건 해킹사고를 방지하지 못하고, 그로 인하여 원고들의 개인정보가 유출되도록 하였으므로 정보통신망법 제32조에 따라 원고들에게 개인정보 유출에 따른 손해배상을 할 의무가 있다(또한 피고 SK컴즈는 네이트와 싸이월드의 서비스 이용약관에 따라 원고들의 개인정보를 보호하기 위한 보안시스템을 구축하고, 개인정보를 취급함에 있어 안전성 확보에 필요한 기술적 및 관리적 대책을 수립·운영할 계약상 의무가 있음에도 다음과 같이 이러한 의무를 위반하여 이 사건 해킹사고를 방지하지 못하고, 그로 인하여 원고들의 개인정보가 유출되도록 하였으므로, 채무불이행에 따른 손해배상 책임도 부담한다).

가) 대용량 개인정보의 유출을 탐지하지 못한 점에 관하여

갑 제43호증, 을가 제9, 17, 36, 42호증의 각 기재, 증인 이**의 증언 및 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정에 비추어 보면, 피고 SK컴즈는 정보통신망법 제28조 제1항, 같은 법 시행령 제15조, 이 사건 고시 제8조에 위반하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입탐지시스템 및 침입방지시스템(이하 '침입탐지시스템 등'이라고 한다)을 적절히 운영하지 못하고, 개인정보의 출력·복사

시 필요한 보호조치를 갖추지 못한 잘못으로 이 사건 해커가 개인정보 DB에 접속하여 원고들을 포함한 34,954,887명의 개인정보를 덤프 파일로 생성하고(이는 이 사건 고시 제8조의 '출력'에 해당한다), 이를 게이트웨이, 김차영 또는 이용석의 컴퓨터, 에듀티에스 사이트 등을 거쳐서 중국으로 유출하는 것을 탐지하지 못하였다고 봄이 상당하다.

① 피고 SK컴즈는 개인정보에 대한 불법적인 접근 및 유출을 차단하기 위하여 침입탐지시스템 등을 갖춤으로써 개인정보가 보관된 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 실시간으로 모니터링하고, 통상적으로 수행되는 업무와 다른 형태의 업무가 수행되거나 비정상적인 트래픽(특정 전송로상에서 일정 시간내에 흐르는 데이터의 양)이 발생할 경우 이를 탐지하여 DB 관리자에게 즉시 경고함으로써 DB 관리자가 이에 대한 조치를 취할 수 있도록 하는 시스템을 갖출 의무가 있고, 실제로 피고 SK컴즈는 앞서 본 바와 같이 피고 안랩과 보완관제서비스 용역계약을 체결하여 피고 안랩으로 하여금 피고 SK컴즈의 개인정보 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 실시간으로 모니터링하도록 하고 있었다.

② 다만 개인정보 DB의 접속내역 및 DB에 접속하여 수행하는 업무내역을 실시간으로 모니터링하면서 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 없다.

③ 이 사건 해킹사고의 발생 당시 피고 SK컴즈의 침입탐지시스템 등이 DB 관

리자에게 경고하지 않았다는 것은 이 사건 해커가 수행한 업무 내역이나 그 과정에서 발생한 트래픽이 피고 SK컴즈가 설정한 경고 발생의 기준에 따를 때 이상 징후로 판단되지 못하였다는 것을 의미하는바, 다음과 같은 사정, 즉 ㉮ 이 사건 해킹사고로 인해 피고 SK컴즈의 내부망에서 총 34,954,887명의 개인정보가 2G, 2G, 6G 등 총 10G의 크기로 외부로 유출되었는데, 피고 SK컴즈는 당시 기밀 또는 중요 정보에 대한 유출을 차단하기 위한 DLP(Data Loss Prevention) 솔루션[7]을 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 피고 SK컴즈의 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, 피고 SK컴즈가 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 조회를 하는 방법으로 대부분의 업무를 처리할 수 있으리라고 보이므로, 이 사건 해커가 exp 명령어를 사용하여 개인정보를 파일로 생성하여 출력하였다는 것은 그 자체로 특이한 업무수행 내역이라고 볼 수 있는데도 피고 SK컴즈

7) DLP란 기밀 또는 중요 정보의 유출을 차단 및 예방하는 활동을 말하며, 이를 하드웨어 또는 소프트웨어로 구현한 것을 DLP 솔루션이라 통칭한다. DLP 솔루션이 갖추어야 할 필수 기능은 특정 정보가 유출되는 일련의 과정을 모니터링하고 이를 선별적으로 차단하는 것인데, 키워드(극비, 기밀 등의 중요 단어)나 특정 패턴(주민등록번호, 핸드폰번호, 신용카드번호, 계좌번호 등)을 통해 정보를 식별할 수 있다.

의 침입탐지시스템 등에서는 이를 이상 징후로 감지하지 못한 점(이미 이 사건 해킹사고 이전에 피고 SK컴즈와 같은 정보통신서비스 제공자가 보관하는 대량의 개인정보가 유출되는 사고가 있었으므로, 피고 SK컴즈로서는 개인정보 보호의무의 일환으로 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 개인정보의 출력이 있을 경우 침입탐지시스템 등에서 이를 이상 징후로 감지하도록 하여, 실제로 정당한 접속권한을 가진 사람이 업무 수행의 일환으로 이러한 작업을 하는 것인지를 확인할 수 있도록 하는 등의 적절한 보안조치를 취했어야 할 것으로 보이는데, 이러한 보안조치를 취하고 있지 않았던 것으로 보인다), ㉰ 나아가 이 사건 해커가 이틀에 걸쳐서 대용량의 개인정보 파일을 DB 서버에서 게이트웨이로 내려받고, FTP 방식으로 위 파일을 게이트웨이에서 김차영 또는 이용석의 컴퓨터를 거쳐 결국 외부망인 에듀티에스 사이트에까지 전송하는 동안에도 이를 전혀 탐지하지 못했다는 것은 개인정보가 대량으로 전송되는 것을 이상 징후로 감지하는 기준이 설정되지 않은 상태였다고 볼 수밖에 없는 점(특히 개인정보가 내부망을 벗어나 외부로 전송되는 것은 더욱 철저히 탐지했어야 한다고 보인다) 등을 종합하면, 피고 SK컴즈가 설정한 경고 발생의 기준이 지나치게 완화되어 있어서 개인정보를 보호하기에 매우 부족한 수준이었고, 그로 인하여 이 사건 해킹사고를 탐지하지 못하였다고 봄이 상당하다.

(다만 원고들은 피고 SK컴즈가 개인정보의 출력·복사시 개인정보관리책임자의 사전승인을 받도록 조치했어야 하는데, 이러한 조치를 하지 않은 잘못이 있다고 주장하면서 그 근거로 2009. 8. 7.자 방송통신위원회 고시 제2009-21호 개인정보의 기술적·관리적 보호조치 기준 제8조[8]에 위와 같은 사전승인 의무가 규정되어 있다는 점

을 들고 있으나, 위 규정은 이 사건 고시로 개정되어서 이 사건 해킹사고 당시에는 효력이 없었을 뿐만 아니라, 개정 전 고시에 의할 때에도 개인정보를 종이로 인쇄하거나 디스켓 등 이동 가능한 저장매체에 복사할 경우에 사전승인을 받도록 규정되어 있으므로 이 사건 해킹사고와 같이 종이나 이동 가능한 저장매체를 이용하지 않은 경우에 그대로 적용된다고 보기도 어려우므로, 원고들의 위 주장은 이유 없다)

나) 피고 SK컴즈의 직원 컴퓨터에서 공개용 알집을 사용한 점에 관하여

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

피고 이스트소프트의 라이센스 정책에 의하면, 공개용 알집은 개인이 가정에서 사용하는 용도로만 무료로 제공되며, 피고 SK컴즈와 같은 기업에서는 기업용 알집을 유료로 구매 또는 대여하여 사용하여야 함에도, 이 사건 해킹사고 당시 피고 SK컴즈의 직원들이 공개용 알집을 사용한 사실은 당사자들 사이에 다툼이 없으므로, 피고 SK컴즈는 직원들이 위와 같이 공개용 알집을 사용하는 것을 방지하지 못한 잘못으로 피고 이스트소프트의 알집 저작권을 침해하였다고 볼 수 있고, 나아가 갑 제3, 47 내지 49호증, 을가 제42호증의 각 기재, 증인 이성관의 증언 및 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정을 종합하면, 피고 SK컴즈가 직원들의 공개용 알집을 사용하는 것을 방지하지 못한 잘못과 이 사건 해킹사고 발생 사이에 상당인과관계

---

8) **개인정보의 기술적·관리적 보호조치 기준(2009. 8. 7.자 방송통신위원회 고시 제2009-21호)**
제8조(출력·복사시 보호조치)
② 정보통신서비스 제공자 등은 개인정보취급자가 개인정보를 종이로 인쇄하거나, 디스켓, 콤팩트디스크 등 이동 가능한 저장매체에 복사할 경우 다음 각 호의 사항을 기록하고 개인정보관리책임자의 사전승인을 받도록 조치한다. 출력·복사물로부터 다시 출력 또는 복사하는 경우도 또한 같다.

를 인정할 수 있다.

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

② 공개용 알집이 아닌 기업용 등 다른 유료 알집의 업데이트 과정에서 악성 ALAD.dll 파일을 내려받은 내역이 발견된 바가 없다는 점에서도, 이 사건 해커가 해킹의 대상으로 삼은 컴퓨터는 공개용 알집을 사용하는 컴퓨터라는 사실을 알 수 있다(피고 이스트소프트는 이 사건 해킹사고 발생 후 공개용 알집 업데이트 프로그램의 보안상 취약점을 인정하여 이를 공지한 바도 있다).

③ 비록 공개용 알집과 기업용 알집의 업데이트서버가 동일하다고 보이기는 하지만(원고들은 업데이트 서버가 분리되어 있다고 주장하나, 갑 제47호증, 을가 제42호증의 각 기재만으로는 이를 인정하기 부족하고, 달리 이를 인정할 증거가 없으므로, 원고들의 위 주장은 받아들이지 아니한다), 다음과 같은 사정, 즉 ㉮ 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 뿐이어서, 실시간으로 상호통신이 이루어지거나 다량의 패킷이 발생하지 않으므로, 공개용 알집과 같

이 실시간으로 외부 서버와 연결되어 있는 프로그램을 이용하는 것이 일반적으로 외부 서버와 연결이 끊어져 있는 프로그램을 이용하는 것보다 보다 용이하게 해킹의 대상이 되리라고 보이는 점, ㉯ 비록 공개용 알집이 실시간으로 알집 서버에 연결되어 있는 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 동일한 수준의 해킹사고가 발생했을 것이라는 피고 SK컴즈의 주장은 받아들이지 아니한다), ㉰ 피고 SK컴즈가 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 보다 용이하게 관리할 수 있었을 것인데, 직원들이 개별적으로 공개용 알집을 이용하였기 때문에, 피고 SK컴즈로서는 그 업데이트 과정을 일일이 관리할 수가 없었으리라고 보이는 점 등에 비추어 보면, 공개용 알집이 기업용 알집보다 보안이 취약하다고 보이는바, 피고 SK컴즈와 같은 개인정보를 취급하는 회사에서 기업용 알집이 아닌 공개용 알집을 사용한 것은 단순히 피고 이스트소프트의 저작권을 침해한 것에서 나아가 위 피고가 보관하고 있는 원고들의 개인정보의 유출 가능성을 한층 크게 한 것이다.

다) FTP 서비스를 제공한 점에 관하여

피고 SK컴즈의 DB에서 유출된 개인정보 파일이 FTP 방식으로 게이트웨이에

서 김차영 또는 이용석의 컴퓨터를 거쳐서 에듀티에스 사이트로 전송된 사실은 앞서 본 바와 같고, 을가 제5호증의 기재, 증인 이성관의 증언 및 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정, 즉 ① FTP는 파일 전송을 위한 프로토콜로 대량의 파일을 쉽게 송수신하는 역할을 수행하는 만큼 일반적으로 보안상 취약하다고 여겨지고 있는 점, ② 피고 SK컴즈 또한 FTP의 이러한 취약점을 인지하고 내부적으로 만든 개인정보보호 업무지침 제26조에서 "개인정보 접근 권한이 있는 컴퓨터에 FTP 서비스 등 보안상 취약한 서비스는 제공하지 않도록 한다"고 규정하고 있는 점(피고 SK컴즈는 위 규정은 개인정보에 접근 권한이 있는 컴퓨터가 FTP 서버로 사용되는 것을 제한하는 의미일 뿐, FTP 클라이언트로 사용되는 것을 제한하는 의미는 아니라고 주장하나, 위 규정의 문언 자체에 비추어 볼 때 위 피고가 주장하는 바와 같이 FTP 서버로 제공되는 경우만 제한하여 규정하고 있다고 보기 어렵고, FTP 클라이언트로 사용되는 컴퓨터에서도 파일의 대량 수신뿐만 아니라 송신도 가능하기 때문에, 보안상 문제가 발생할 수 있는 것은 마찬가지이다), ③ 윈도우(Windows), 리눅스(Linux), 맥(Mac OS) 등 컴퓨터 운영체제에 기본적으로 FTP 기능이 포함된다고 하더라도 정보통신망법 제45조에 따라 제정된 정보보호조치 및 안전진단 방법·절차·수수료에 관한 지침(2010. 02. 03. 자 방송통신위원회 고시 제2010-3호) 제2조 별표1 2.2.8.(위 규정의 내용은 별지2. 관련 법령 기재와 같다)에 따르면 피고 SK컴즈는 정보통신망의 안정성 등을 확보하기 위해 게이트웨이에서 불필요한 FTP를 제거할 의무가 있는데, 이러한 의무를 이행하지 않은 점(피고 SK컴즈는 게이트웨이에서 FTP 기능을 이용할 필요가 있었다고 주장하나, 이를 인정할 증거가 없다) 등을 종합하면, 피고 SK컴즈는 보안상 취약한 FTP가 게이트웨이 및 개인정보 접근권한이 있는 컴퓨터에서 기능하도록 방치함으로써, 이 사건

해커가 FTP 방식으로 개인정보가 대량으로 외부에 유출되도록 하는 데에 기여하였다고 봄이 상당하다.

라) 로그아웃을 하지 않고, 자동 로그아웃 시간을 설정하지 않은 점에 관하여

갑 제43 내지 45호증, 을가 제42호증의 각 기재 및 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사실, 즉 ① 이 사건 고시 제4조 제4항은 정보통신서비스 제공자 등은 개인정보 DB에 접속할 권한이 있는 자가 정보통신망을 통해 외부에서 DB에 접속이 필요한 경우 공인인증서 등 안전한 인증 수단을 적용하도록 규정하고 있는데, 이는 키로깅 등의 방법으로 DB 관리자의 아이디나 비밀번호가 유출될 경우를 대비하여 추가적인 인증 수단을 적용하여야 한다는 취지의 규정인 점, ② 피고 SK컴즈는 추가적인 인증 수단으로서 일회용 비밀번호인 OTP(One Time Password)를 이용하고 있기 때문에, DB 관리자의 아이디와 비밀번호로 로그인을 하면, DB 관리자의 이메일로 OTP 번호가 발송되고, 이를 입력하여야만 DB 서버에 접속이 가능하며, 일단 로그아웃을 하면 DB 관리자가 새롭게 OTP 번호를 받지 않아서 이를 입력하지 않는 이상 DB 관리자의 아이디와 비밀번호만으로는 DB 서버에 접속할 수 없는 점, ③ 피고 SK컴즈의 DB 접속기록에 비추어 보면 이 사건 해킹사고가 발생하기 전날인 2011. 7. 25. 16:48경부터 17:29경까지 DB 관리자가 자신의 아이디와 비밀번호 및 OTP 번호를 받아서 DB 서버에 접속하여 업무를 수행하였고, 이 사건 해커는 그로부터 약 7시간이 경과한 후인 같은 달 26. 02:20경부터 DB 서버에 접속하여 이 사건 해킹사고를 발생한 사실, ④ 이 사건 해커는 앞서 본 키로깅 프로그램인 Nateon.dll을 통해 DB 관리자의 아이디나 비밀번호를 알아낼 수는 있으나, 이러한 방법으로는 일회용 비밀번호인 OTP를 알 수가 없는 사실 등을 종합하면, 피고 SK컴즈의 DB 관리자가 DB 서버에 접

속하여 업무를 수행한 후 로그아웃을 하지 않았고, 일정 시간 이상 작업을 수행하지 않으면 자동으로 로그아웃이 되는 아이들 타임(idle time)이나 접속 가능한 최대시간인 커넥트 타임(connect time)도 설정되어 있지 않았기 때문에 로그인이 된 상태로 계속 남아있었으며, 이를 이용하여 이 사건 해커가 OTP 번호를 새로 받지 않고도 DB 서버에 접근할 수 있었던 것으로 봄이 상당하므로, 피고 SK컴즈의 직원이 업무수행 후 로그아웃을 하지 않은 과실과 위 피고가 아이들 타임이나 커넥트 타임을 적절히 설정하지 않은 과실이 결합하여 이 사건 해킹사고가 발생한 원인 중 하나가 되었다고 보아야 할 것이다.

이에 대하여 피고 SK컴즈는 포털사이트의 특성상 장시간이 소요되는 작업이 많아서 업무시간 중에 작업 명령을 내리고 로그아웃을 하지 않고 퇴근하여야 할 필요가 있으며, DB 관리자의 컴퓨터는 일정 시간 이상 작업을 하지 않으면 자동으로 잠김 상태로 전환되도록 설정되어 있다고 주장하나, 이 사건 해킹사고가 발생하기 전날 DB 관리자가 자신의 컴퓨터를 새벽까지 로그아웃을 하지 않은 상태로 두고 퇴근했어야 할 필요가 있었다고 인정할만한 자료가 없고, DB 관리자의 컴퓨터가 일정 시간 작업을 하지 않으면 자동 잠김 상태로 전환되도록 설정되어 있어서 로그아웃을 한 것과 같은 효과가 발생한다고 인정할만한 자료도 없으므로, 위 피고의 주장은 받아들이지 아니한다.

마) 개인정보 암호화 방식에 관하여

피고 SK컴즈는 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 '해쉬값'이라고 한다)를 구하는 것은 간단하지만, 해쉬값에서 원래의 자료를 구

하는 것은 어려운 특성을 가지는 일방향 해쉬함수를 통해 암호화하여 안전하게 저장할 의무가 있는데, 갑 제4, 19, 21, 43호증의 각 기재, 증인 이성관의 증언 및 변론 전체의 취지를 종합하면, 피고 SK컴즈는 이 사건 해킹사고 발생 당시 MD5 방식의 해쉬함수를 이용하여 회원들의 비밀번호를 암호화하여 저장하고 있었는데, MD5는 그 보안 강도가 다른 해쉬함수에 비해 낮아서 일반적으로 권고되지 않는 암호화 방법인 사실을 인정할 수 있으므로, 피고 SK컴즈는 비밀번호 등 개인정보를 안전한 방법으로 저장할 의무를 위반하였다고 봄이 상당하며, 설령 피고 SK컴즈가 비밀번호를 MD5가 아닌 다른 해쉬함수를 이용하여 암호화하였다고 하더라도, 암호화 방식에 따라 암호를 해독하는데 소요되는 시간이 다를 뿐 어떠한 암호화 방식을 사용했더라도 암호화된 자료를 원래의 자료대로 만드는 것이 결국에는 가능하기 때문에, 이 사건 해킹사고를 통해 암호화된 상태로 유출된 원고들의 개인정보는 원래의 자료대로 노출될 가능성이 상당하므로, 앞서 본 바와 같이 피고 SK컴즈의 개인정보 보호의무 위반으로 인해 이 사건 해킹사고가 발생하였다고 봄이 상당하고, 따라서 피고 SK컴즈에게 원고들의 개인정보 유출에 대한 손해배상책임을 인정하는 이상, 위 해킹사고로 인해 유출된 원고들의 개인정보가 어떠한 방식으로 암호화되어 있는지 여부는 피고 SK컴즈의 손해배상책임의 범위를 산정하는데 있어서 크게 고려할 요소는 아니라고 보아야 할 것이다.

2) 원고들은 앞서 인정한 것 외에도 피고 SK컴즈가 다음과 같이 개인정보를 보호할 의무를 위반한 잘못도 있다고 주장하나, 이는 다음과 같이 모두 이유 없다.

가) 원고들은, 피고 SK컴즈가 네이트나 싸이월드에 가입하기 위해 필수적으로 성명, 주민등록번호, 아이디(ID), 비밀번호, 이메일 주소, 주소, 전화번호 등의 개인정보를 제공하도록 함으로써, 정보통신망법 제23조 제2항을 위반하여 필요한 최소한의 정

보 외의 개인정보를 수집하고, 이러한 개인정보의 제공을 강요한 잘못이 있다고 주장한다.

살피건대, 피고 SK컴즈가 네이트나 싸이월드에 가입하기 위해 필수적으로 성명, 주민등록번호, 아이디(ID), 비밀번호, 이메일 주소, 주소, 전화번호 등의 개인정보를 제공하도록 한 사실은 앞서 본 바와 같으나, 이러한 개인정보 중 어떠한 개인정보가 정보통신망법 제23조 제2항에서 정한 필요한 최소한의 정보에 해당하는지가 불분명하고(원고들은 개인정보보호법 제16조 제1항[9]을 근거로 필요한 최소한의 개인정보 수집이라는 입증책임은 피고 SK컴즈가 부담한다고 주장하나, 위 법은 2011. 3. 29. 제정되어 부칙 제1조에 따라 이 사건 해킹사고 발생 후인 같은 해 9. 29.부터 시행되며, 위 법이 위 해킹사고 발생 전으로 소급하여 적용된다고 볼만한 사정도 없으므로, 원고들의 위 주장은 받아들이지 아니한다), 을가 제4, 7호증의 각 기재 및 변론 전체의 취지를 종합하면, 이 사건 해킹사고 발생 당시 시행되고 있던 정보통신망법 제23조의2 제1항에서는 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 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 있었으므로, 당시에는 정보통신망법에 따라 정보통신서비스 제공자가 서비스 이용자들

---

9) **개인정보보호법**
제16조(개인정보의 수집 제한)
① 개인정보처리자는 제15조 제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
부칙 <제10465호, 2011. 3. 29>
제1조(시행일)
이 법은 공포 후 6개월이 경과한 날부터 시행한다.

로부터 주민등록번호를 수집하는 것이 가능하였고,[10] 실제로 대부분의 정보통신망서비스 제공자들이 주민등록번호를 수집하고 있었다고 보이며, 피고 SK컴즈는 위 규정에 따라 인터넷에서 주민번호를 대체하기 위해 사용되는 개인 식별 번호인 I-PIN(Internet Personal Identification Nimber)을 통해 주민등록번호를 사용하지 않고도 네이트나 싸이월드에 가입할 수 있는 방법을 제공하고 있었으므로, 피고 SK컴즈가 정보통신망법 제23조 제2항을 위반하여 필요한 최소한의 정보 외의 개인정보를 수집하고, 이러한 개인정보의 제공을 강요한 잘못이 있다는 원고들의 주장은 이유 없다.

나) 원고들은, 피고 SK컴즈의 직원 중 네이트나 싸이월드의 회원 개인정보를 보관한 DB에 접속할 권한은 이용석과 김도영만 가지고 있으므로, 위 두 사람이 사용하는 컴퓨터 외의 컴퓨터에서는 DB에 접근할 수 없도록 IP 주소를 제한할 의무가 있는데(이 사건 고시 제4조 제5항 제1호), 이 사건 해커가 김차영의 컴퓨터를 이용하여 이용석의 아이디로 DB의 관문 역할을 하는 게이트웨이에 접속한 것에 비추어 보면, 허용되지 않은 IP 주소로도 게이트웨이에 접속할 수 있도록 한 잘못이 있다고 주장한다.

살피건대, 이 사건 해커가 김차영의 컴퓨터를 이용하여 이용석의 아이디로 DB의 게이트웨이에 접속한 사실은 앞서 본 바와 같으나, 을가 제42호증의 기재만으로는 김차영에게 DB 서버에 접속할 권한이 없었다고 인정하기에 부족하고, 달리 이를 인정할 증거가 없으며, 오히려 같은 증거 및 변론 전체의 취지를 종합하면, 김차영, 이용석, 김도영은 모두 DB 기술팀 소속으로 DB 접속권한이 있고, DB 기술팀의 직원들이 DB 서버에 접속하기 위해서는 가상 사설 네트워크인 VPN(Virtual Private Network)을 통해 먼저 게이트웨이에 접속하는데, 피고 SK컴즈는 게이트웨이에 접속가능한 IP 주소를

10) 현행 정보통신망법(2012. 2. 17. 법률 제11322호로 개정된 것) 제23조의2 제1항은 원칙적으로 주민등록번호의 수집·이용을 금지하고, 예외적인 경우에만 이를 수집·이용할 수 있는 것으로 개정되었다.

DB 서버에 접속할 권한이 있는 직원들이 사용하는 컴퓨터의 IP 주소로 한정시키고, DB 서버에 접속가능한 IP 주소는 게이트웨이의 IP 주소로 한정시키는 방법으로, 허용되지 않은 IP 주소를 통해 게이트웨이나 DB 서버에 접근할 수 없도록 조치를 취하고 있는 사실을 인정할 수 있으므로, 피고 SK컴즈가 이러한 조치를 취하지 않았다는 원고의 주장도 이유 없다.

다) 원고들은, ① 이 사건 해커는 이 사건 해킹사고와 동일한 방법으로 중국에서 원격접속을 통해 NHN의 내부망에 접근하였으나, NHN이 침입방지시스템을 통해 이를 차단하였고, ② 이 사건 해킹사고 발생 후 피고 SK컴즈가 이 사건 해커가 사용한 IP 주소를 차단하지 않아서 이 사건 해커가 2011. 7. 28. 같은 IP 주소를 이용하여 피고 SK컴즈의 직원 컴퓨터로 다시 접속을 시도한 점 등에 비추어 보면, 피고 SK컴즈가 침입탐지시스템 등을 부주의하게 운영하였다고 주장한다.

살피건대, ① 을가 제42호증의 기재에 의하면, 이 사건 해커가 2011. 7. 18. 이 사건 해킹사고와 동일한 방법으로 피고 이스트소프트의 알집 업데이트 서버를 이용해서 NHN 직원 컴퓨터에 ALAD2.exe라는 악성 파일을 감염시킨 사실, 이 사건 해커가 위와 같이 감염시킨 악성 파일 등을 이용하여 중국에서 NHN의 내부망으로 접근하였으나, NHN의 침입방지시스템에 의하여 차단된 사실은 인정할 수 있으나, 위 인정사실만으로는 NHN이 이 사건 해커의 접근을 차단한 시점 및 이를 차단한 구체적인 경위를 알 수 없고, NHN이 차단한 것을 피고 SK컴즈가 차단하지 못했다는 것만으로는 피고 SK컴즈의 침입탐지시스템 등의 운영에 어떠한 잘못이 있다고 단정할 수 없으며, ② 을가 제35호증의 기재에 의하면, 2011. 7. 28. 23:44경 피고 SK컴즈의 컴퓨터에서 이 사건 해킹사고에 사용된 중국 IP 주소로의 접근이 있어서 피고 안랩이 이를 탐지한 사

실은 인정할 수 있으나, 같은 증거 및 변론 전체의 취지를 종합하면, 위와 같은 접근은 피고 SK컴즈가 이 사건 해킹사고가 발생한 후 보안상의 취약점을 테스트하려는 목적으로 시행한 것으로 보이므로, 원고들의 이 부분 주장은 모두 이유 없다.

라) 원고들은, 피고 SK컴즈가 개인정보의 보호를 위해 복수의 백신을 사용할 의무가 있음에도 불구하고, 피고 시만텍이 공급하는 백신인 엔드포인트 프로텍션만을 사용한 잘못이 있고, 만약 피고 SK컴즈가 피고 이스트소프트사의 백신인 알약이나 피고 안랩의 백신인 V3를 사용하였더라면 이 사건 해킹사고가 발생할 가능성이 적었다고 주장한다.

살피건대, 피고 SK컴즈가 다른 종류의 백신을 복수 사용할 의무가 있음을 인정할만한 자료가 없고, 갑 제17, 42호증의 각 기재를 종합하면, 보안 관련 연구 단체인 바이러스 블런틴(www.virusbtn.com)은 2개월마다 백신 프로그램 성능 시험을 시행하여, 위 시험을 통과하는 경우 VB100 인증을 부여하는데, 피고 시만텍이 2011. 6.부터 2012. 2.까지 위 인증을 받지 못한 반면, 피고 안랩은 2011. 10., 피고 이스트소프트는 2011. 10. 및 같은 해 12. 위 인증을 각 받은 사실은 인정되나, 위 백신 프로그램 성능 시험은 매 시험마다 그리고 시험시 적용되는 컴퓨터 운영체제에 따라 그 결과가 달라지기 때문에 VB100 인증 여부만으로 백신의 우수성을 평가할 수 없으므로, 앞서 인정한 사실만으로는 알약이나 V3가 피고 SK컴즈가 사용한 피고 시만텍의 엔드포인트 프로텍션보다 우수하여 이 사건 해킹사고에 이용된 악성 파일을 더 잘 탐지하여 이를 치료할 가능성이 더 높았다고 인정하기에 부족하고, 달리 이를 인정할 증거가 없으며, 오히려 을가 제26, 39호증, 을다 제2 내지 4호증의 각 기재 및 변론 전체의 취지를 종합하면, 2011년을 기준으로 피고 시만텍의 세계 백신 시장 점유율은 8.77%로 6위에 해당

하는 등(피고 이스트소프트나 피고 안랩은 1% 미만이다) 일반적으로 품질이 인정되고 있는 제품인 사실을 인정할 수 있으므로, 결국 원고들의 이 부분 주장 역시 이유 없다.

마) 원고들은, 이 사건 해킹사고는 2011. 7. 26.과 같은 달 27. 이틀에 걸쳐서 새벽에 발생하였는데, 피고 SK컴즈가 2011. 7. 26. 업무시간 중 같은 날 새벽에 원격접속의 방법으로 이루어진 대용량 개인정보 접속 내역에 대하여 아무런 모니터링을 하지 않았기 때문에 같은 달 27. 추가적으로 발생한 해킹사고를 방지하지 못한 잘못이 있다고 주장한다.

살피건대, 피고 SK컴즈가 개인정보 DB 접속내역 등을 실시간으로 모니터링하여 이상 징후를 발견하고 이에 대한 경고를 하는 역할을 하는 침입탐지시스템 등을 갖추고 있었음에도 이를 적절히 운영하지 못하여 경고 발생의 기준을 지나치게 완화하여 설정하였기 때문에 이 사건 해킹사고 발생 당시 이를 탐지하지 못한 잘못이 있음은 앞서 본 바와 같으나, 실시간 모니터링을 하는 외에 이 사건 해킹사고가 발생한 당일의 업무시간 중 실시간 모니터링에서 탐지되지 않은 이상 징후를 발견하기 위한 사후적인 점검조치를 했어야 한다고 보기 어렵고, 따라서 앞서 인정한 실시간 모니터링상의 잘못 외에 사후적인 점검조치를 하지 않아서 2011. 7. 27. 발생한 해킹사고를 방지하지 못한 잘못을 별도로 인정하기는 어려우므로, 원고들의 위 주장도 이유 없다.

나. 손해배상책임의 범위

1) 재산상 손해에 관하여

원고들은, 개인정보는 원고들의 재산이므로, 피고 SK컴즈는 개인정보의 유출로 인하여 원고들에게 발생한 재산상 손해를 배상할 의무가 있다고 주장하나, 갑 제5, 29호증, 을가 제10호증의 각 기재만으로는 이 사건 해킹사고로 인하여 원고들에게 어

떠한 재산상 손해가 발생하였음을 인정하기에 부족하고, 달리 이를 인정할 증거가 없으므로, 원고들의 위 주장은 이유 없다.

2) 정신적 손해에 관하여

개인정보 유출로 인하여 그 정보주체에게 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 인한 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, 2011다60803(병합), 2011다60810(병합), 2011다60827(병합), 2011다60834(병합) 판결 참조}.

살피건대, 앞서 인정한 사실에 갑 제29호증의 기재 및 변론 전체의 취지를 종합하여 인정되는 다음과 같은 사정, 즉 ① 이 사건 해킹사고로 유출된 원고들의 개인정보는 성명, 주민등록번호, 아이디, 비밀번호, 주소, 전화번호 등 가장 기본적이면서 보호가 필요한 성격의 정보이며, 정보주체의 식별과 직접적으로 연결되어 있는 점, ② 비록 이 사건 해커가 원고들의 개인정보를 유출한 목적은 불분명하지만, 개인정보를 제3자에게 판매하여 이익을 얻고자 하였을 가능성도 상당하므로, 유출된 개인정보가 광범위하게 확산될 가능성도 크다고 보이는 점, ③ 피고 SK컴즈는 앞서 본 바와 같이 침입탐지시스템 등의 경고 발생 기준을 지나치게 완화하여 대용량의 개인정보가 파일로 생

성되고 외부로 유출되는 것을 탐지하지 못하고, 개인정보 접근권한이 있는 컴퓨터에서 보안상 취약한 공개용 알집을 사용하고 FTP 서비스를 제공하는 것을 방치하였으며, 개인정보 DB 관리자인 직원이 업무 수행 후 로그아웃을 하지 않고 자동 로그아웃 시간도 설정하지 않는 등 여러 면에서 개인정보를 보호할 의무를 소홀히 하여 이 사건 해킹사고를 방지하지 못한 점 등에 비추어 보면, 피고 SK컴즈는 이 사건 해킹사고로 인하여 원고들이 입은 정신적 손해를 배상할 의무가 있고, 그 범위는 각 200,000원으로 정함이 상당하다.

다. 소결론

따라서 피고 SK컴즈는 원고들에게 각 200,000원 및 이에 대하여 이 사건 해킹사고가 발생한 2011. 7. 26.부터 위 피고가 그 이행의무의 존부 및 범위에 관하여 항쟁함이 상당한 이 사건 판결선고일인 2013. 2. 15.까지는 민법이 정한 연 5%의, 그 다음날부터 다 갚는 날까지는 소송촉진 등에 관한 특례법이 정한 연 20%의 각 비율에 의한 지연손해금을 지급할 의무가 있다.

3. 피고 이스트소프트에 대한 청구에 관한 판단

가. 원고들의 주장

1) 피고 이스트소프트는 정보통신망법 제2조 제1항 제3호에서 규정한 정보통신서비스 제공자로서 같은 법 제32조에 따라 이 사건 해킹사고로 인해 원고들의 개인정보가 유출된 것에 대한 손해배상책임을 부담한다.

2) 피고 이스트소프트가 이 사건 해킹사고가 발생하기 전인 2011. 7. 19. 위 피고의 직원 컴퓨터에서 이 사건 해커가 만든 악성 ALAD.dll 파일을 발견하고 이를 치료한 점에 비추어 위 피고는 위 일시경에 알집 업데이트 서버가 해킹당한 사실을 알고 있었

음에도 정보통신방법 제48조의3 제1항을 위반하여 이러한 해킹 사실을 방송통신위원회 등에 신고하지 않은 잘못이 있는바, 만약 피고 이스트소프트가 이를 신고하였다면 이 사건 해킹사고가 방지되었을 것이다.

3) 이 사건 해커는 피고 이스트소프트의 ISAPI 필터에 stmpxml.dll 파일을 등록하는 방법으로, 피고 SK컴즈가 악성 ALAD.dll 파일을 다운로드 받게 하였는데, 피고 이스트소프트는 알집 업데이트 서버의 관리를 소홀히 한 잘못으로 이 사건 해커가 피고 이스트소프트의 관리자 권한을 탈취하여 위와 같이 ISAPI 필터를 변조하도록 하고, 이를 발견하지 못한 잘못이 있다.

나. 판단

1) 피고 이스트소프트가 정보통신서비스 제공자인지에 관하여

살피건대, 이 사건 해킹사고로 인해 유출된 원고들의 개인정보는 원고들이 피고 SK컴즈가 제공하는 정보통신서비스를 이용하기 위하여 위 피고에게 제공한 것이어서, 정보통신망법에 따라 이러한 개인정보를 보호할 의무는 피고 SK컴즈만이 부담하므로, 피고 이스트소프트는 원고들에 대한 관계에서 정보통신서비스 제공자라고 볼 수 없고, 따라서 이와 다른 전제에서 피고 이스트소프트에 정보통신망법 제32조가 적용되어야 한다는 원고들의 주장은 이유 없다.

2) 알집 업데이트 서버의 해킹사실을 신고하지 않은 잘못이 있는지에 관하여

살피건대, 을가 제42호증의 기재 및 변론 전체의 취지를 종합하면, 피고 이스트소프트가 2011. 7. 18. 직원의 컴퓨터에서 악성 ALAD.dll 파일을 발견하고, 위 피고가 제조·공급하는 백신 프로그램인 알약으로 위 악성 파일이 치료될 수 있도록 조치를 취한 사실은 인정되나, 위 인정사실만으로는 피고 이스트소프트가 이 사건 해킹사고 발

생 전에 알집 업데이트 서버가 해킹되었기 때문에 악성 ALAD.dll이 감염되었다고 알았거나 알 수 있었다고 보기 부족하고, 달리 이를 인정할 증거가 없으므로, 피고 이스트소프트가 알집 업데이트 서버 해킹사실을 알면서도 이를 신고하지 않았다는 원고들의 주장도 이유 없다.

3) 알집 업데이트 서버의 관리와 관련된 잘못이 있는지에 관하여

살피건대, 피고 이스트소프트의 알집 업데이트 서버의 ISAPI 필터가 이 사건 해커로 인하여 변조된 사실 및 위 피고가 이 사건 해킹사고의 발생 전까지 이를 발견하지 못한 사실은 앞서 본 바와 같으나, 이 사건 해커가 어떠한 방법으로 ISAPI 필터를 변조하였는지에 관해 전혀 밝혀진 바가 없고, 피고 이스트소프트가 ISAPI 필터의 변조를 의심할만한 사정이 있었음을 인정할만한 사정도 없으므로, 앞서 인정한 사실만으로는 피고 이스트소프트에게 알집 업데이트 서버의 관리와 관련된 잘못이 있음을 인정하기에 부족하고, 달리 이를 인정할 증거가 없다(설령 피고 이스트소프트에게 알집 업데이트 서버 관리와 관련하여 어떠한 잘못이 있다고 하더라도, 앞서 본 바와 같이 피고 SK컴즈의 직원들이 피고 이스트소프트의 저작권을 침해하여 공개용 알집을 사용한 것이 이 사건 해킹사고가 발생한 원인 중 하나가 되었고, 피고 이스트소프트로서는 위 피고의 서버가 해킹됨으로써 위 피고가 보유하고 있는 개인정보가 아니라 피고 SK컴즈가 보유하고 있는 개인정보가 유출되리라고 예견하기도 매우 어려웠으리라고 보이므로, 피고 이스트소프트의 알집 업데이트 서버 관리상의 잘못과 이 사건 해킹사고로 인한 원고들의 손해발생 사이에 상당인과관계가 있다고 보기도 어렵다).

4. 피고 시만텍에 대한 청구에 관한 판단

가. 원고들의 주장

1) 피고 시만텍은 2011. 7. 26. 이 사건 해커가 감염시킨 악성 파일 중 windowsrpc.dll 파일의 시그니처(signature)[11]를 생성하였음에도, 이를 백신 프로그램에 등록하지 못한 잘못으로 같은 달 27. 이 사건 해킹사고가 발생하는 것을 방지하지 못한 잘못이 있다.

2) 피고 시만텍은 엔드포인트 프로텍션 백신을 피고 SK컴즈에게 공급한 자로서 새롭게 발생하는 악성코드에 대한 정보를 분석하여 이에 대응할 수 있도록 위 백신을 업데이트할 의무를 이행하지 않음으로써 V3, 알약 등 다른 백신이 탐지할 수 있었던 이 사건 해킹사고에 사용된 악성 파일을 탐지하지 못한 잘못이 있다.

나. 판단

1) windowsrpc.dll 파일의 시그니처 생성과 관련하여

살피건대, 을다 제6, 7호증의 각 기재 및 변론 전체의 취지를 종합하면, 피고 시만텍은 이 사건 해킹사고가 종료된 2011. 7. 27. 17:17경에야 windowsrpc.dll 파일의 시그니처 생성을 완료한 사실을 인정할 수 있으므로, 피고 시만텍이 이 사건 해킹사고 전에 위 파일의 시그니처를 생성하였음에도 이를 백신 프로그램에 등록하지 않은 잘못이 있다는 원고들의 주장은 이유 없다(또한 windowsrpc.dll 파일이 이 사건 해킹사고와 관련하여 어떠한 역할을 하였는지가 불분명하므로, 위 파일이 피고 시만텍의 백신 프로그램에 의해 이 사건 해킹사고 발생 전에 발견되어 치료되었다고 하더라도, Nateon.dll, nateon.exe 등 다른 악성 파일이 치료되지 않고 남아있는 이상 이 사건 해킹사고가 발생하지 않았으리라고 보기도 어렵다).

2) 백신 업데이트와 관련하여

11) 시그니처 기반 백신은 악성 코드로 의심되는 파일(샘플)의 패턴을 분석하여 시그니처를 생성한 후 이를 백신 프로그램에 등록하는 방법으로 악성 코드를 탐지한다.

살피건대, 갑 제17, 42호증의 각 기재만으로는, 이 사건 해킹사고에 사용된 악성파일이 피고 시만텍의 엔드포인트 프로텍션 백신이 아닌 V3나 알약 등 다른 백신에 의해서라면 충분히 탐지될 수 있었다고 인정하기에 부족하고, 달리 피고 시만텍이 새롭게 발생하는 악성코드에 대한 정보를 분석하여 이에 대응할 수 있도록 엔드포인트 프로텍션 백신을 업데이트하는 것을 소홀히 하였다고 볼만한 사정도 없으므로, 원고들의 위 주장도 이유 없다.

5. 피고 안랩에 대한 청구에 관한 판단

가. 원고들의 주장

피고 안랩은 피고 SK컴즈의 침입탐지시스템 등을 다음과 같이 적절히 운영하지 못하여 이 사건 해킹사고를 방지하지 못한 잘못이 있다.

1) 피고 안랩은 이 사건 해킹사고 발생 후인 2011. 7. 28. 이 사건 해커가 사용한 중국 IP 주소에서 피고 SK컴즈 직원 컴퓨터로의 접속을 탐지하였는데, 이 사건 해킹사고가 발생하기 전에는 이 사건 해커가 피고 SK컴즈의 내부망에 접근하는 것을 탐지하지 못한 점에 비추어 보면, 위 해킹사고 발생 당시 당시 피고 안랩이 실시간 모니터링을 소홀히 하고 있었다고 볼 수 있다.

2) 이 사건 해킹사고 발생 당시 심야에 대량으로 이루어진 개인정보 DB 접속 및 개인정보 파일생성, 전송 등을 이상 징후로 탐지하지 못하였다.

나. 판단

1) 살피건대, 2011. 7. 28. 23:44경 피고 SK컴즈의 컴퓨터에서 이 사건 해킹사고에 사용된 중국 IP 주소로의 접근이 있어서 피고 안랩이 이를 탐지한 것은 사실이나 위와 같은 접근은 피고 SK컴즈가 이 사건 해킹사고가 발생한 후 보안상의 취약점을 테스트

하려는 목적으로 시행한 것으로 보인다는 점은 앞서 본 바와 같으므로, 피고 안랩이 이 사건 해킹사고 발생 전에 이 사건 해커의 접근을 충분히 탐지할 수 있었음에도, 실시간 모니터링을 할 의무를 소홀히 하여 이를 탐지하지 못하였다는 원고들의 주장은 이유 없다.

2) 나아가, 이 사건 해킹사고가 발생하고 있는 동안 피고 SK컴즈의 침입탐지시스템 등이 대용량의 개인정보가 새벽에 파일로 생성되고 FTP 방식으로 전송되는 것을 이상 징후로 감지하지 않아서 경고를 하지 않았다는 점에 비추어 피고 SK컴즈가 경고 발생의 기준을 지나치게 완화하여 설정함으로써 개인정보 보호의무를 충분히 이행하지 못하였다고 볼 수 있고, 피고 안랩은 피고 SK컴즈와 사이의 보안관제서비스 용역계약에 따라 피고 SK컴즈의 침입탐지시스템 등을 운영하고 있는 점은 앞서 본 바와 같으나, 피고 안랩은 피고 SK컴즈와 체결한 위 용역계약에 따라 피고 SK컴즈에 대하여 보안관제서비스 제공의무를 부담할 뿐이고, 그 구체적인 업무의 내용은 피고 SK컴즈와의 계약에 따라 정해지며, 어떠한 경우를 이상 징후로 감지하여 침입탐지시스템 등에 경고가 발생하도록 할 것인지의 기준을 정하는 주체는 정보통신서비스 제공자이자 개인정보의 보관자로서 침입탐지시스템 등을 운영할 의무가 있는 피고 SK컴즈라고 할 것이고, 피고 안랩이 원고들에 대한 관계에서 어떠한 계약상 또는 법령상 개인정보 보호의무를 부담한다고 볼 수도 없으므로, 피고 안랩이 이 사건 해킹사고의 발생을 탐지하지 못하였다고 하여 원고들이 위 피고를 상대로 개인정보 유출로 인한 손해배상을 청구할 수는 없다고 할 것이다.

6. 결론

그렇다면, 원고들의 피고 SK컴즈에 대한 청구는 위 인정범위 내에서 이유 있어 이를

인용하고, 원고들의 피고 SK컴즈에 대한 나머지 청구 및 피고 이스트소프트, 시만텍, 안랩에 대한 각 청구는 이유 없어 이를 각 기각하기로 하여 주문과 같이 판결한다.

재판장 판사 배호근

판사 황은규

판사 김윤희

별지2.

관 련 법 령

[정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)]

제2조(정의)

① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

제4장 개인정보의 보호

제23조(개인정보의 수집 제한 등)

② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다.

제23조의2(주민등록번호 외의 회원가입 방법)

① 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 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다.

제28조(개인정보의 보호조치)

① 정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치

5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

제32조(손해배상)

이용자는 정보통신서비스 제공자 등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자 등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자 등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

제45조(정보통신망의 안정성 확보 등)

① 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

② 방송통신위원회는 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치 및 안전진단의 방법·절차·수수료에 관한 지침을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다.

제48조의3(침해사고의 신고 등)

① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다.

1. 정보통신서비스 제공자
2. 집적정보통신시설 사업자

[정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(정보통신망법 시행령)]

제15조(개인정보의 보호조치)

① 법 제28조 제1항 제1호에 따라 정보통신서비스 제공자 등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다.

1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항
2. 개인정보취급자의 교육에 관한 사항
3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항

② 법 제28조 제1항 제2호에 따라 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행
2. 개인정보처리시스템에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 및 침입탐지

시스템의 설치·운영

3. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영

4. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

③ 법 제28조 제1항 제3호에 따라 정보통신서비스 제공자 등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독

2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

④ 법 제28조 제1항 제4호에 따라 정보통신서비스 제공자 등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.

1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장

2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장

3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치

4. 그 밖에 암호화 기술을 이용한 보안조치

⑤ 법 제28조 제1항 제5호에 따라 정보통신서비스 제공자 등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다.

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조 제1항 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

[개인정보의 기술적·관리적 보호조치 기준(이 사건 고시)]

제4조(접근통제)

④ 정보통신서비스 제공자 등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.

⑤ 정보통신서비스 제공자 등은 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

제6조(개인정보의 암호화)

① 정보통신서비스 제공자 등은 비밀번호 및 바이오정보는 복호화되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자 등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

제8조(출력·복사시 보호조치)

① 정보통신서비스 제공자 등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일 생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화한다.

② 정보통신서비스 제공자 등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

[정보보호조치 및 안전진단 방법·절차·수수료에 관한 지침]

제2조(정보보호조치의 내용)

법 제45조 제2항에 따라 정보통신서비스 제공자가 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위하여 마련하여야 하는 관리적·기술적·물리적 보호조치의 구체적인 내용은 별표 1과 같다.

[별표1]

보호조치의 구체적인 내용

구 분			세 부 조 치 사 항
2. 기술적 보호조치	2.2. 정보통신 설비 보안	2.2.5. 라우터[12]/스위치 보안	▸ ACL 등의 접근제어 기능을 적용할 수 있는 설비를 사용
		2.2.8. 접근통제 및 보안설정 관리	▸ 인가된 자만 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 등을 사용하도록 하여 인가 절차를 강화 ▸ 불필요한 프로토콜 및 서비스 제거 등 보안설정

비고 7. 2.2.7~2.2.11의 사항은 2.2.1~2.2.6에 해당하는 설비에 적용된다. 끝.

12) 라우터는 네트워크 장비의 일종으로, 패킷을 다른 네트워크로 보내면서 이와 함께 최적의 네트워크 경로를 찾아주는 역할도 한다. 라우터는 네트워크를 연결하는 점에서 게이트웨이와 상통하고, 게이트웨이가 라우터보다 포괄적인 개념이라고 보나, 라우터와 게이트웨이를 혼용하여 쓰는 경우도 있다.