시정조치등취소청구

[서울행정법원 2019. 4. 25. 2018구합65682]

【전문】

【원 고】 주식회사 이스트소프트(소송대리인 법무법인 세종 담당변호사 김용호 외 2인)

【피 고】 방송통신위원회(소송대리인 법무법인 인 담당변호사 권창범 외 1인)

【변론종결】2019. 3. 26.

【주문】

】

1. 원고의 청구를 모두 기각한다.

2. 소송비용은 원고가 부담한다.

【청 구 취 지】피고가 2018. 3. 28. 원고에 대하여 한 별지 처분 내역 기재 처분 중 제1 내지 3항(시정조치, 공표명령), 제4항 가목(과징금 부과)을 모두 취소한다.

【이유】

】1. 처분의 경위

가. 원고는 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2018. 9. 18. 법률 제15751호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다)에 따른 정보통신서비스 제공자로서, 알툴즈 패키지(알툴바, 알집, 알송, 알PDF 등) 소프트웨어를 개발하고, '알툴즈'라는 온라인 사이트(http://www.altools.com)를 운영하면서 알툴즈 패키지를 제공하는 사업을 운영하는 법인이다.

나. 피고는 2017. 9. 2.부터 2018. 1. 10.까지 원고에 대하여 개인정보 처리 운영·실태를 조사한 다음 원고가 보관·관리하는 알툴즈 계정에 등록된 166,179명의 알패스 정보 25,461,263건에 관한 회원정보(이하 '이 사건 회원정보'라 한다)가 중국 국적의 소외 4 등(이하 '이 사건 해커'라 한다)에 의하여 2017. 6. 2.부터 2017. 9. 12.까지 사전대입 공격으로 유출된 것을 확인하였다.

다.

피고는 2018. 3. 28. 원고에 대하여 아래와 같은 이유로 구 정보통신망법 제28조 제1항, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(이하 '정보통신망법 시행령'이라 한다) 제15조 제2항, 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시 제2015-3호, 이하 '이 사건 보호조치 기준'이라 한다) 제4조 제5항, 제9항을 위반하였다고 보아 구 정보통신망법 제64조, 제64조의3 등에 따라 별지 처분 내역 기재 처분과 같이 시정명령, 시정명령 받은 사실의 공표, 교육 및 대책 수립 후 보고, 과징금 1억 1,200만 원, 과태료 1,000만 원 등을 명하는 처분을 하였다(이하 별지 처분 내역 기재 처분 중 제1 내지 3항, 제4항 가목의 처분을 '이 사건 각 처분'이라 한다).

처분사유세부내용해당 법령1. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위(이하 '이 사건 제1 처분사유'라 한다) ■ 이 사건 보호조치 기준 제4조 제5항: 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 ■ 원고의 침입차단 내지 침입탐

지시스템 설치행위 관련: 이 사건 해커는 알패스(Alpass) 3.0.exe와 이전에 확보한 아이디와 비밀번호를 통하여 이용자가 알툴바 서버에 접속하는 경우와 유사하게 알툴바 서버에 접속한 뒤 이 사건 회원정보를 유출하였는데, 원고는 알패스 프로그램 등을 운영하면서 Snort라는 오픈소스를 사용한 침입탐지만을 적용하고, 운영체제에서 제공하는 기본 방화벽(iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었으나 이는 원고의 사업 규모, 개인정보 보유수 등에 맞는 침입차단시스템이나 침입탐지시스템을 설치한 것으로 보기 어려워 침입차단 내지 침입탐지시스템을 설치하지 않았다.

■ 원고의 침입차단 내지 침입탐지시스템 운영행위 관련: 이 사건 해커가 사용한 사전대입 공격은 침입탐지시스템 로그를 분석하였다면 2017. 6. 2.부터 2017. 9. 12.까지 전체 접속기록 2억 261만 2,768건의 81%에 해당하는 1억 6,504만 9,639건의 접속실패 기록을 확인하여 이상행위를 발견할 수 있었음에도 이러한 로그기록을 분석하지 않았고, 이전에 2016. 11.경 사전대입 공격을 인지하기도 하였으나 접근제한 정책이나 모니터링, 로그분석 등을 조치를 취하지 않았다.

구 정보통신망법 제28조 제1항 제2호정보통신망법 시행령 제15조 제2항 제2호이 사건 보호조치 기준 제4조 제5항2. 알패스 서비스 이용자 개인정보가 열람권한 없는 자에게 공개되거나 외부에 유출되지 않도록 조치하지 않은 행위(이하 '이 사건 제2 처분사유'라 한다) ■ 이 사건 보호조치 기준 제4조 제9항: 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

■ 원고는 2016. 11.경 사전대입 공격이 있었음에도 불구하고, 비밀번호 초기화, 접속차단, 캡차주2) 등을 조치를 하지 않아 2016. 11.경 384,758명의 계정 비밀번호가 유출되었음에도 이 사건 해커의 공격으로 그 중 155,049명의 알패스 정보가 유출된 이외에 이 사건 회원정보가 유출되기도 하였다.

구 정보통신망법 제28조 제1항 제2호정보통신망법 시행령 제15조 제2항 제5호이 사건 보호조치 기준 제4조 제9항처분내용별지 처분 내역 기재와 같다.

캡차

[인정근거] 다툼 없는 사실, 갑 제1호증, 을 제5, 7호증(가지번호 있는 것은 각 가지번호 포함, 이하 같다)의 각 기재, 변론 전체의 취지

2. 처분의 적법 여부

가. 원고의 주장

다음과 같은 이유로 이 사건 각 처분은 위법하다.

1) 침입행위 부존재

이 사건 해커에 의하여 이 사건 회원정보가 유출되기는 하였으나, 이는 사전대입 공격에 의하여 이루어진 것으로 아이디와 패스워드를 입력하여 정상적인 로그인 절차를 거쳐 알패스 프로그램(이하 '이 사건 프로그램'이라 한다)에 로그인한 것일 뿐 무단 침입에 의하여 이 사건 회원정보가 유출되었다고 볼 수 없다.

2) 이 사건 제1 처분사유 관련

가) 개인정보처리시스템 미해당

이 사건 회원정보는 데이터베이스(Database)에 보관되어 있고, 데이터베이스를 관리하기 위한 데이터베이스 관리 시스템(DBMS; Database Management System)이 별도로 존재하는데, 개인정보처리시스템이란 내부영역인 데이터베이스나 데이터베이스 관리 시스템을 의미하고, 이 사건 프로그램처럼 데이터베이스에 접근하기 위한 응용프로그램은 개인정보처리시스템에 포함되지 않으며, 웹페이지도 개인정보처리시스템에 포함된다고 볼 수 없다.

나) 원고의 침입차단・침입탐지시스템 설치・운영의무 준수

원고는 iptables, Webknight, Snort와 같은 보안성이 입증되어 널리 사용된 침입차단・침입탐지시스템을 설치하였다.

구체적으로 Webknight는 침입차단 및 탐지기능을 갖춘 시스템으로 한국인터넷진흥원에서 기술안내서 가이드를 발간한 제품이고, Snort는 네트워크 보안 제품 중 5위에 선정된 우수한 제품이며, Cisco사, 시큐아이 등의 보안장비 솔루션 제공업자가 오픈소스인 Snort 엔진을 기반으로 솔루션을 제공하고 있고, iptables도 리눅스 운영체제에서 제공하는 방화벽(침입차단시스템)으로 널리 사용되고 있다.

피고는 원고가 2016. 11.경의 사전대입 공격이 있은 후에 이상 행위 대응, 로그 분석의 조치를 취하지 않아 침입탐지시스템을 운영하였다고 볼 수 없다고 하나 침입에 대비하여 주식회사 이글루시큐리티(이하 '이글루시큐리티'라 한다)로부터 보안관제서비스를 제공받고 있고, 이글루시큐리티는 침입차단 및 탐지시스템의 로그들을 24시간 관제하는 침입탐지기능을 수행하였다.

3) 이 사건 제2 처분사유 관련

가) 이 사건 보호조치 기준 제4조 제9항 미적용

이 사건 보호조치 기준 제4조 제9항은 정보통신서비스 제공자의 부주의 등과 같은 내부적 요인에 따라 검색엔진을 통하여 개인정보가 누출되지 않도록 조치를 하라는 의미이므로, 이 사건과 같이 외부적 요인인 해킹에 의하여 개인정보가 유출된 경우에는 적용되지 않는다.

나) 원고의 개인정보 노출방지 조치 시행

원고는 2016. 11.경 사전대입 공격이 이루어진 후 부정접속이 의심되는 계정의 이용자들에게 비밀번호 변경을 요청하였고, 2016. 11.경 알패스 단독프로그램의 운영을 종료하였으며, 알툴바를 통한 알패스 서비스의 제공에 있어서도 5회 이상 로그인에 실패할 경우 5분 동안 정상적인 로그인을 차단하는 조치나 동일한 IP로 1시간 내에 500회 이상 로그인 시도 시 로그인을 임시차단하고, 임시차단이 된 이후에도 1시간 동안 5,000회 이상 로그인을 시도하는 경우 블랙리스트로 자동등록하여 접근을 차단하였으며, 1회라도 공격을 한 IP주소 등을 블랙리스트에 등록하기도 하였고, 유료 방화벽인 시큐아이 MF2-6000을 도입하여 분석된 시간별로 IP를 분석하여 이상이 발생하는 경우 경보알림을 받기로 하기도 하였는바, 개인정보 노출방지를 위한 조치를 시행하였다고 볼 수 있다.

나. 관계 법령

별지 관계 법령 기재와 같다.

다.

인정사실

1) 이 사건 각 처분과정에서 작성된 심의・의결서의 주요 내용은 아래와 같다.

■ 사실조사 결과▲ 행위사실● 유출규모이 사건 해커의 알툴바 서비스에 대한 사전대입 공격으로 피심인(원고, 이하 이 표에서 '피심인'이라 한다)이 '알툴즈 소프트웨어' 제공서비스를 운영하면서 수집한 2017. 9. 26. 기준 회원정보(아이디, 비밀번호, 이름, 이메일 등) 총 2,189,950명(휴면회원 1,490,927명 포함) 중 166,179명(중복제거)의 알툴즈 이용자 계정에 등록된 알패스 정보 25,461,263건이 유출되었다.

피심인의 유출 정보 현황구 분유출된 항목건수중복제거사전대입공격 ('17. 2. 9.~9. 25.)알패스 정보외부사이트 도메인, 아이디, 비밀번호25,461,263건166,179명* 검거된 해커의 PC에 저장('17. 2. 9. ~ 9. 25.)되어 있던 개인정보 유출 자료 알패스 유출정보의 웹사이트 종류별 유출 계정 건수합계(건)포털공공가상통화금융통신기타25,461,2631,015,430689,1711,90959,285201,71723,493,751● 유출경로△ 2017년 사전대입 공격피심인의 데이터베이스(이하 'DB'라 한다)내 존재하는 2017. 6. 2.부터 2017. 9. 12.까지 기간의 접속기록을 분석한 결과, 피심인의 알툴바 서비스에 총 2억 261만 2,768건의 대량 접속 시도가 있었고, 이 중 81%에 해당하는 1억 6,504만 9,639건이 접속에 실패하였으며, 최소 52만 2,532명의 계정이 이 사건 해커에 의해 접속 성공된 것을 확인하였다.

또한, 이 사건 해커에 대한 경찰청 조사 결과에 따르면 이 사건 해커는 2017. 2. 9.경부터 2017. 9. 25.경까지 '알툴바' 서비스에 사전대입 공격을 한 것을 확인하였다.

△ 2016. 11.경 사전대입 공격 관련이 사건 조사과정 중 피심인의 소명을 통하여 알패스 서비스에 2016. 11.경에 별건의 사전대입 공격이 있었다는 사실을 확인하였다.

피심인이 2016. 11. 10.경 별건의 사전대입 공격에 대하여 자체적으로 분석한 자료를 확인한 결과 당시 불상의 해커는 대량의 알패스 계정정보(아이디, 비밀번호)를 이용하여 알패스 서비스를 대상으로 54개 IP에서 약 1백만 번의 접속 시도를 하였고 이 중 부정접속이성공한 것으로 의심되는 이용자 계정은 총 2,143,766건(휴면회원 포함) 중 최소 384,758건(약 17.9%)으로 확인하였다.

피심인은 불상의 해커에 의한 사전대입 공격을 인지한 후 2016. 11. 19. 부정한 접속이 의심되는 이용자 384,758명에게 비밀번호 변경을 안내하는 메일을 발송하였다.

△ 개인정보 유출알패스 이용자는 아이디, 비밀번호를 이용하여 정상적으로 알툴바에 접속하는 경우 알패스 프로그램에 저장된 외부 사이트 주소, 그 사이트에 대한 아이디 및 비밀번호를 화면으로볼 수 있다.

이 사건 해커는 해킹프로그램인 '알패스(Alpass) 3.0.exe'와 사전에 대량으로 확보한 이용자의 아이디, 비밀번호를 이용하여 이용자가 알툴바에 접속하는 경우와 유사하게 알툴바서버에 접속하여 이용자 166,179명이 등록한 알패스 정보(외부사이트 도메인, 아이디, 비밀번호) 25,461,263건을 txt파일로 저장하여 외부로 유출하였다.

또한, 이 사건 해커는 2017. 9. 1.부터 2017. 9. 8.까지 피심인으로부터 탈취한 이용자의 계정정보(아이디, 비밀번호) 254,614건(중복제거) 및 알패스정보(외부사이트도메인, 아이디, 비밀번호) 271,747개가 담겨있는 알툴즈 계정 3,019개(중복제거) 파일과 동영상 파일, 보도자료 등을 제시하며 전화통화 및 전자우편 등으로 67회(전화 8회, 전자우편 52회, 게시글 6회, SMS문자 1회)에 걸쳐 끈질기게 현금 5억 원에 해당하는 비트코인을 요구하며 피심인을 협박하였으나, 피심인은 이에 응하지 않았다.

해커의 사전대입 공격 및 자료 유출 현황구분유출기간건수사전대입 공격'16. 8. 30. ~ 11. 10.(접속기록 분석 기간)최소 384,758건(부정 접속이 의심되는 알툴즈 계정)'17. 6. 2. ~ 9. 12.(접속기록 분석 기간)최소522,532건(접속이 성공한

알툴즈계정)해커 협박 메일'17. 9. 1. ~ 9. 8.(해커 협박 기간)271,747건(알패스 정보)206,762건(알툴즈 계정)검거된 해커 PC'17. 2. 9. ~ 9. 25.(PC에 저장되어 있던 기간)25,461,263건(알패스 정보)166,179건(알툴즈 계정)이 사건 해커가 제시한 254,614건의 계정정보를 알툴즈 DB에 있는 이용자 계정과 비교한 결과 206,762개가 실제 알툴즈 계정으로 확인되었고, 특히 2016. 11.경 당시 사전대입 공격으로 접속이 성공한 계정 384,758건 중 155,049건이 동일한 계정으로 확인되었다.

△ 이용자 2차 피해 발생이 사건 해커는 유출한 알툴즈 계정의 알패스정보(외부 사이트 도메인, 아이디, 비밀번호)를 이용하여 이용자들이 가입한 다른 웹사이트에 부정 접속한 후 이용자들이 저장한 신분증(주민등록증 등)과 신용카드 사진을 추가로 확보한 뒤 이를 도용하여 범행에 사용할 휴대전화를 개통하고 서버 5대를 임대하였다.

또한 가상통화 거래를 하는 이용자계정으로는 거래사이트에 부정접속하여 해당 이용자의 비트코인(당시시세: 800만 원, 수량: 2.1 코인)을 절취하여 이용자에게 2차 피해가 발생한 것을 검거된 이 사건 해커에 대한 경찰청 조사 결과를 통해 확인하였다.

● 개인정보 유출 경로 요약이 사건 해킹의 방법 및 절차 등은 크게 2단계로 구분해볼 수 있는데,① 이 사건 해커는 해킹 프로그램인 '알패스(Alpass) 3.0.exe'와 출처를 알 수 없는 대량의 아이디, 비밀번호를 확보하여 피심인의 '알툴바' 서비스에 접속을 시도하는 사전대입 공격(2017. 2. 9. ~ 2017. 9. 25.)을 하였고,② 이를 통해 접속이 성공한 '알툴즈' 이용자의 계정에 등록된 '알패스' 정보를 txt 파일로 저장하여 유출한 것으로 조사되었다.

〈개인정보 유출사고 개요도 생략〉■ 위법성 판단▲ 개인정보의 분실・도난・유출・변조 또는 훼손을 방지하기 위한 기술적・관리적 보호조치를 아니한 행위(정보통신망법 제28조 제1항, 이 사건 제1 처분사유)● 이 사건 보호조치 기준(이하 이 표에서 '고시'라 한다) 제4조 제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호), 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호) 기능을 포함한 시스템을 설치・운영하여야한다"라고 규정하고 있다.

고시해설서는 ▲ "정보통신망을 통해 개인정보처리시스템에 불법적으로 접근하는 행위를 방지・차단하기 위해 침입차단기능 및 침입탐지기능을 갖는 시스템등을 설치・운영함으로써 네트워크 보안을 강화하여야한다"라고,▲ "침입차단 및 침입탐지 기능을 갖춘 설비의 설치방법으로, 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치・운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS: Intrusion Prevention System), 웹 방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다"라고,▲ "전문 침입차단시스템 및 침입탐지시스템의 설치운영이 곤란한 SOHO 등 소기업의 경우 인터넷데이터센터(IDC) 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를활용함으로써 초기 투자비용 등을 줄일 수 있다"라고,▲ "또한, 공개용(무료) S/W를 사용하여 해당기능을 구현한 시스템을 설치・운영할 수 있다.

다만 공개용(무료) S/W를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검할 필요가 있다"라고,▲ "불법적인 접근 및 침해사고 방지를 위한 목적 달성을 위해서는 침입차단과 침입탐지 기능을 갖는 시스템 도입과 더불어 침입차단 정책 설정 및 침입탐지 로그 분석, 로그 훼손 방지 등 적절한 운영・관리가 중요하다"라고 설명하고 있다.

고시 제4조 제5항의 입법목적은 '정보통신망을 통한 불법적인 접근 및 침해사고 방지'인바, 그 내용은 첫째 침입차단 및 침입탐지기능을 포함한 시스템의 '설치' 의무이고, 둘째 침입차단 및 침입탐지기능을 포함한 시스템의 '운영'의무이다.

먼저 시스템 '설치' 의무에 대하여 살펴보면, 정보통신서비스 제공자등은 ① 접속권한을 IP주소 등으로 제한하여 비인가 접근을 '차단'하는 기능(침입차단기능)과 함께 ② 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법 유출시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

피심인은 전문기업의 별도 시스템 설치 및 운영은 임의적 이행사항에 불과하며, 오픈소스 기반의 침입탐지시스템과 운영체제에서 제공하는 기본 방화벽을 설치 및 운영하고 있었으므로 위법하지 않다고 주장하고 있다.

구 개인정보의 기술적·관리적 보호조치 기준(2015. 5. 19. 방송통신위원회고시 제2015-3호로 개정되기 전의 것) 제1조는 기술적·관리적 보호조치의 '구체적인 기준'을 정하는 것을 목적으로 한다고 규정하고 있었으나, 방송통신위원회는 2015. 5. 19. 개인정보 보호조치에 대한 사업자의 자율성·책임성을 강화하기 위하여 개인정보의 기술적·관리적 보호조치 기준 제1조를 개정하여 고시 상의 의무들이 사업자가 준수해야 할 '최소한의 기준'임을 명시적으로 규정하고, 고시 제1조 제2항에 사업자들이 사업의 규모, 개인정보 보유 수 등을 고려하여 자발적으로 보호조치를 이행하도록 하는 규정을 신설하였다.

피심인은 개인정보가 저장관리되고 있는 이용자 수가 100만 명 이상으로 , 이용자가 알패스에 등록한 중요정보(외부 사이트, 아이디, 비밀번호)가 수천만 건 이상이고, 전년도 정보통신서비스 부문 매출액이 100억 원 이상으로 '일정 규모 이상 사업자주3)로서 그 사업규모, 개인정보 보유 수를 고려하여 개인정보 보호조치를 취하여야 할 것이다.

또한, 수집·보관 중인 이용자의 알패스 개인정보는 이용자가 다른 사이트를 이용하기 위한 비밀번호로 유출 시 이용자가 입게 되는 피해의 정도가 매우 심각하므로 일반적인 개인정보를 처리하는 정보통신서비스 제공자에 비해 개인정보 보호조치를 강화할 필요가 있다.

그런데 피심인은 오픈소스(Snort)를 이용한 침입탐지만을 적용하였고, 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었으나, 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템 등의 보안장비를 도입하여 운영한 사실은 없었으며 2017. 7.경에서야 방화벽(시큐아이 MF2-6000)을 신규 도입하였다.

즉, 피심인의 사업 규모, 개인정보 보유 수 등을 고려할 때, 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하지 않은 것은 설치의 의무를 소홀히 한 것으로 판단된다.

다음으로 '운영' 의무와 관련하여, 시스템의 '운영'은 단순히 시스템의 전원을 켜 놓은 상태를 의미하는 것이 아니라 목적(침입차단 및 침입탐지) 달성에 필요한 기능을 활용하는 것을 의미하므로, 단순히 시스템의 전원을 켜 놓은 상태나 침입차단 및 침입탐지에 필요한 기능을 활용하지 못한 상태 등은 '운영'이라고 할 수 없다 , 이 사건 해커의 수법인, IP를 변경하며 봇을 이용한 사전대입 공격은 피심인이 일정기간 보관된 침입탐지시스템 등의 로그를 한 번이라도 분석하였다면(DB 내 ALTools Member_ Data 테이블에 존재하는 2017. 6. 2. ~ 2017. 9. 12. 기간 접속 기록을 분석한 결과, 전체 접속기록 2억 261만 2,768건의 81%에 해당되는 1억 6,504만 9,639건의 접속 실패기록이 확인됨) 이상행위를 쉽게 발견할 수 있었다.

또한, 피심인은 2016. 11.경 해커의 사전대입 공격을 통해 이미 이 사건 해커의 이러한 공격 수법을 알고 있었음에도 불구하고 2017. 9.까지 침입탐지시스템 등의 로그를 확인하지 않는 등 신규 위협 대응, 정책 설정 운영(신규 위협 대응

등을 위하여 접근제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영・관리), 이상 행위 대응(모니터링 등을 통해 인가받지 않은 점근을 제한하거나 인가자의 비정상적인 행동에 대응), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 차단) 등의 방법을 활용하여 접근 제한 및 유출 탐지기능이 충족되도록 체계적으로 운영・관리하지 않아 2017. 2. 9.부터 9. 25.까지 발생한 사전 대입공격을 탐지하지 못하였으므로 침입탐지시스템을 '운영'하였다고 볼 수 없다.

아울러 피심인은 이 사건 해커가 접속한 '알툴바' 웹페이지나 웹서버는 개인정보처리스템에 해당하지 않으므로 침입탐지시스템 설치・운영이 문제가 되지 않는다고 주장하고 있으나,고시 제2조 제4호는 "개인정보처리시스템이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

"라고 규정하고 있는바, 피심인의 웹사이트 또는 알툴바 프로그램은 이용자의 개인정보가 저장된 데이터베이스와 연결되어 정당한 권한을 가진 이용자가 접속하는 경우 이용자의 개인정보를 DB에서 불러와 조회할 수 있도록 피심인이 체계적으로 구성한 개인정보처리시스템에 해당하고, 결과적으로 침입차단시스템을 접근 제한 및 유출 탐지 기능이 충족되도록 체계적으로 운영・관리하였다면 이 사건 해킹을 방지할 수 있었다는 사실에는 변함이 없다.

결국 '개인정보처리시스템'은 개인정보의 생성, 기록, 저장, 검색, 이용과정 등 데이터베이스 시스템 전체를 의미하는 것으로, 데이터베이스와 연결되어 개인정보의 처리 과정에 관여하는 웹 서버 등을 포함하는 개념으로 보아야 하고, 고시 제4조 제5항에 정한 '시스템 설치・운영'의 의미는 이러한 개인정보처리시스템에 대한 불법적인 접근을 막고 불법적인 개인정보 유출 시도를 탐지하는 기능을 갖춘 상용화되고 인증된 설비를 설치・운영하는 것을 의미한다고 할 것이다.

따라서, 피심인은 개인정보를 처리할 때에는 개인정보의 분실・도난・유출・변조 또는 훼손을 방지하기 위하여 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치・운영하여야 하나, 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하지 않았으며, 2016. 11.경 해커의 사전대입 공격이 있었음을 알고도 부정 접속이 의심되는 이용자에게 비밀번호 변경 안내만 하였을 뿐, 신규 위협 대응, 정책 설정 운영, 이상 행위 대응, 로그 분석 등의 방법을 활용하여 접근 제한 및 유출 탐지 기능이 충족되도록 침입탐지시스템 등을 체계적으로 운영・관리하지 않아 2017. 2. 9.부터 9. 25.까지 발생한 사전대입 공격을 탐지하지 못하는 등 침입차단 및 탐지시스템을 소홀히 설치・운영 함으로써 정보통신망법 제28조 제1항 제2호(기술적・관리적 보호조치 중 접근통제), 같은 법 시행령 제15조 제2항, 고시 제4조 제5항을 위반하였다.

▲ '알패스' 서비스 이용자 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치하지 않은 행위(이 사건 제2 처분사유)고시 제14조 제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다"라고 규정하고 있다.

피심인은 2016. 11.경 알툴바 해킹 의심 관련 게시글을 확인한 후, 알툴즈 서버의 접속기록을 분석하여 알패스 서비스에 봇을 이용한 대량의 아이디, 비밀번호를 대입하는 사전대입 공격을 인지하였다.

그러나 피심인은 해커가 알패스 서비스의 아이디, 비밀번호를 취득하는 경우 이용자에게 심각한 2차 피해가 발생할 수 있음을 알면서도, 당시 사전대입 공격으로 부정한 접속 성공이 의심되는 계정 이용자 384,758명에게 비밀번호 변경

안내 메일을 발송한 것 외에 해당 이용자의 비밀번호 초기화, 접속차단 등의 조치를 하지 않아 이 중 155,049명의 이용자는 2차 사전대입 공격으로 알패스 정보(외부사이트 도메인, 아이디, 비밀번호)가 유출되었다.

또한, 봇을 이용한 공격을 방지하기 위한 캡차 및 추가적 인증수단 등을 적용하는 조치를 취하지 않아, 해커의 2017. 2. 9.부터 2017. 9. 25.까지의 사전대입 공격에서 알패스 이용자 정보(외부사이트 도메인, 아이디, 비밀번호)가 알툴바 서비스를 통하여 외부로 유출되는 사고를 방지하지 못한 사실이 있다.

이에 대하여 피심인은 고시 제4조 제9항은 정보통신서비스제공자의 부주의로 개인정보가 노출되는 것을 방지하기 위한 규정으로, 이 사건은 2016. 11.경 해커가 불상의 방법으로 취득한 아이디/비밀번호로 대량접속시도를 하는 사전대입 공격으로 피심인의 내부적인 부주의나 과실로 개인정보가 외부에 공개되거나 유출된 것이 아니므로 고시 제4조 제9항이 적용되지 않는다고 주장하고 있다.

개인정보의 기술적·관리적 보호조치 기준 제4조 제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다"라고 규정하고 있는바, 이는 인터넷 홈페이지를 통해 개인정보가 외부로 유출되는 것을 방지하기 위한 조치로 피심인의 주장과 같이 내부적인 부주의로 인한 개인정보의 노출방지로 한정되는 규정이 아니다.

또 피심인은 2016.경에 있었던 공격은 같은 IP주소로 동일 계정으로 접근을 시도하는 단순한 방식이었기 때문에 알패스 단독제품을 종료하는 것으로 충분한 조치를 취한 것이었으나, 실제 유출이 일어난 2017.경의 공격은 단순한 사전대입 공격이 아니라, IP주소를 계속하여 자동으로 바꾸고 접속 시도가 실패할 경우 다른 계정으로 접근을 시도하는 등 다른 기술에 의하여 발생하였다고 주장하나,피심인이 제출한 2016. 11. 8. 개발부문 부문장의 내부 점검 결과 공유 메일에는 "1~2개 IP는 아니고 여러 IP로 알패스 웹서비스를 가지고 지속적으로 요청", "아마 지속적으로 IP를 바꿔서 접속 시도를 할 것으로 생각된다"는 등의 내용이 담겨 있는 것으로 볼 때 피심인의 주장은 근거가 없다.

또한 , 피심인은 2016. 11.경 부정접속이 의심되는 사례가 발생한 후 알패스 단독제품을 종료하고, ① 5회 이상 로그인에 실패할 경우, 5분 동안은 정상적인 로그인까지 차단하는 조치를 취하였고, ② 동일한 IP로 1시간 내에 500회 이상 로그인 시도 시 로그인을 임시차단하고, 임시차단이 된 이후에도 1시간 동안 5,000회 이상 로그인을 시도하는 경우 블랙리스트로 자동 등록하여 접근 차단한 후 관리자가 수동으로 해제하여야만 접속이 가능하도록 조치하였으며, ③ 1회라도 공격시도를 한 IP주소 및 KISA에서 차단 권고한 IP주소는 모두 블랙리스트에 등록하여 접속을 차단하는 등 알패스 서비스의 보안을 강호하는 조치를 취하였다고 소명하고 있다.

이 중 피심인이 취한 ①의 조치는 단순히 이용자가 비밀번호를 5회 이상 실패할 경우 차단하는 조치이고, ③의 조치는 단순 위험 IP에 대한 차단조치에 불과하므로 2016. 11.경 인지한 다수의 아이디, 비밀번호를 이용한 사전대입 공격을 방어하기 위한 조치로 볼 수 없다.

피심인이 취한 ②의 조치의 경우에도 조사 당시 피심인으로부터 제출받은 접속기록을 분석한 결과, 2017. 1. 7. 20:00:38부터 20:59:28까지 (IP 주소 7 생략) IP에서 1,644번의 접속시도가 있었음에도 해당 IP가 차단되지 않은 것이 확인이 되므로 피심인이 주장하는 조치가 적용되었다고 볼 수 없을 뿐만 아니라 이러한 조치가 봇을 이용한 사전대입 공격을 근본적으로 차단하는 조치도 될 수 없다.

대법원 판례에서는, "특정 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 조치를 취하여야할 법률상 의무를 위반하였는지 여부를 판단함에 있어서는 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술수준, 정보통

신서비스 제공자의 업종・영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피가능성 등을 종합적으로 고려하여 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부가 기준이 된다"고 판시하였다.

피심인은 알약 등 백신을 판매하는 국내 대표적인 보안업체로 2016년 매출액이 205억 원이고, 2017년 9월 기준 개인정보를 보관하고 있는 건수가 200만 명 이상으로 일정규모 이상의 사업자에 해당하며, 제공하는 알패스 서비스는 이용자가 이용하는 외부사이트의 아이디, 비밀번호를 관리해주는 서비스로 보관 중인 정보가 수천만 건에 이르며, 이러한 이용자의 비밀정보, 민감한 정보, 금전적 피해를 줄 수 있는 정보를 해커가 취득하는 경우 이용자에게 심각한 2차 피해가 발생할 수 있어 다른 어떤 서비스보다 보안을 철저히 할 필요가 있다.

'모든' 해커의 공격에 따른 개인정보 유출이 발생하지 않도록 조치를 하는 것은 현실적으로 불가능하나, 피심인은 적어도 2016. 11.경 봇을 이용한 사전대입 공격으로 이에 대한 수법을 인지하였으므로 부정한 접속 성공이 의심되는 계정에 대해서는 비밀번호 초기화 또는 접속차단 조치를 통해 추가로 발생할 수 있는 이용자의 피해를 최소화하고, 캡차 및 추가적인 인증 등을 적용하는 조치를 통해 또 다시 발생할 수 있는 봇에 의한 사전대입 공격을 차단할 수 있도록 하였어야 한다.

이러한 부정한 접속 성공이 의심되는 계정에 대한 비밀번호 초기화, 접속차단조치를 통해 또다시 부정한 접속으로 인한 추가적인 개인정보 유출을 방지하는 것과 캡차 및 추가적인 인증 등을 적용하는 조치를 통해 봇에 의한 자동화된 사전대입 공격을 방지하는 것은 누구나 생각할 수 있는 보편적으로 알려져 있는 정보보안 기술수준이고, 이를 조치하는데 비용이 발생하지도 않으며(캡차는 무료로도 제공됨), 적용 시 피해발생이 줄어들 수 있는 등 사회통념상 합리적으로 기대 가능한 정도의 보호조치에 해당한다.

따라서 피심인은 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 하나, 2016. 11.경 알패스 서비스에 사전대입 공격이 있었음을 인지한 이후에도 이용자의 비밀번호를 보관하는 알패스 서비스 특성상 해커가 알패스 이용자의 타 사이트, 아이디, 비밀번호를 취득하는 경우 이용자에게 심각한 피해가 발생할 수 있음을 알면서도, 부정 접속된 이용자의 비밀번호 초기화, 접속차단 등의 조치를 하지 않고, 봇을 이용한 사전대입 공격을 방지하기 위한 캡차 또는 추가적 인증수단 적용 등의 조치를 취하지 않아 알패스 이용자 정보가 알툴바 서비스를 통하여 외부로 유출되게 함으로써 정보통신망법 제28조 제1항 제2호(기술적・관리적 보호조치 중 접근통제), 같은 법 시행령 제15조 제2항, 고시 제4조 제9항을 위반하였다.

일정 규모 이상 사업자

2) 피고와 한국인터넷진흥원이 2017. 12. 발간한 개인정보의 기술적・관리적 보호조치 기준 해설서(이하 '이 사건 보호조치 고시 해설서'라 한다)의 주요 내용은 아래와 같다.

■ 개인정보처리 시스템 관련 ◎ 이 사건 보호조치 기준 제2조 제4항: '개인정보처리시스템'이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.

● 여기서 말하는 데이터베이스시스템이란 일반적으로 데이터가 저장되는 데이터베이스(DB)와 데이터베이스 내의 데이터를 처리할 수 있도록 해주는 데이터베이스 관리 시스템(DBMS) , 응용프로그램 등이 통합된 것을 의미한다.

● 따라서 개인정보처리 시스템에는 개인정보가 저장되는 데이터베이스(DB) , 데이터 베이스를 생성하고 관리하는 데이터베이스 관리 시스템(DBMS) , 데이터베이스를 용이하게 이용하는데 필요한 응용프로그램 등 데이터베이스시스템의 구성요소가 모두 포함된다.

● 개인정보처리시스템은 정보통신서비스 제공자등의 개인정보 처리 방법, 시스템 구성 및 운영 환경 등에 따라 달라질 수 있다.

개인정보처리시스템(예시) ☞ 응용프로그램(Web 서버, WAS 등) 등을 데이터베이스의 개인정보를 처리할 수 있도록 구성한 때■ 접근통제 조치 관련 ◎ 이 사건 보호조치 기준 제4조 제5항: 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 ● 정보통신서비스 제공자등은 불법적인 접근 및 침해사고 방지를 위해 다음과 같은 시스템 등을 스스로의 환경을 고려하여 접근 제한 기능 및 유출 탐지 기능이 적합하게 수행되도록 설치・운영하여야 한다.

참고 ☞ 불법적인 접근: 인가되지 않은 자(내・외부자모두 포함)가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말한다.

☞ 침해사고: 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(정보통신망법 제2조). - 해당 시스템으로는 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제 (Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있다.

다만, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 한다.

- SOHO 등 소기업은 인터넷데이터센터(IDC), 클라우드 서비스 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를 활용하거나 공개용(무료) S/W를 사용하여 해당 기능을 구현한 시스템을 설치・운영할수 있다.

다만, 공개용(무료) S/W를 사용할 때에는 적절한 보안이 이루어지는지를 사전에 점검할 필요가 있다.

참고 ☞ 보안제품 등을 도입할 때에는 IT보안인증사무국(http://www.itscc.kr)에서 제공하는 인증제품 목록(제품유형 : 개인정보보호, DB접근통제, 통합로그관리 등) 등을 활용할 수도 있다.

● 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 다음과 같은 방법 등을 활용하여 체계적으로 운영・관리하여야 한다.

- 정책 설정 운영: 신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영・관리 - 이상 행위 대응: 모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응 이상 행위 대응(예시) ☞ 동일 IP, 해외 IP 주소에서의 과도한 또는 비정상적인 접속시도 탐지 및 차단 조치 ☞ 개인정보처리시스템에서 과도한 또는 비정상적인 트래픽 발생 시 탐지 및 차단 조치 등 - 로그 분석: 로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단 참고 ☞ '로그'는 침입차단시스템 또는 침입탐지시스템의 로그기록에 한정하지 않고 개인정보처리시스템의 접속기록, 네트워크 장비의 로그기록, 보안장비소프트웨어의 기록 등을 포함 ● IP주소 등에는 IP주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)를 포함한다.

◎ 이 사건 보호조치 기준 제4조 제9항: 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

● 인터넷 홈페이지를 통한 개인정보 유·노출 방지 조치 - 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안 기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 한다.

참고 ☞ 인터넷 홈페이지를 통한 개인정보 유·노출 유형 * 검색엔진(구글링 등) 등을 통한 개인정보 유·노출 * 웹 취약점을 통한 개인정보 유·노출 * 인터넷 게시판을 통한 개인정보 유·노출 * 홈페이지 설계·구현 오류로 인한 개인정보 유·노출 * 기타 방법을 통한 개인정보 유·노출 - (보안대책 마련) 인터넷 홈페이지 설계 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하여야 한다.

보안대책 (예시) ☞ 입력 데이터의 유효성을 검증 ☞ 인증, 접근통제 등의 보호조치 적용 ☞ 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성 ☞ 세션을 안전하게 관리하도록 구성 등- (보안 기술 적용) 인터넷 홈페이지 개발 시 개인정보 유·노출 방지를 위한 보안 기술을 적용하여야 한다.

보안 기술 적용 (예시) ☞ 홈페이지 주소(URL), 소스코드, 임시 저장 페이지 등에 개인정보 사용 금지 ☞ 홈페이지에 관리자 페이지의 주소 링크 생성 금지, 관리자 페이지 주소는 쉽게 추측하기 어렵도록 생성, 관리자 페이지 노출 금지 ☞ 엑셀 파일 등 숨기기 기능에 의한 개인정보 유·출 금지 ☞ 시큐어 코딩(secure coding) 도입 ☞ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치 ☞ 인증 우회(authentication bypass)에 대비하는 조치 등 - (운영 및 관리) 인터넷 홈페이지 운영·관리 시 개인정보 유·노출방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다.

운영 및 관리 (예시) ☞ 인터넷 홈페이지 등에 보안대책을 정기적으로 검토 ☞ 홈페이지 게시글, 첨부파일 등에 개인정보 포함 금지, 정기적 점검 및 삭제 등의 조치 ☞ 서비스 중단 또는 관리되지 않는 홈페이지는 전체 삭제 또는 차단 조치 ☞ 공격패턴, 위험분석, 침투 테스트 등을 수행하고 발견되는 결함에 따른 개선 조치 ☞ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치 등

[인정근거] 다툼 없는 사실, 갑 제1호증, 을 제10호증의 각 기재, 변론 전체의 취지

라. 판단

1) 침입행위 관련 주장에 관한 판단

가) 구 정보통신망법 제28조 제1항은 '정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다'고 규정하면서 제2호에서 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영'을 규정하고 있고, 제64조 제4항 본문은 '방송통신위원회는 이 법을 위반한 정보통신서비스 제공자등에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자등에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다'고 규정하며, 제64조의3 제1항은 '방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금

으로 부과할 수 있다'고 규정하면서 제6호에서 '이용자의 개인정보를 분실・도난・유출・위조・변조 또는 훼손한 경우로서 제28조 제1항 제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 조치를 하지 아니한 경우'를 규정하고 있고, 제48조 제1항은 '누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다'고 규정하고 있다.

나) 살피건대, 구 정보통신망법 제64조 제4항 및 제64조의3 제1항에 따른 시정명령 및 그에 대한 공표조치나 과징금 부과는 침입행위가 아닌 이용자의 개인정보를 분실・도난・유출한 경우 등을 요건으로 하고 있어 침입행위가 존재하지 아니하였다는 사정만으로 이 사건 각 처분이 위법하다고 볼 수 없다.

설령 침입행위가 필요하다고 하더라도 위와 같은 규정에다가 위 인정사실 및 변론 전체의 취지에 의하여 인정되는 다음과 같은 사정 즉, ① 이 사건 해커는 이 사건 회원정보를 유출하기 위한 목적에서 2017. 6. 2.부터 2017. 9. 12.까지 3개월 동안 '알툴바' 서비스에 총 2억 261만 2,768건의 접속시도를 하였고, 그 중 접속 실패 건수는 1억 6,504만 9,639건(약 81%)이므로 정상적인 접속시도라고 보기 어려운 점, ② 이러한 해커의 접속은 정보통신서비스를 제공받는 이용자(구 정보통신망법 제2조 제1항 제4호)의 의사에 반하여 이루어진 것으로 이 사건 해커가 접속에 관한 정당한 권한을 가진 것으로 보기 어려운 점, ③ 개인정보의 유출을 방지할 의무가 있는 정보통신서비스 제공자인 원고(구 정보통신망법 제28조 제1항)도 개인정보 유출목적을 가진 이 사건 해커의 접근을 허용하여서는 아니되는 점 등을 종합하여 보면, 이 사건 해커가 사전대입 공격을 통하여 개인정보에 접근한 행위는 침입행위에 해당한다고 봄이 상당하다.

따라서 원고의 이 부분 주장은 이유 없다.

2) 이 사건 제1 처분사유 관련

가) 개인정보처리시스템 해당 여부

(1) 구 정보통신망법 제28조 제1항 제2호, 정보통신망법 시행령 제15조 제2항 제2호에 의하면, 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 대한 '침입차단시스템' 및 '침입탐지시스템'을 설치・운영하여야 한다.

정보통신망법 시행령 제15조 제2항 제1호 및 이 사건 보호조치 기준 제2조 제4호는 개인정보처리시스템에 관하여 '개인정보처리시스템이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다'고 규정하고 있다.

한편 이 사건 보호조치 고시 해설서는 '일반적으로 체계적인 데이터 처리를 위해 DBMS(Database Management System)를 사용하고 있으나, 이용자의 개인정보 보관・처리를 위해 파일처리시스템 등을 구성한 경우 개인정보처리시스템에 포함시키는 것이 타당하다'고 설명하고 있다.

(2) 위와 같은 규정에다가 위 인정사실 및 변론 전체의 취지에 의하여 인정되는 아래와 같은 사정을 종합하여 보면, 이 사건 프로그램이나 웹서버 역시 개인정보처리가 이루어지는 시스템 즉, 개인정보처리시스템에 해당한다고 봄이 상당하다.

따라서 원고의 이 부분 주장은 이유 없다.

① 개인정보란 생존하는 개인에 관한 정보로서 성명・주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호・문자・음성・음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여

알아볼 수 있는 경우에는 그 정보를 포함한다)를 말하고(구 정보통신망법 제2조 제1항 제6호), 개인정호의 처리란 '개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위'를 말하며(구 정보통신망법 제25조 제1항 참조), 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실・도난・유출・위조・변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치・운영의 기술적・관리적 조치를 하여야 한다(구 정보통신망법 제28조 제1항 제2호).

한편 이를 구체화한 정보통신망법 시행령 제15조 제2항 제2호는 '법 제28조 제1항 제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치・운영의 조치를 하여야 한다'고 규정하고 있고, 여기에서 말하는 개인정보처리시스템은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템이다(정보통신망법 시행령 제15조 제2항 제1호).

결국 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치・운영의 목적은 개인정보처리시스템에 존재하는 개인정보의 분실・도난・유출 등을 방지하고 개인정보에 대한 불법적인 접근을 차단하기 위함이다.

② 한편 이용자에 대한 개인정보가 망분리의 구조상 내부의 데이터베이스 서버에 위치한다고 하더라도 이용자에 대한 개인정보의 출력은 ㉠ 이용자의 로그인, ㉡ 로그인 정보의 웹서버 전송, ㉢ 웹서버의 웹 어플리케이션을 통한 데이터베이스서버의 개인정보 요청, ㉣ 데이터베이스서버의 웹 어플리케이션을 통한 개인정보의 웹서버 제공, ㉤ 웹서버로 전송된 개인정보의 화면 출력의 단계로 이루어진다.

개인정보의 처리는 개인정보의 수집이나 제공을 포함하는데, ㉠ 이용자의 개인정보의 제공과 이에 따른 수집이나 이용자에 대한 개인정보의 제공은 데이터베이스서버 내부에서 이루어지는 것이 아니고 웹서버 전송을 통하여 이루어지는 점, ㉡ 개인정보의 보호조치는 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치・운영'에 관한 조치를 포함하는데(구 정보통신망법 제28조 제1항 제2호 참조), 개인정보에 대한 불법적인 접근의 유형은 내부망에 바로 침입하는 유형 이외에도 정당한 권한에 기하지 않은 이용자의 아이디와 패스워드를 사용한 유형도 존재할 수 있는 점, ㉢ 개인정보의 처리에 있어서는 앞서 본 바와 같이 웹서버, 웹 어플리케이션, 데이터베이스서버가 모두 필수적인바, 내부의 데이터베이스 서버만을 개인정보처리시스템이라고 해석하기 어렵고, 데이터베이스서버 단독으로 이용자의 개인정보를 수집하는 것은 이용자가 직접 데이터베이스서버에 접속할 수 없어 불가능한 점 등을 종합하면, 개인정보처리시스템이란 웹서버나 웹 어플리케이션을 포함하는 의미로 해석함이 상당하다.

③ 이 사건 회원정보는 이 사건 해커가 해킹프로그램인 '알패스(Alpass) 3.0.exe'와 사전에 대량으로 확보한 이용자의 아이디, 비밀번호를 이용하여 이용자가 알툴바에 접속하는 경우와 유사하게 알툴바서버에 접속하여 유출되었는바, ㉠ 원고의 개인정보의 수집은 이용자가 알툴바에 접속하여 정보를 제공하면서 이루어지는 점, ㉡ 이용자가 알툴바에 접속하여 이용자의 개인정보를 수정할 수 있었고 수정된 정보 역시 알툴바서버에 저장되는 점, ㉢ 망분리된 알툴바서버가 독자적으로 개인정보를 수집한다는 것은 상정하기 어려운 점 등을 종합하여 보면, 이 사건 프로그램 내지 알툴바는 개인정보처리시스템에 해당한다고 봄이 상당하다.

나) 침입차단・침입탐지시스템 설치・운영의무 준수 여부

(1) 구 정보통신망법 제28조 제1항 제2호, 정보통신망법 시행령 제15조 제2항 제2호에서 요구하는 개인정보에 대한 불법적인 접근을 차단하기 위한 필요한 조치와 관련하여, 이 사건 보호조치 기준 제4조 제5항은 '정보통신서비스 제공자 등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치·운영하여야 한다'고 규정하고 있다.

한편 정보통신서비스가 '개방성'을 특징으로 하는 인터넷을 통하여 이루어지고 정보통신서비스 제공자가 구축한 네트워크나 시스템과 그 운영체제 등은 불가피하게 내재적인 취약점을 내포하고 있어서 이른바 '해커' 등의 불법적인 침입행위에 노출될 수밖에 없고, 완벽한 보안을 갖춘다는 것도 기술의 발전 속도나 사회 전체적인 거래비용 등을 고려할 때 기대하기 쉽지 않다.

또한 해커 등은 여러 공격기법을 통해 정보통신서비스 제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스 제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입행위를 방지하기 위한 보안기술은 해커의 새로운 공격방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적이다.

이처럼 정보통신서비스 제공자가 취해야 할 개인정보의 안전성 확보에 필요한 보호조치에 관해서는 고려되어야 할 특수한 사정이 있다.

그러므로 정보통신서비스 제공자가 구 정보통신망법 제28조 제1항, 정보통신망법 시행령 제15조 제2항 제2호에 규정된 보호조치를 이행하였는지 여부를 판단함에 있어서는, 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다(대법원 2018. 1. 25. 선고 2014다203410 판결 등 참조).

(2) 위와 같은 법리에다가 위 인정사실, 갑 제2호증, 을 제9호증의 각 기재 및 변론 전체의 취지에 의하여 인정되는 아래와 같은 사정을 종합하여 보면, 원고는 사회통념상 합리적으로 기대 가능한 정도의 침입차단·침입탐지시스템 설치·운영의무를 준수하지 않았다고 봄이 상당하다.

따라서 원고의 이 부분 주장은 이유 없다.

(가) 침입차단·침입탐지시스템 설치의무 관련

① 이 사건 보호조치 기준은 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 하는데(제1조 제1항 참조), 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치하여야 한다(제4조 제5항 참조).

② 한편 위와 같은 침입차단・탐지시스템의 설치에 관하여 필요한 조치를 이행하였는지는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종・영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 그 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여야 한다.

이 사건에 있어서 ㉠ 개인정보가 저장・관리되고 있는 원고의 이용자 수가 100만 명 이상인 점, ㉡ 이용자가 알패스에 등록한 중요정보(외부 사이트, 아이디, 비밀번호)가 수천만 건 이상인 점, ㉢ 전년도 정보통신서비스 부문 매출액이 100억 원 이상인 점, ㉣ 원고가 수집・보관 중인 이용자의 알패스 개인정보는 이용자가 다른 사이트를 이용하기 위한 비밀번호로 유출시 이용자가 입게 되는 피해의 정도가 매우 심각한 점 등에 비추어 보면 원고로서는 일반적인 개인정보를 처리하는 정보통신서비스 제공자 보다 개인정보 보호조치를 강화할 필요가 있다고 할 것이다.

③ 원고는 오픈소스(Snort)를 이용한 침입탐지만을 적용하였고, 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었으나, 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템 등의 보안장비를 도입하여 운영한 사실은 없었는바, 원고가 침입차단・침입탐지시스템 설치와 관련한 조치를 이행하였다고 보기는 어렵다고 할 것이다.

④ 원고는 이에 대하여 iptables, Webknight, Snort는 보안성이 입증되어 널리 사용된 침입차단・침입탐지시스템이라고 주장한다.

그러나 뒤에서 보는 바와 같이 원고가 iptables, Webknight, Snort와 같은 시스템을 사용하여 로그기록을 분석 및 이에 기초한 이상접속에 대하여 접속차단 등의 조치가 이루어지지 않은 이상 개인정보 보안조치 중 하나인 침입차단・침입탐지시스템을 설치하였다고 볼 수 없어 원고의 위 주장은 받아들이기 어렵다.

(나) 침입제한・침입탐지시스템 운영의무 관련

① 침입제한・침입탐지시스템은 사전에 정해진 규칙에 따라 차단・탐지하는 시스템으로 위와 같은 시스템의 운영은 정보통신망을 통한 불법적인 접근 및 침해사고 방지에 필요한 기능을 활용하는 것을 의미하고, 이와 같은 기능을 활용하기 위하여는 침입 차단 정책을 설정한 후 침입탐지 로그 분석 등과 같은 시스템의 운영이 필수적이라고 할 것이다.

② 이 사건에 있어서 이 사건 해커는 IP를 변경하며 봇(bot)을 이용한 사전대입 공격으로 이 사건 회원정보를 유출하였는바, 이 사건 해커의 2017. 6. 2.부터 2017. 9. 25.까지 사전대입 공격 기록에 의하면, 총 접속기록 2억 261만 2,768건의 대량접속 시도가 있었을 뿐만 아니라 그 중 81%에 해당되는 1억 6,504만 9,639건의 접속 실패기록이 확인되었다.

이러한 이상 접속은 원고가 로그기록을 확인하였다면 해커의 침입을 쉽게 확인할 수 있었을 것으로 보인다.

특히 원고는 2016. 11.경 해커의 사전대입 공격을 받아 공격 방법을 알고 있었음에도 불구하고 침입탐지시스템 등의 로그를 확인하지 않은 것으로 보이므로, 접근 제한 및 유출 탐지기능을 체계적으로 운영・관리함으로써 침입탐지시스템을 운영하였다고 할 수 없다.

③ 원고는 이에 대하여 이글루시큐리티와 보안관제서비스 계약을 하여 침입차단 및 탐지시스템의 로그들을 24시간 관제하는 기능을 운영하였다고 주장한다.

그러나 원고가 로그분석 등을 통하여 실질적으로 침입차단시스템을 운영하였다거나 이용자의 개인정보 보호를 위하여 동일 IP의 접속을 제한하는 등의 조치를 취하였다고 인정할 구체적 자료가 없으므로, 위 주장은 받아들이기 어렵다.

3) 이 사건 제2 처분사유 관련

가) 이 사건 보호조치 기준 제4조 제9항 적용 여부

(1) 구 정보통신망법 제28조 제1항 제2호, 정보통신망법 시행령 제15조 제2항 제5호에서 요구하는 개인정보에 대한 불법적인 접근통제를 위해 필요한 조치와 관련하여, 이 사건 보호조치 기준 제4조 제9항은 '정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다'고 규정하고 있다.

(2) 위와 같은 규정에다가 위 인정사실 및 변론 전체의 취지에 의하여 인정되는 다음과 같은 사정 즉, ① 이 사건 보호조치 기준은 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 하는 것으로(제1조 제1항), 이 사건 보호조치 기준 제4조 제9항도 정보통신서비스 제공자등의 최소한의 기술적·관리적 보호조치를 정하고 있는 것으로 보아야 하는 점, ② 이 사건 보호조치 기준 제4조 제9항은 정보통신서비스 제공자등이 취급하는 개인정보가 유출되는 방법을 인터넷 홈페이지, P2P, 공유설정 등이라고 규정하고 있는데 이를 내부적 요인에 따라 개인정보가 유출된 경우에만 위 기준을 적용하겠다는 취지로 보기 어려운 점, ③ 이 사건 보호조치 기준 제4조 제9항도 제1항 내지 제5항 등과 마찬가지로 개인정보처리시스템의 접근통제를 위한 규정으로서 외부의 접근에 따른 개인정보 유출을 방지할 필요성이 있는 점 등을 종합하여 보면, 위 규정을 내부적인 부주의로 인한 개인정보의 노출방지만을 위한 규정으로 한정하여 해석할 수 없다.

따라서 원고의 이 부분 주장은 이유 없다.

나) 원고의 개인정보 노출방지 조치 시행 여부

(1) 이 사건 보호조치 기준 제4조 제9항에 규정된 정보통신서비스 제공자등이 개인정보 유출방지를 위한 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하였는지 여부는 정보통신서비스 제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다(대법원 2018. 1. 25. 선고 2014다203410 판결 등 참조).

(2) 위와 같은 법리에다가 위 인정사실, 을 제8호증의 기재 및 변론 전체의 취지에 의하여 인정되는 아래와 같은 사정을 종합하여 보면, 원고가 개인정보처리시스템의 컴퓨터에 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 하였다고 볼 수 없다.

따라서 원고의 이 부분 주장은 이유 없다.

① 앞서 본 바와 같이 원고는 100만 명 이상의 이용자에 대한 개인정보를 저장·관리하고 있었던 점, 알패스에 등록된 중요정보가 수천만 건 이상이었으며, 정보통신서비스 매출은 100억 원 이상인 점, 알패스 개인정보의 중요성 등에 비추어 보면, 이 사건의 경우 원고에게 요구되는 사회통념상 합리적으로 기대 가능한 정도의 보호조치는 일반적인

정보통신서비스 제공자보다 높다고 할 것이다.

② 앞서 본 바와 같이 원고가 사회통념상 합리적으로 기대되는 전문적인 침입차단・탐지시스템을 설치・운영하였다고 할 수 없는 이상, 개인정보처리시스템의 컴퓨터에 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 하였다고 볼 수 없다.

③ 이에 대하여 원고는, 사전대입 공격이 이루어진 후 부정접속이 의심되는 계정의 이용자들에게 비밀번호 변경을 요청하였고, 2016. 11.경 알패스 단독프로그램의 운영을 종료하였으며, 알툴바를 통한 알패스 서비스의 제공에 있어서도 5회 이상 로그인에 실패할 경우 5분 동안 정상적인 로그인을 차단하는 조치나 동일한 IP로 1시간 내에 500회 이상 로그인 시도 시 로그인을 임시차단하고, 임시차단이 된 이후에도 1시간 동안 5,000회 이상 로그인을 시도하는 경우 블랙리스트로 자동등록하여 접근을 차단하였으며, 1회라도 공격을 한 IP주소 등을 블랙리스트에 등록하였고, 유료 방화벽인 시큐아이 MF2-6000을 도입하여 분석된 시간별로 IP를 분석하여 이상이 발생하는 경우 경보알림을 받는 등으로 개인정보 노출방지를 위한 조치를 시행하였다고 주장한다.

그러나 ㉠ 사전대입 공격을 방지하기 위한 조치란 해커 등이 이용자의 개인정보를 탈취하여 비밀번호에 사용될 문구들을 대입한 로그인 시도를 방지하기 위한 조치인바, 원고가 부정접속 의심자에게 비밀번호의 변경을 요청하거나 알패스 단독프로그램의 운영을 종료하였더라도 사전대입 공격을 방지하기 위한 조치라고 할 수 없는 점, ㉡ 5회 이상 로그인에 실패할 경우 5분 동안 정상적인 로그인을 차단하는 조치를 취하였다고 하더라도 원고가 관리하는 정보의 중요성에 비추어 볼 때 계정 비밀번호의 초기화 등이 이루어지지 않는 이상 사전대입 공격을 차단하기 위한 충분한 조치로 보기는 어려운 점, ㉢ 원고가 동일한 IP로 500회 등 접속하는 경우 로그인을 차단하는 조치나 임시차단 이후 5,000회 이상 로그인을 시도하는 경우 블랙리스트로 등록하여 접근을 차단하는 조치를 하였다고 인정할 증거는 없고 오히려 2017. 1. 7. 20:00부터 20:59까지 동일한 IP에서 1,644번의 접속시도가 있었음에도 접속차단이 이루어지지 않은 점, ㉣ 원고가 공격을 시도한 IP의 접속을 차단하였다고 하더라도 원고는 2016. 11.경 사전대입 공격이 특정 IP를 근거로 한 것이 아니라 여러 IP를 통하여 접근한 것을 인지하고 있었으므로(을 제8호증 제7쪽), 이는 다수의 IP를 이용한 사전대입 공격을 방어하기 위한 조치로 볼 수 없는 점, ㉤ 나아가 원고가 2016. 11.경 봇을 이용한 사전대입 공격을 인지하고 있었고, 사전대입 공격을 통하여 이용자의 패스워드가 유출되는 경우 단순한 개인정보의 노출을 넘어 금전적인 피해까지 이용자가 입게 될 가능성이 있는 이상, 원고는 2016. 11.경 이후에는 부정한 접속 성공이 의심되는 계정에 대해서는 비밀번호 초기화 또는 접속차단 조치를 통해 추가로 발생할 수 있는 이용자의 피해를 최소화하고, 알패스의 로그인에 있어서는 캡차 및 추가적인 인증 등을 적용하는 조치를 통하여 봇에 의한 사전대입 공격을 차단할 수 있는 조치 등을 취하였어야 한다고 봄이 상당한 점 등에 비추어 보면, 원고의 위 주장은 받아들이기 어렵다.

3. 결론

그렇다면 원고의 청구는 이유 없으므로 이를 모두 기각하기로 하여 주문과 같이 판결한다.

(별지 생략)

판사 이정민(재판장) 김주성 차선영