시정조치등취소청구

[서울고등법원 2020. 11. 4. 2019누43964]

【전문】

【원 고】 주식회사 이스트소프트(소송대리인 법무법인(유한) 세종 담당변호사 김용호 외 3인)

【피 고】 개인정보 보호위원회(경정 전 방송통신위원회)(소송대리인 법무법인 인 담당변호사 권창범 외 1인)

【제1심판결】 서울행정법원 2019. 4. 25. 선고 2018구합65682 판결

【변론종결】2020. 10. 7.

【주문】

】

1. 피고가 2018. 3. 28. 원고에 대하여 한 별지1 처분 내역 제1 내지 3항 기재 시정조치, 공표명령 및 제4의 가항 기재 과징금 부과처분 중 별지2 처분 내역 기재 시정조치 및 공표명령 부분을 초과하는 부분을 취소한다.

2. 원고의 나머지 청구를 기각한다.

3. 소송비용 중 70%는 원고가, 나머지는 피고가 각 부담한다.

【청 구 취 지】피고가 2018. 3. 28. 원고에 대하여 한 별지1 처분 내역 제1 내지 3항 기재 시정조치, 공표명령 및 제4의 가항 기재 과징금 부과처분을 모두 취소한다(원고는 당초 방송통신위원회를 피고로 삼아 2018. 3. 28.자 별지1 처분 내역 제1 내지 3항 기재 시정조치, 공표명령 및 제4의 가항 기재 과징금 부과처분의 취소를 구하는 소를 제기하였는데, 방송통신위원회는 2020. 9. 11. 이 법원에서 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무가 피고에게 승계되었음을 이유로 행정소송법 제14조 제6항, 제13조 제1항 단서에 따라 피고경정신청을 하였고, 이 법원은 2020. 9. 14. 피고경정신청을 허가하였다. 행정소송법 제14조 제6항, 제4항, 제5항, 제13조 제1항 단서에 의하면, 피고경정을 허가한 경우 종전의 피고에 대한 소송은 취하된 것으로 보고 새로운 피고에 대한 소송은 처음에 소를 제기한 때에 제기된 것으로 본다. 따라서 경정 전 피고 방송통신위원회에 대한 소송은 취하 간주되어 제1심판결이 실효되었고, 이 법원의 심판대상은 경정된 피고 개인정보 보호위원회의 2018. 3. 28.자 별지1 처분 내역 제1 내지 3항 기재 시정조치, 공표명령 및 제4의 가항 기재 과징금 부과처분에 대한 취소청구이다).

【이유】

】1. 처분의 경위, 2. 처분의 적법 여부 중 가. 원고의 주장, 나. 관계 법령

이 법원이 이 부분에 관하여 설시할 이유는 아래와 같이 제1심판결의 해당부분을 고치는 외에는 제1심판결의 해당부분 이유와 같으므로 행정소송법 제8조 제2항, 민사소송법 제420조 본문에 의하여 이를 그대로 인용한다.

○ 제2면 12행 '피고'를 '방송통신위원회(2020. 2. 4. 법률 제16930호로 개정되어 2020. 8. 5. 시행된 개인정보 보호법 부칙 제3조 제1항에 따라 방송통신위원회의 소관사무 중 개인정보 보호에 해당하는 사무가 피고에게 승계되었고, 부칙 제3조 제4항에 따라 방송통신위원회가 개인정보 보호에 해당하는 사항에 관하여 행한 행정처분은 피고의 행위로 보게 된다.

이하 일괄하여 '피고'라 한다)'로 고친다.

○ 제2면 각주 1)을 '사전대입공격(Dictionary Attack)이란 공격자가 사전에 확보한 아이디/비밀번호 정보 또는 일반적으로 사용되는 정보파일을 가지고 프로그램을 통해 하나씩 모두 대입시켜 보는 공격기법을 말한다.

사전대입공격의 한 유형이라고 볼 수 있는 크리덴셜 스터핑(Credential Stuffing)은 공격자가 사전에 확보한 아이디/비밀번호 정보로 인증을 시도하는 사전대입공격이다.

크리덴셜은 개인을 인증하는 데 활용되는 식별・인증정보의 조합이고 스터핑은 악의적 프로그램을 실행시켜 반복적으로 해당정보를 입력해서 인증을 시도하는 행위를 말한다.

이하에서는 사전대입공격과 크리덴셜 스터핑이라는 용어를 혼용한다.

'로 고친다.

2. 처분의 적법 여부

다.

인정사실

1) 원고의 지위

원고는 1993. 9. 24. 설립되어 PC용 유틸리티 제품 패키지인 알툴즈 패키지(알툴바, 알집, 알송, 알PDF 등) 소프트웨어를 개발・제공하는 알툴즈 웹 사이트(www.altools. com)를 운영하고 있는 정보통신서비스제공자이다.

알툴즈 중 알툴바(ALToolbar)는 원고가 개발한 '도구 모음'으로 인터넷 익스플로러에서 검색 및 자동로그인, 마우스 액션, 온라인 즐겨찾기, 주소표시줄 검색, 메모 등 부가기능을 제공하는 프로그램이다.

2) 개인정보 처리과정

가) 데이터베이스(Database, 이하 'DB'라 한다)는 개인정보 그 자체의 집합이고, 데이터베이스 관리 시스템(Database Management System, 이하 'DBMS'라 한다)은 DB를 보다 수월하게 관리하기 위한 소프트웨어로 Oracle, My SQL 등이 그 예이며, 데이터베이스 관리 책임자(DBA) 등 개인정보취급자는 별도 프로그램(Toad, SQL 등)에 SQL 명령어 등을 입력하여 DBMS에서 개인정보를 열람, 정정, 삭제 등을 한다.

그런데 별도 프로그램을 통한 방식은 전문적 지식・기술이 필요하고 상당한 시간이 소요되며 비효율적이므로, 별도 프로그램과 다른 방식으로 제한된 처리사항만을 원활히 수행하기 위해 웹 애플리케이션(웹 응용프로그램) 및 웹 페이지를 사용하여 DBMS에 명령어를 입력하여 DB를 관리한다.

나) 웹 환경에서 개인정보 처리과정은 아래와 같다.

① 이용자가 웹 브라우저(웹 페이지)에 아이디와 비밀번호를 입력하여 로그인하면, 사용자가 입력한 값(로그인정보)이 웹 서버 등에 전송되고[사용자의 웹페이지 로그인 단계], ② 웹 서버 등에서는 입력 값을 받아 내부 프로세스(웹 애플리케이션, 웹 응용프로그램)를 통해 DB 서버에 개인정보(아이디, 비밀번호의 일치 여부)를 요청하고[웹서버의 로그인 요청 데이터 처리 단계], ③ DB 서버는 해당 정보를 다시 웹 애플리케이션을 거쳐 웹 서버 등에 반환하고, ④ 웹 서버 등은 반환받은 결과를 전송하고, 웹 브라우저는 그 결과를 화면에 표시하면서, 로그인의 성공 여부 정보를 알려준다.

⑤ 이후 DB에 있는 개인정보를 조회하는 경우, 위 절차와 동일하게 진행된다.

웹 페이지, 웹 애플리케이션은 이용자와 DB 서버를 중개하여 DB를 처리한다.

3) 알패스 서비스

가) 알패스(ALPass)는 회원제로 운영되는 많은 웹 사이트의 아이디와 비밀번호를 관리할 수 있는 프로그램으로, 가입제 커뮤니티・포털 사이트에서 사용하는 아이디와 비밀번호를 기억했다가 해당 사이트를 재방문 시 그 정보를 기억하고 로그인 창에 자동으로 아이디와 비밀번호를 입력시켜주는 프로그램이다.

나) 알패스 단독프로그램은 윈도우 부팅과 동시에 실행되고 자동 로그인 설정이 있어 시작하자마자 사이트 목록이 보이고 목록에서 더블클릭하면 새창이 나와 원하는 사이트를 열 수 있었다.

원고는 2007. 3. 21.경 알패스 단독프로그램에서 온라인 서비스 로그인 설정을 하고 알툴즈 아이디와 비밀정보를 입력하면 알패스 오프라인 데이터를 알툴바의 알패스On에 그대로 가져와 사용할 수 있도록 하였다.

알툴바의 알패스On은 인터넷 브라우저(익스플로러)를 실행하여 자동 로그인이 된 후 알패스On을 한 번 누르고 비밀번호를 한 더 입력해야 사이트 목록이 보이고 한번 클릭해 주면 원하는 사이트가 보고 있던 현재 창에 펼쳐진다.

다) 알패스 서비스는 알패스 단독프로그램뿐만 아니라 알툴바 프로그램, 스윙 브라우저(프로그램) 접속을 통해서도 이용할 수 있었다.

이용자가 아이디, 비밀번호를 이용하여 정상적으로 알툴바에 접속하는 경우 자신이 알툴즈(알툴바) DB에 저장・보관하였던 개인정보(외부 사이트 주소, 그 사이트에 대한 아이디 및 비밀번호, 이하 '알패스 정보' 또는 '알패스 데이터'라고도 한다)를 화면으로 조회할 수 있다.

라) 원고는 2012. 4. 4. 알패스 단독제품의 다운로드를 종료하면서 알툴바의 알패스를 계속 사용할 수 있고 알패스 오프라인 데이터를 알툴바의 알패스에 저장하여 사용할 수 있으며, 알툴즈 사이트 온라인 아이디로 로그인하여 알패스를 사용하였다면 알툴바의 알패스 기능으로 사용할 것을 권장하였다.

4) 원고의 침입탐지차단시스템

가) 원고는 오픈소스(Snort)를 이용한 침입탐지를 적용하였고, 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(Iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었다.

원고는 웹 방화벽(Webknight)이 동일 IP로 1시간 동안 1,000건 이상 공격하는 사항을 탐지하도록 하는 정책을 설정하고 있었다.

나) 원고는 2016. 7. 29. 보안관제업체인 이글루시큐리티와 원격보안관제서비스 계약을 체결하고, 2016. 8.부터 이글루시큐리티로부터 불법적인 침입을 탐지하는 보안관제서비스를 제공받고 있었다.

보안관제서비스란 고객의 정보 기술(IT) 자원 및 보안 시스템에 대한 운영 및 관리를 전문적으로 아웃소싱하여 각종 침입에 대하여 중앙관제센터에서 실시간으로 감시 및 분석, 대응하는 서비스를 말한다.

5) 2016년 1차 사전대입공격

가) 해킹시도

(1) 불상의 해커가 2016. 8. 30.경부터 2016. 11. 10.경까지 대량의 알툴즈(알패스) 이용자 계정정보(아이디, 비밀번호)를 가지고 54개 IP에서 알패스 단독 프로그램을 대상으로 1,109,516번의 로그인 접속시도를 하였다.

위 기간 동안 알툴즈 이용자 총 2,143,766명(2016. 11. 14. 기준, 휴면회원 포함) 중 최소 384,758명(약 17.9%)의 계정에서 로그인이 성공하여 부정접속이 의심되었는데, 위 384,758명 중 알패스 이용자는 258,632명이다.

알툴즈(알툴바) DB에는 13,727,666개의 알패스 정보가 저장되어 있었다.

(2) 원고는 피고에게 로그기록을 제출하였는데, 2016. 10. 18.자 로그기록 일부(을 제52호증)는 아래 와 같다.

동일한 IP에서 아주 짧은 로그인 시간 간격으로 여러 다른 이용자의 아이디, 비밀번호로 알툴바에 접속하고 있음을 알 수 있다.

생략

(3) 피고가 위 로그기록을 바탕으로 WHOIS 서비스를 이용하여 접속경로를 사후 확인한 결과 1차 사전대입공격에 다수의 VPN IP가 동원되었다.

54개 IP주소를 통한 전체 시도 횟수 1,109,516번 중 한국 VPN 의심 사업자를 통한 접속시도가 625,255번(56%), 중국 사업자를 통한 접속시도가 399,507번(36%)이고 이들 둘을 합산한 비율은 92%에 이른다.

접속경로 확인 자료(을 제46호증)는 아래 와 같다.

생략

나) 해킹의심 신고

원고는 '알툴즈 아이디로 알패스를 사용하는 이용자'의 네이버 일부 계정이 해킹으로 의심되어 2016. 10. 28.부터 2016. 11. 1.까지 사이에 네이버에서 보호조치를 하였다는 내용을 접수받았고, 같은 이용자가 2016. 11. 2.경 ○○ 자유게시판 및 △△△△△(스윙 브라우저의 유저포럼) 사이트에 올린 알툴바 해킹 의심 관련 게시글을 확인한 후, 2016. 11. 3. 내부점검을 하였다.

다) 원고의 원인분석

(1) 소외인 개발부문 부문장은 2016. 11. 8. 내부 관계자에게 알패스 해킹이 의심되는 정황을 이메일로 보고하였다.

이에 따르면 '① 최근 해킹 문의 때문에 DB를 살펴본 결과 특정 IP에서 지속적으로 로그인을 시도하는 정황이 있다.

1-2개 IP가 아닌 여러 IP로 알패스 웹 서비스를 가지고 지속적으로 요청이 오고 있는 상황이다.

로그에 남은 IP는 BD에서 막아 놓기는 했지만 근본적인 해결책이 아니고 아마 지속적으로 IP를 바꿔서 로그인을 시도할 것으로 생각한다.

② 예전 알패스 프로그램을 이제 지원하지 않으니 서비스를 내렸으면 한다(알툴바와 스윙의 알패스 제외). ③ 3개월분 로그만으로 확인이 어렵지만 지속적으로 로그인을 시도해서 많은 아이디와 비밀번호를 확보하고 있을 것으로 생각되어 이용자들(특히 알패스 이용자)에게 알툴즈 비밀번호의 변경을 유도했으면 한다.

'는 것이다.

원고는 2016. 11. 10.경 자체 로그를 분석한 결과 위와 같은 사항을 확인하였고, 이를 통해 알패스 단독제품에 대한 대량 접속 시도가 있었고 로그인에 성공한 계정이 있음을 알았다.

(2) 원고는 2016. 11. 11. 공격으로 의심되는 IP로 로그인이 성공한 회원들 정보와 로그인 기록을 확인하고, 알패스 단독 제품이 brute force(무차별 대입) 공격에 대비되어 있지 않기 때문에 온라인 접근 차단을 위해 온라인 접속서비스 종료를 논의하였다.

소외 2 소프트웨어사업본부장은 2016. 11. 11. 경영진 그룹에 본부주간보고를 하면서 알패스 회원을 대상으로 한 해킹 시도에 관하여 '서버에 대한 공격은 아니고 알패스에 지속적으로 동일 IP에서 로그인 시도를 하였고, 해당 IP들을 차단했으나 로그인이 성공한 기록이 있어서 확인 중'이라고 밝혔다.

라) 원고의 대응조치

(1) 원고는 2016. 11. 7.경 알툴바 및 스윙 브라우저를 통해 로그인을 시도하는 경우 횟수제한이 적용되도록 하였다.

① 5회 이상 로그인에 실패할 경우 5분 동안 정상적인 로그인까지 차단하고, 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 원고를 상대로 공격시도를 한 IP주소 및 KISA에서 차단 권고한 IP주소는 모두 블랙리스트에 등록하여 접속을 차단하였다.

(2) 원고는 알툴바 또는 스윙 프로그램보다 오래된 알패스 단독제품이 '로그인 시도 횟수제한'이 없어 외부 공격에 취약하다고 판단하고, 2016. 11. 13. 공지를 거쳐 2016. 11. 14. 알툴즈의 알패스 단독프로그램의 온라인 로그인 서비스를 종료하였으며, 아울러 알패스 온라인 로그인으로 이용하였던 알패스 기능은 알툴바를 설치하여 이용하면 데이터가 그대로 연동되어 이용 가능하다고 안내하였다.

원고는 알툴바 및 스윙 프로그램을 통해 접속하여 알패스 서비스를 이용하도록 하였다.

(3) 원고는 2016. 11. 17.경 부정한 로그인 성공이 의심되는 알툴즈 이용자 384,758명에게 이용자의 알툴즈 계정으로 해외에서 로그인 시도가 있어 알툴즈 로그인 비밀번호를 변경할 것을 권장하고, 특별히 알툴즈 서비스 중 알툴바의 알패스를 이용하는 경우 보안에 더욱 유의해 주기 바란다는 메일을 발송하였다.

6) 2017년 2차 사전대입공격

가) 해킹시도

(1) 해커는 2017. 2. 9.경부터 2017. 9. 25.경까지 해킹프로그램인 '알패스(Alpass) 3.0.exe'와 사전에 대량으로 확보한 이용자의 계정정보를 가지고 VPN업체의 IP주소 대역 내 수천 개의 IP주소를 이용하여 알툴바에 로그인을 시도하는 사전대입공격을 하였다.

해커는 자동화 소프트웨어인 '봇'을 이용하여 IP주소 및 계정 아이디를 자동으로 계속 변경하면서 접속을 시도하였다.

(2) 원고가 DB에 보관하였다가 피고에게 제출한 로그기록(갑 제17호증)에 의하면, 2017. 8. 6. 14:33부터 16:59까지 약 2시간 26분 동안 약 100만개의 접속시도 중 898,581개(89.8%)의 접속시도가 원고의 DB에 없는 아이디(사용자번호

0으로 표시)로 로그인 시도를 하였고, 951,181개(95.1%)의 로그인 시도가 실패하였다.

그중 2017. 8. 6.자 로그기록 일부는 아래 와 같다.

생략

(3) 원고는 로그기록을 확인하지 않았다.

원고의 DB 내 ALToolsMember_Data에 존재하는 2017. 6. 2.부터 2017. 9. 12.까지 기간의 접속기록을 사후 분석한 결과, 원고의 알툴바에 총 202,612,768건의 로그인 접속 시도가 있었고, 이 중 81%에 해당하는 195,049,639건이 접속에 실패하였으며, 최소 이용자 522,532명의 알툴즈 계정이 IP주소 (IP 주소 3 생략). - (IP 주소 4 생략) 대역(주식회사 퍼플스톤즈 업체의 IP 1,020개 및 (IP 주소 5 생략) - (IP 주소 6 생략) 대역(주식회사 넥스이노 업체의 IP 32개)에서 해커에 의해 접속이 성공되었음을 확인하였다.

2017. 8. 2.의 경우 IP주소 180.210.*.*. 및 45.64.173.*에서 가장 많은 인증실패가 발생하였고, WHOIS 조회 시 위 IP주소는 국내 VPN 업체인 주식회사 퍼플스톤즈와 주식회사 넥스이노에게 할당되어 있다.

나) 알패스 정보 유출

이 사건 해커는 여러 번 로그인을 시도한 끝에 알툴바 로그인에 성공하면 알툴바 서버에 접속하여 알툴바 DB에 저장・보관된 알패스 정보를 조회할 수 있었다.

2017. 9. 26. 기준 원고의 알툴즈 이용자(회원)는 총 2,189,950명(휴면회원 1,490,927명 포함)이었는데, 해커는 이 중 이용자 166,179명(중복제거)의 계정에 등록된 알패스 정보 25,461,263건을 txt파일로 저장하여 외부로 유출하였다.

유출된 정보는 웹사이트 종류별로 아래 와 같다.

합계(건)포털공공가상통화금융통신기타25,461,2631,015,430689,1711,90959,285201,71723,493,751

다) 원고에 대한 협박

해커는 2017. 9. 1.부터 2017. 9. 8.까지 원고에게 '알툴즈 이용자 254,614명(중복제거)의 계정정보(아이디, 비밀번호)' 및 '알툴즈 계정 3,019개(중복제거)에 등록되어 있는 알패스정보(외부사이트 도메인, 아이디, 비밀번호) 271,747개' 파일과 동영상 파일, 보도자료 등을 제시하면서, 전화통화 및 전자우편 등으로 67회(전화 8회, 전자우편 52회, 게시글 6회, SMS문자 1회)에 걸쳐 끈질기게 현금 5억 원에 해당하는 비트코인을 요구하며 원고를 협박하였으나, 원고가 이에 응하지 않고 2017. 9. 2.경 사전대입공격 방식의 해킹으로 알툴즈 계정정보와 알패스 정보가 유출되었다고 신고하였다.

해커가 제시한 알툴즈 이용자 254,614명의 계정정보를 알툴즈 DB에 있는 이용자 계정과 비교한 결과 206,762명이 실제 알툴즈 이용자로 확인되었다.

라) 이용자의 2차 피해 발생

해커는 유출한 알툴즈 계정의 알패스정보를 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 해커는 가상통화 거래를 하는 이용자계정을 통해 거래사이트에 부정접속하여 해당 이용자의 비트코인(당시시세: 800만 원, 수량: 2.1 코인)을 절취하였다.

마) 피고의 현장 조사

피고는 2017. 9. 2.부터 2018. 1. 10.까지 원고에 대한 개인정보 취급· 운영실태 현장조사를 하였고, 원고가 2016. 11. 10.경 자체적으로 로그를 분석한 결과 및 그 로그기록을 제출받았다.

바) 해커의 검거 및 처벌

해커는 2017. 12. 중순경 경찰에 의해 검거되었다.

7) 원고의 알패스 서비스 종료

원고는 2018. 3. 5. 스윙 브라우저 알패스 지원을 종료하고, 2018. 3. 26. 알툴바에서 제공하던 알패스 서비스도 종료하였다.

[인정 근거] 갑 제1, 12, 14, 15, 17, 29호증, 을 제1, 4, 5, 6 내지 9, 33, 46, 52호증의 기재(가지번호 포함, 이하 같다), 변론 전체의 취지

라. 판단

1) 사전대입공격이 개인정보에 대한 불법적 접근에 해당하는 여부

구 정보통신망법 제28조 제1항은 '정보통신서비스 제공자 등이 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, 제48조 제1항은 '누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다'고 규정하고 있다.

같은 법 제64조 제4항 본문은 '방송통신위원회는 이 법을 위반한 정보통신서비스 제공자 등에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자 등에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다.

'고 규정하며, 제64조의3 제1항은 '방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자 등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 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 있다.

위 규정내용과 위 인정사실에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면 해커가 사전대입공격을 통해 정상적인 이용자인 것처럼 알툴즈 계정에 등록된 알패스 정보에 접근한 행위는 개인정보에 대한 불법적 접근에 해당한다.

① 구 정보통신망법 제2조 제1항 제6호에 의하면 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 말한다.

알패스 정보는 이용자의 외부사이트 도메인, 아이디, 비밀번호로서 이를 통해 특정한 개인을 알아볼 수 있는 정보이므로 개인정보에 해당한다.

② 해커는 알패스 정보를 유출하기 위한 목적에서 2017. 6. 2.부터 2017. 9. 12.까지 3개월 동안 알툴바에 총 2,02,612,768건의 접속시도를 하였고, 그중 접속 실패 건수는 165,049,639건(약 81%)이므로 정상적인 접속시도라고 보기 어렵다.

③ 개인정보의 유출을 방지할 의무가 있는 정보통신서비스 제공자인 원고는 개인정보 유출목적을 가진 해커의 접근을 허용하여서는 아니 된다.

④ 해커의 접속은 정보통신서비스를 제공받는 이용자의 의사에 반하여 이루어진 것으로 해커가 접속에 관한 정당한 권한을 가졌다고 보기 어렵다.

⑤ 개인정보에 대한 불법적인 접근은 내부망에 바로 침입하는 유형 이외에도 정당한 권한 없이 이용자의 계정정보를 이용하는 유형도 존재할 수 있다.

해커가 이용자의 알툴즈 계정정보를 이용하여 권한 없이 정상적인 이용자인 것처럼 원고의 알툴바에 로그인하여 알패스 정보에 접근한 행위는 개인정보에 대한 불법적인 접근에 해당한다.

2) 이 사건 제1 처분사유

가) 침입차단・침입탐지시스템 설치・운영의무

구 정보통신망법 제28조 제1항 제2호는 '정보통신서비스 제공자 등이 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 접근 통제장치의 설치・운영이라는 기술적・관리적 조치를 하여야 한다.

'고 규정하고 있고, 이를 구체화한 정보통신망법 시행령 제15조 제2항 제2호는 '법 제28조 제1항 제2호에 따라 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치・운영이라는 조치를 하여야 한다.

'고 규정하고 있다.

이에 따라 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템을 설치・운영하여야 한다.

나) 개인정보처리시스템의 범위

(1) 구 정보통신망법 제25조 제1항에 의하면 개인정보의 처리란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말하고, 정보통신망법 시행령 제15조 제2항 제1호 및 이 사건 보호조치 기준 제2조 제4호는 '개인정보처리시스템이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

'고 규정하고 있다.

개인정보처리시스템을 DB 자체에 한정하지 않고 '데이터베이스시스템'으로 보다 넓게 정의하고 있다.

피고와 KISA가 2012. 9. 발행한 개인정보의 기술적・관리적 보호조치 기준 해설서(갑 제11호증)에 의하면 일반적으로 체계적인 데이터 처리를 위해 DBMS를 사용하고 있으나, 이용자의 개인정보 보관・처리를 위해 파일처리시스템 등으로 구성한 경우 개인정보처리시스템에 포함시키는 것이 타당하다.

행정자치부와 KISA가 2017. 1. 발행한 개인정보의 안정성 확보조치 기준 해설서(을 제11호증)에 의하면 개인정보처리시스템이란 일반적으로 DB 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며, DB를 구축하거나 운영하는데 필요한 시스템을 말한다.

업무용 컴퓨터에 DB 응용프로그램이 설치・ 운영되어 다수의 개인정보취급자가 사용하거나, 웹 서버라도 DB에 연결되어 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있다.

다만, DB 응용프로그램이 설치・ 운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외된다.

피고와 KISA가 2017. 12. 발간한 개인정보의 기술적・관리적 보호조치 기준 해설서(을 제10, 45호증)에 의하면 데이터베이스시스템(database system)이란 일반적으로 데이터가 저장되는 DB와 DB 내의 데이터를 처리할 수 있도록 해주는 DBMS , 응용프로그램 등이 통합된 것을 의미한다.

따라서 개인정보처리 시스템에는 개인정보가 저장되는 DB , DB를 생성하고 관리하는 DBMS , DB를 용이하게 이용하는데 필요한 응용프로그램 등 데이터베이스시스템의 구성요소가 모두 포함된다.

개인정보처리시스템의 예시로 '응용프로그램(Web 서버, WAS 등) 등을 DB의 개인정보를 처리할 수 있도록 구성한 때' 등을 들고 있다.

이용자가 접속하는 웹 페이지를 통해 DB 내의 데이터(개인정보)에 접근하여 조회, 수정, 삭제 등 처리할 수 있다면 개인정보처리시스템에 해당된다.

(2) 위와 같은 관련 규정 및 해설서의 내용에다가, 위 인정사실에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면, 개인정보처리시스템은 개인정보의 생성, 기록, 저장, 검색, 이용과정 등 데이터베이스시스템 전체를 의미하고, DB와 연결되어 개인정보의 처리 과정에 관여하는 웹 서버 등을 포함하는 개념으로 보아야 하므로, 응용프로그램인 알툴즈(알툴바), 웹 서버, 웹 애플리케이션 역시 개인정보처리시스템에 해당한다고 봄이 상당하다.

① 데이터베이스시스템은 중앙에서 데이터를 통제하여 데이터의 중복과 불일치성을 막고 데이터의 비밀을 유지하며 여러 이용자가 데이터를 공동으로 이용할 수 있게 하는 시스템이고, 여기에는 데이터베이스 관리 책임자(DBA), DB, DB가 저장되는 하드웨어(DB 서버), DBMS, 응용프로그램 등 데이터가 처리되는 데 필요한 모든 인적·물적 요소가 포함된다.

② 개인정보의 처리는 개인정보의 수집이나 제공을 포함하는데, 개인정보는 DB 서버뿐만 아니라 웹 애플리케이션, 웹 서버 등에서도 처리된다.

이용자가 웹 브라우저에서 로그인하거나 회원 가입· 회원 정보 수정 등으로 개인정보를 '입력'하면, 개인정보는 홈페이지 등 웹 서버나 웹 애플리케이션을 거쳐 DB 서버에 전송되고, DB 서버는 전송받은 개인정보를 '검색'하여 매치하거나 '저장' 또는 '편집' 등을 하며, 그 처리 결과를 웹 애플리케이션이나 웹 서버를 거쳐 사용자의 웹 브라우저를 통해 '출력'하여 보여준다.

원고의 웹 사이트 또는 알툴즈(알툴바)는 이용자의 개인정보가 저장된 DB와 연결되어 정당한 권한을 가진 이용자가 접근하는 경우 이용자의 개인정보를 DB에서 불러와 조회할 수 있도록 하고 있다.

③ 정보통신망법 시행령 제15조 제2항 등은 개인정보처리시스템을 '개인정보를 처리하는 데이터베이스관리시스템(DBMS)'이라고 규정하지 않고 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템'이라고 규정하고 있다.

이용자의 개인정보의 제공과 이에 따른 수집이나 이용자에 대한 개인정보의 제공은 DB 서버 내부에서 이루어지는 것이 아니고 웹 서버 전송을 통하여 이루어진다.

이용자가 직접 DB 서버에 접속하여 개인정보를 제공하는 것은 불가능하고, 웹 시스템상 DB 서버는 독자적으로 개인정보를 처리할 수 없으며 중간 전달매체인 웹 서버, 웹 애플리케이션을 통하여 개인정보를 처리한다.

개인정보가 처리되기 위해서는 웹서버, 웹 어플리케이션, DB 서버가 필수적이고 체계적으로 구성되어야 한다.

응용프로그램은 개인정보를 처리하는 기능적인 면에서 DB 서버와 분리하여 상정하기 어렵다.

응용프로그램은 DB 서버에 접근하여 개인정보를 처리하는 기능을 수행하고 이용자가 DB 서버에 접근하는 것에 대한 관문 역할을 수행한다.

DB 서버 자체에서 이용자의 개인정보를 수집하는 것은 아니므로, DB 서버만을 개인정보처리시스템이라고 해석하기 어렵다.

개인정보처리시스템이란 DB에 연결되어 개인정보를 처리하는 응용 프로그램, 웹 서버나 웹 어플리케이션을 포함하는 의미로 해석함이 상당하다.

알툴즈(알툴바), 알툴즈(알툴바) DB는 원고가 이용자에게 알패스 서비스를 제공하기 위한 개인정보처리시스템인 알툴바 시스템의 필수적 구성요소라고 할 수 있다.

④ 해커는 해킹프로그램인 '알패스(Alpass) 3.0.exe'와 사전에 대량으로 확보한 이용자의 계정정보를 가지고 응용프로그램인 알툴바의 로그인에 성공한 후 알툴즈(알툴바) DB에 저정된 대량의 알패스 정보를 조회하고 유출하였다.

해커가 망분리가 되어 있는 알툴즈(알툴바) DB 자체에 침입한 것은 아니지만, 권한 없이 관리자의 의사에 반하여 정상적인 이용자인 것처럼 알툴바에 로그인하여 알툴즈(알툴바) DB에서 알패스 정보를 조회, 유출한 것이므로, 개인정보처리시스템에 침입하였다고 볼 수 있다.

⑤ 정보통신망법 시행령 제15조 제2항 제3호는 정보통신서비스 제공자 등이 개인정보에 대한 불법적인 접근을 차단하기 위한 조치의 하나로 "개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단"을 들고 있으나, 망분리는 개인정보시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단을 의미하는 것이고 개인정보시스템에 대한 외부 인터넷망 차단을 의미하지 않는다.

이 규정 내용에 의하더라도 개인정보취급자 컴퓨터 등이 개인정보처리시스템과 구별된다고 볼 수 있으나, 응용프로그램인 알툴즈(알툴바), 웹 서버가 개인정보취급자 컴퓨터 등의 범주에 속하여 개인정보처리시스템과 구별된다는 의미로 보기 어렵다.

응용 프로그램, 웹 서버는 DB 서버와 분리되어 있지 않고 DB의 개인정보가 응용 프로그램, 웹 서버를 통하여 처리되고 있음을 고려하면 DB뿐만 아니라 응용 프로그램, 웹 서버도 개인정보처리시스템에 포함된다고 보아야 하고, 망분리 여부가 개인정보시스템의 해당 여부를 판가름하는 기준이 될 수 없다.

⑥ 이 사건 보호조치 기준 제4조 제1항이 '정보통신서비스 제공자 등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.

'고 되어 있다.

개인정보시스템은 DB와 DBMS를 포함하는데, DB와 DBMS에 대한 접근권한 부여를 규정하면서 보다 포괄적 의미의 개인정보시스템으로 지칭한 것으로 보이고, 아울러 응용 프로그램이나 웹 서버에 대한 접근권한도 부여될 필요가 있으므로, 이 규정을 두고 개인정보시스템을 DB와 DBMS에 한정된다고 보기 어렵다.

다) 침입차단・침입탐지시스템의 설치・운영의무 위반 여부

(1) 관련 규정 및 법리

(가) 구 정보통신망법 제28조 제1항 제2호, 정보통신망법 시행령 제15조 제2항 제2호에서 요구하는 개인정보에 대한 불법적인 접근을 차단하기 위한 필요한 조치와 관련하여, 이 사건 보호조치 기준은 정보통신서비스 제공자 등이 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 한다(제1조 제1항). 이 사건 보호조치 기준 제1조 제2항은 '정보통신서비스 제공자 등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.

'고 규정하고 있고, 제4조 제5항은 '정보통신서비스 제공자 등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ① 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하고, ② 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함한 시스템을 설치・운영하여야 한다.

'고 규정하고 있다.

(나) 피고와 KISA가 2012. 9. 발행한 개인정보의 기술적・관리적 보호조치 기준 해설서에 의하면 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.

전문 침입차단시스템 및 침입탐지시스템의 설치 운영이 곤란한 SOHO 등 소기업의 경우 인터넷데이터센터(IDC) 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹 방화벽 등)를 활용함으로써 초기 투자비용 등을 줄일 수 있다.

또한, 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.

행정자치부와 KISA가 2017. 1. 발행한 개인정보의 안정성 확보조치 기준 해설서에 의하면 개인정보처리자는 개인정보처리시스템에 대한 접속 권한을 IP주소, 포트(Port), MAC(Media Access Control)주소 등으로 제한하여 인가받지 않은 접근을 제한하도록 한다(침입차단 기능). 개인정보처리시스템에 접속한 IP주소, 포트, MAC주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하고(침입탐지 기능) 접근 제한・ 차단 등 적절한 대응 조치를 하여야 한다.

불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비 설치와 더불어 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상 행위 대응, 로그 훼손 방지 등 적절한 운영・ 관리가 필요하다.

피고와 KISA가 2017. 12. 발간한 개인정보의 기술적・관리적 보호조치 기준 해설서에 의하면 해당 시스템으로는 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Acess Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있다.

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

접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영, 이상 행위 대응, 로그 분석 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. (예시) 신규 취약점 또는 침해사고 발생 시 보안 업데이트 적용, 과도하게 허용되거나 사용되지 않는 정책 등에 대하여 주기적 검토 및 조치 등 - 이상 행위 대응: 모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응. (예시) 동일 IP, 해외 IP주소에서의 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

또한 위 해설서에 의하면 IP주소 등에는 IP주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)를 포함한다.

(다) 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 참조).

(2) 설치의무 위반 여부

이 사건 제1처분의 첫 번째 처분사유는 원고의 사업 규모, 개인정보 보유 수 등을 고려할 때, 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하지 않은 것은 설치의 의무를 소홀히 하였다는 것이다.

피고는 이 사건 소송에서 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템 등의 보안장비를 도입하여 운영하여야 한다고 주장한다(이하 이를 '새로운 시스템'이라 한다).

위와 같은 법리에다가 위 인정사실, 갑 제2, 3, 6, 10, 12, 18, 19, 28, 35호증, 을 제9, 24, 25, 33, 44호증의 기재에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면, 원고는 사회통념상 합리적으로 기대 가능한 정도의 침입차단·침입탐지시스템 설치의무를 준수하지 않았다고 보기 어렵고 달리 이를 인정할 증거가 없다.

① 원고는 알툴즈(알툴바)DB에 대하여 웹 서버에서 오픈소스(Snort)를 이용한 침입탐지를 적용하였고, 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었다(이하 이를 합하여 '기존 시스템'이라 한다).

Snort는 Emerging Threats가 제작한 오픈 소스 네트워크 기반의 공개용 침입탐지시스템(Intrusion Detection System, IDS)인데, Snort시스템에 설정된 룰(rule)과 웹 서버에 접근하는 패킷(IP주소는 패킷헤더에 포함되어 있다)을 비교분석하는 과정에서 규칙에 어긋나는 비정상적 패킹이 감지된 경우 이를 경고한다.

Snort는 Network Security Tools 중 5위(무료 시스템 중 1위)에 선정될 정도로 그 성능의 우수성을 높이 평가받고 있고, Cisco사, 시큐아이 등 많은 상용 보안장비 솔루션 제공사업자가 오픈소스인 Snort 엔진을 기반으로 한 솔루션을 제공하고 있다.

웹 방화벽(Webknight)은 AQTRONIX사에서 개발한 IIS 웹 서버에 설치할 수 있는 공개용 웹 방화벽인데, ISAPI 필터 형태로 동작하고 IIS 서버 앞단에 위치하여 웹 서버에 전달되기 이전에 IIS 웹 서버로 들어온 모든 웹 요청에 대해 웹 서버 관리자가 설정한 필터 룰에 따라 검증을 하고 SQL Injection 공격 등 특정 웹 요청을 사전에 차단함으로써 웹 서버를 안전하게 지키는 침입차단기능을 갖추고 있다.

피고와 KISA는 이에 대한 기술안내서를 배포하여 사용을 장려할 정도로 널리 사용되고 있다.

기본 방화벽(iptables)도 리눅스 운영체제에서 제공하는 방화벽(침입차단시스템)으로서 인가된 IP주소의 접근만 허용하고 인가받지 않는 접근을 차단하는 데 널리 사용되고 있다.

이들 설비는 접속권한을 IP별로 제한하고 입출력 로그를 저장하는 기능을 갖고 있다.

② 원고는 이글루시큐리티와 원격보안관제서비스 계약을 체결하고, 2016. 8.부터 이글루시큐리티로부터 불법적인 침입을 탐지하는 보안관제서비스를 제공받았다.

이글루시큐리티가 제공하는 서비스제공내역에는 방화벽(Firewall)과 IPS(Intrusion prevention system, 침입차단 및 탐지가 구현된 침입방지시스템) 항목이 있다.

Snort에 의해 탐지된 로그, Webknight의 차단내역 및 로그기록은 이글루시큐리티의 ESM서버로 전송되어 모니터링이 되고 관제매뉴얼에 따라 로그분석이 이루어지며 유선/이메일로 경고(Alert)를 받고 있다.

이글루시큐리티는 원고가 설치한 침입차단 및 탐지시스템의 로그들을 24시간 관제(모니터링)하는 침입탐지기능을 수행하였다.

이글루시큐리티는 원고에게 월간 Web 방화벽 상세 보고서를 작성하여 매월 보안관제결과, 현황, 동향을 보고하였고, 원고에 대한 공격을 탐지하면 원고에게 이벤트 분석 보고서를 보내 이상접근 IP의 공격방식과 대응방안을 제시하였다.

③ 원고는 2014. 11.경 접근통제, 운영관리, 보안관리, 사고 예방 및 대응 항목이 포함된 정보보호관리체계 인증(Information Security Management System, ISMS)을 받았다.

KISA가 주관하는 ISMS 인증은 심사항목으로 네트워크 접근, 로그 및 접속기록 관리, 로그 및 접속기록 점검, 보안시스템 운영, 이상행위 분석 및 모니터링 등을 포함하고 있다.

④ 원고가 갖춘 기존 시스템 설비는 침입탐지차단기능을 갖춘 상용화된 설비라고 볼 수 있다.

뒤에서 보는 바와 같이 원고가 기존 시스템을 이용하더라도 로그기록을 분석하고 이에 기초한 이상접속에 대하여 접속차단 등 조치를 취하는 방법으로 사전대입공격에 대처할 수 있었다.

원고가 사전대입공격에 취약하였던 이유는 기존 시스템의 성능(설치)이 아니라 운영의 문제로 보인다.

⑤ 피고는 기존 시스템과 별도로 새로운 시스템을 도입하여야 한다고 주장한다.

새로운 시스템이 트래픽 지연 최소화, 탐지 룰 개수 증가, 다양한 보안 정책 탑재 등이점을 가지고 있는 것으로 보이나, 새로운 시스템의 구체적 사양과 기능이 무엇인지 명확하지 않다.

또한, 기존 시스템의 정상적 운영으로는 이 사건 해커가 사용한 사전대입공격을 막을 수 없고 새로운 시스템을 도입하면 기존 시스템과 차별화되는 어떠한 탐지, 차단 효과가 있어 어떻게 사전대입공격을 막을 수 있다는 점에 대하여 구체적인 주장이 결여되어 있고, 피고가 제출한 을 제13, 14, 49, 50호증의 기재만으로는 이러한 점을 인정하기에 부족하다.

⑥ 원고는 신규 사업 확장을 위해 최대 10Gbps 트래픽 처리가 가능한 장비를 도입하기로 하고, 2017. 3. 보안전문업체인 시큐아이로부터 유료 방화벽(MF2-6000)을 구입하여 6개월간 구축하고 2017. 9.부터 사용하였다.

MF2-6000에 적용하는 라이센스에 따라 방화벽, VPN, IDS, IPS 등을 사용할 수 있고, 장비 도입 당시부터 IDS, IPS 기능을 설정하여 사용하고 있었다.

그러나 을 제13, 14, 49, 50, 51호증의 기재만으로는 이를 2차 사전대입공격 당시 도입하였다면 설치 자체만으로 별도의 룰 설정을 강화하지 않더라도 2차 사전대입공격을 효과적으로 탐지・차단할 수 있었다고 인정하기에 부족하고 달리 이를 인정할 증거가 없다.

⑦ ㉠ 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 유출될 경우 이용자가 입게 되는 피해 정도가 매우 심각한 점 등에 비추어 보면 원고로서는 일반적인 개인정보를 처리하는 정보통신서비스 제공자보다 개인정보 보호조치를 강화할 필요가 있다고 볼 수도 있으나, 이용자 수, 매출액 등을 기준으로 비공개용 유료 시스템을 도입・설치할 의무를 지우는 규정이 없고, 이러한 필요성만으로는 원고가 새로운 시스템을 도입하여 설치하여야 할 의무가 있다고 보기 어렵다.

⑧ 피고와 KISA가 2017. 12. 발간한 개인정보의 기술적・관리적 보호조치 기준 해설서에 의하면 SOHO 등 소기업은 인터넷데이터센터(IDC), 클라우드 서비스 등에서 제공하는 보안서비스를 활용하거나 공개용(무료) S/W를 사용하여 해당 기능을 구현한 시스템을 설치・운영할 수 있고, 다만 공개용(무료) S/W를 사용할 때에는 적절한 보안이 이루어지는지를 사전에 점검할 필요가 있다.

원고가 기존 시스템의 적정 운용으로 사전대입공격에 대하여 합리적으로 기대가능한 수준에서 대처가 가능하다면, 원고가 비록 소기업에 해당하지 않는다고 하더라도, 위 해설서의 소기업에 관한 부분을 근거로 비공개용(유료) 보안서비스를 당연히 구입하여 시스템을 설치할 의무가 있다고 보기 어렵다.

(3) 운영의무 위반 여부

이 사건 제1처분의 두 번째 사유는 원고가 2016. 11.경 해커의 1차 사전대입공격이 있었음을 알고도 부정 접속이 의심되는 이용자에게 비밀번호 변경 안내만 하였을 뿐, 신규 위협 대응, 정책 설정 운영, 이상 행위 대응, 로그 분석 등 방법을 활용하여 접근 제한 및 유출 탐지 기능이 충족되도록 침입탐지시스템 등을 체계적으로 운영·관리하지 않아 2017. 2. 9.부터 2017. 9. 25.까지 발생한 2차 사전대입공격을 탐지하지 못하는 등 침입차단 및 탐지시스템을 소홀히 운영하였다는 것이다.

위와 같은 법리에다가, 위 인정사실과 갑 제2, 7, 14, 16, 20 내지 23, 27 내지 30, 37호증, 을 제8, 9, 16, 17 내지 21, 23, 31, 32, 33, 39, 40, 44, 46, 48호증의 기재에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면, 원고는 사회통념상 합리적으로 기대 가능한 정도의 침입차단·침입탐지시스템 운영의무를 소홀히 하였다고 봄이 상당하다.

따라서 정보통신망법 제28조 제1항 제2호, 같은 법 시행령 제15조 제2항, 이 사건 보호조치 기준 제4조 제5항을 위반하였다고 할 것이다.

(가) 운영의 의미

침입차단·침입탐지시스템의 운영이란 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 통상적인 기능과 용법에 맞게 적정하게 활용하는 것을 말한다.

침입차단·침입탐지시스템은 사전에 정해진 정책 설정에 따라 차단·탐지 기능을 수행하므로, 이를 적정하게 활용하려면 상시적인 모니터링, 로그 분석 등을 통한 새로운 위험요소를 인지하고, 시스템에 침입차단 및 침입탐지 정책 재설정 등을 반영하여 개인정보에 대한 불법적 접근을 탐지·차단하여야 한다.

침입차단·탐지시스템의 적정한 운영에는 상시적인 모니터링, 웹 서버 접속 로그기록 등에 대한 로그 분석, 침입차단 및 침입탐지 정책 설정 등 조치가 포함된다고 할 것이다.

정보통신망법 규정의 목적 및 규정 취지(정보통신망을 통한 불법적 접근 및 침해사고의 방지), 이 사건 보호조치 기준은 정보통신망법이 정한 보호조치의 구체적 기준을 정하는 행정청 내부의 사무처리준칙에 불과하고, 보호조치의 구체적 기준은 정보통신망법의 규정 목적과 취지 등에 따라 판단하여야 하는 점, 해설서의 내용, 웹 서버 접속 로그기록에는 사용자 아이디, IP주소, 로그인 시간, 접속주소 등 불법적 접근 및 침해 여부를 확인할 수 있는 자료를 담고 있는 점에 비추어 볼 때 이 사건 보호조치 기준 제4조 제5항이 정한 접속권한 제한 및 재분석 대상인 IP주소 등에는 IP주소, 포트에 한정되지 않고 웹 서버 접속 로그기록도 포함되고, 웹 서버 접속 로그기록을 실시간으로 분석하거나 사후적으로 분석하는 행위도 침입탐지차단시스템의 운영에 포함된다고 봄이 상당하다.

(나) 2016년 사전대입공격에 대한 인식수준

보안업체가 2016년 사전대입공격에 대하여 주의나 경각심을 가지지 못할 정도로 생소한 해킹 방법이었다고 보기 어렵다.

① 크리덴셜 스터핑은 피고가 2015년부터 웹 취약점 점검 항목으로 참고하도록 한 국제웹보안표준기구(The Open Web Application Security Project, 이하 'OWASP'라 한다)에서 2015. 2.부터 보고되어 왔던 해킹 유형이다.

OWASP는 2016. 9.부터 홈페이지에 크리덴셜 스터핑의 방어방법을 공개하고 있는데, Multi-Factor Authentication(인증 시 다중요소의 사용), Multi-Step Login Process(2차 인증수단 등 다단계 로그인 절차의 도입), IP blacklists(사용자가 통상적으로 로그인하는 IP와 달리 의심스러운 IP를 일시적으로 차단), Device Fingerprinting(사용자기기 식별), Disallow Email Adresses as User IDs(이메일을 아이디로 사용하는 것을 제한) 등의 방법 등을 제시하고 있다.

OWASP는 2016. 11. 자동대입 공격에 대한 핸드북(OWASP Autuomated threat handbook)을 발간하여 크리덴셜 스터핑에 대한 대응방법을 제시하고 있다.

그 일부인 모니터링 방법으로 가입, 로그인, 비밀번호 재설정, 비밀번호 변경, 사용자 이름 변경, 재인증 등에 대한 성공 및 실패한 시도를 기록하여 분석하도록 하고 있다.

② 2016. 12. 30.자 데일리 시큐 인터넷 뉴스에는 '2016년 글로벌 최악의 사이버 공격 사건 10선 정리'라는 제목으로 사이버 범죄자들이 크리덴셜 스터핑이라는 기술을 사용해 한 계정의 아이디와 비밀번호로 다른 계정까지 해킹하기 위해 사용한다는 내용이 실려 있다.

2017. 1. 18.자 시큐리티 월드 인터넷 보안뉴스기사에 의하면 '크리덴셜 유출, 더 이상 간과할 것이 아니다'라는 제목으로 '2016년에 도난당한 수억 개의 온라인 크리덴셜이 자동 로그인 해킹 범죄에 불을 지피고 있다.

..... 오늘 사이버 보안 업체인 쉐이프시큐리티(Shape Security)에 나온 보고서에 따르면 미국 경제잡지 포춘(Fortune)이 선정한 100개 기업의 인터넷에 연결된 시스템들에 나타난 로그인 활동 90% 이상이 이러한 자동로그인 해킹 범죄 시도였다.

..... 원리는 간단하다.

일반 사용자들이 여러 웹사이트에 같은 크리덴셜을 사용한다는 걸 응용한 것뿐이다.

한 곳에서 크리덴셜을 훔쳐, 그걸 여러 웹사이트에 막 대입하는 것인데, 여기에 자동화 기술을 접목해 시간을 단축하는 것이다.

시간이 단축되니 더 많은 사이트에서 크리덴셜을 시험해볼 수 있게 되고, 그러니 성공률이 의미 있게 올라간다.

.....'고 되어 있다.

2017. 4. 이전까지 구글이나 네이버 검색에서도 영문 credential stuffing으로 검색하면 여러 게시글을 찾아볼 수 있다.

(다) 2016년 1차 사전대입공격의 원인 분석 및 대처수준

① 원고가 2016. 11. 10. 자체 로그를 분석한 결과 해커는 적어도 2016. 8. 30.경부터 2016. 11. 10.경까지 대량의 알툴즈 이용자 계정정보를 가지고 54개 IP주소를 통해 알패스 단독 프로그램에 약 1백만 번의 로그인 접속을 시도하였고, 최소 384,758명의 알툴즈 이용자 계정에 대한 부정접속이 성공하였다고 의심하였다.

② 2016. 11. 원고의 내부 분석결과에 의하면 원고는 해커가 봇(bot)을 이용하여 여러 IP로 1차 사전대입공격을 하였고 로그에 남은 IP를 차단하였으나 근본적 해결책이 아니고 지속적으로 IP를 바꿔서 로그인을 시도할 것으로 생각하고

지속적으로 로그인을 시도해서 많은 아이디와 비밀번호를 확보하고 있을 것으로 생각된다고 분석하였다.

원고는 1차 사전대입공격이 특정 IP를 통한 것이 아니라 여러 IP를 통하여 접근하는 것임을 알고 있었고, 이는 2017년보다 본격화된 2차 사전대입공격의 양상과 크게 차이가 없다.

③ 통상 해커는 추적을 피하기 위해 VPN 업체의 IP주소를 사용한다.

1차 사전대입공격에는 54개의 IP가 이용된 것으로 보이고, 공격이 의심되는 IP에 대하여는 접속경로를 확인해 보는 것은 당연한 작업이라고 할 것이다.

WHOIS 등에서 54개 IP를 조회하였다면 기관명, 주소 등 IP 할당정보로 접속경로를 쉽게 확인가능하다.

앞서 본 바와 같이 피고가 로그기록을 바탕으로 WHOIS 서비스로 접속경로를 사후 확인한 결과 54개 IP주소를 통한 전체 시도 횟수 1,109,516번 중 한국 VPN 의심 사업자를 통한 접속시도 약 56%, 중국 사업자를 통한 접속시도 약 36% 합계 약 92%에 이르므로, 2016년 사전대입공격은 주로 VPN 업체의 IP주소로 접속하여 이루어졌다고 볼 수 있다.

54개의 IP가 한국 IP인지 해외 IP인지 여부, 한국 IP라면 통신3사의 IP인지 VPN 업체의 IP인지 여부 등을 확인한 다음 위 분석결과와 종합하여 정상 IP인지 비정상 IP인지 여부를 판단하고 해당 IP를 차단하고 향후 유사한 사전대입공격에 상응하는 탐지 및 차단조치를 취하여야 한다.

그럼에도 원고는 WHOIS 서비스 등으로 로그기록에 대한 접속경로를 확인하지 아니한 결과 해커가 VPN 업체의 IP주소를 통해 부정접속을 시도하였다는 점을 인식하지 못하였다.

④ 원고가 사전에 웹 방화벽이나 보안장비에 룰을 세팅하고 세팅된 룰에 맞는 공격이 이루어질 경우 이를 탐지하고 차단하게 된다.

룰 세팅이란 침입을 식별하는 방법을 정의하는 규칙을 말한다.

크리덴셜 스터핑에 대한 방어 여부는 결국 서비스제공자가 어느 정도의 '룰 세팅'을 하느냐에 달려 있다.

원고가 위와 같은 분석에 따라 아래와 같은 조치를 취하기는 하였으나 사전대입공격을 막기 위한 필요하고도 충분한 조치라고 보기 어렵다.

원고는 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 차단하여 관리자가 해제하지 않는 한 영구적으로 접속을 제한하였으며, 1회라도 공격을 한 IP주소 및 KISA에서 차단 권고한 IP주소를 블랙리스트에 등록하고 차단하는 조치를 취하기는 하였다(비밀번호 변경 안내, 알패스 단독 프로그램 종료 조치는 뒤에서 살펴보기로 한다). 원고는 이글루시큐리티로부터 해킹 공격이 의심되는 주요 IP주소를 제공받아 접근을 제한하는 조치를 취하였다.

그러나 ㉠ 5회 이상 로그인에 실패할 경우 5분 동안 정상적인 로그인을 차단하는 조치를 취하였다고 하더라도 5분이 경과하면 다시 로그인 시도를 할 수 있고, 원고가 관리하는 알패스 정보의 중요성에 비추어 볼 때 계정 비밀번호의 초기화 등이 이루어지지 않는 이상 사전대입공격을 차단하기 위한 충분한 조치로 보기 어렵다.

㉡ 원고는 1차 사전대입공격 시 해커가 봇을 이용하여 지속적으로 IP주소를 바꿔가며 공격하는 양상을 파악하고 있었다.

원고가 2016. 11. 20. 이후 동일한 IP로 500회 이상 로그인 시도 시 로그인 차단, 임시차단 이후 5,000회 이상 로그인 시도 시 접근 차단 조치를 취하였더라도, 공격 IP주소를 바꿔가며 500회, 5,000회를 넘지 않는 범위로 로그인을 시도하는 경우 로그인 차단, 접속 차단 조치가 이루어질 수 없는 한계가 있다.

2016년 1차 사전대입공격 시에도 500회, 5,000회를 넘지 않는 범위로 로그인을 시도하는 IP주소도 존재하고 있었던 것으로 보인다.

㉢ 원고가 1차 사전대입공격에 사용된 IP의 접속을 차단하였다고 하더라도, 1차 사전대입공격이 봇을 이용하여 여러 IP를 바꿔가며 이루어졌음을 인지하고 있었음에도, 1차 사전대입공격과 동일 내지 유사한 공격이 다시 발생할 수 있음을 예상하고 이를 대비하는 조치를 취하여야 한다.

그러나 원고는 여러 IP주소를 바꿔가며 짧은 시간에 대량의 아이디, 비밀번호를 이용하여 500회, 5000회 이하로 로그인을 시도하여 접속에 성공하거나 실패하는 경우를 공격으로 상정하고 이를 탐지・차단하려는 노력을 충분히 기울이지 않았다.

㉣ 통상적으로 보안관제업체는 서비스 운영업체가 요구한 탐지・차단 룰에 대해서 점검 및 대응을 한다.

원고가 2016년 1차 사전대입공격과 관련하여 이글루시큐리티에게 이를 알리고 재발 방지를 위한 대비를 요청하였다고 인정할 증거가 없다.

㉤ 원고가 수집, 관리한 알패스 정보는 다른 외부사이트의 도메인, 아이디와 비밀번호이므로, 사전대입공격을 통하여 위 개인정보가 유출되는 경우 단순한 개인정보의 노출을 넘어 금전적인 피해까지 이용자가 입게 될 가능성이 있어 피해의 정도가 심각할 수 있다.

그만큼 위 개인정보에 대한 부정한 접근을 탐지, 차단할 필요성이 크다.

㉥ 원고는 1차 사전대입공격을 경험하였으므로, 동일 내지 유사한 형태의 사전대입공격이 다시 이루어질 것을 예상하여 룰 세팅을 강화하는 한편, 모니터링, 로그분석을 통해 새로운 사전대입공격이 발생하였는지, 위와 같은 조치로 침입탐지 및 차단이 충분히 이루어지고 있는지를 계속적으로 점검하고 미흡할 경우 새로운 침입탐지 및 차단 정책을 설정하여 보안조치를 강화할 필요가 있었다.

(라) 사전대입공격에 대한 대처 요청

KISA는 2017. 5. 19. 원고에게 '무차별 대입공격에 따른 모니터링 강화 요청'이라는 제목으로 무차별 대입 공격 시도가 발견되어 정보를 공유하고, 현재 100만여 건의 이메일 정보(계정명, 비밀번호)를 기반으로 해외 IP에서 무작위 로그

인 시도가 발생하고 있으며, 추가 피해가 발생하지 않도록 모니터링 강화를 부탁한다는 이메일을 보냈다.

(마) 2017년 2차 사전대입공격에 대한 탐지 및 차단 조치 소홀

① 이 사건 해커는 2017. 2. 9.경부터 2017. 9. 25.경까지 IP주소와 아이디를 지속적으로 변경하면서 봇을 이용하여 특정 IP에서 초당 수십 회 이상 아이디와 비밀번호를 비정상적으로 입력하는 2차 사전대입공격을 벌여 웹 서버를 통해 DB에 보관된 알패스 정보를 조회하고 이를 유출하였다.

② 사전대입공격은 특정 IP에서 다량의 아이디와 비밀번호를 가지고 과도하게 비정상적으로 접속 시도를 하므로, 평상 시보다 로그인 시도가 증가하고 로그인 실패 횟수도 증가하며, 한 개의 IP를 통한 로그인 시도가 사람이 시도하기 어려울 정도로 짧은 시간에 반복적으로 이루어지는 이상 징후를 보인다.

㉠ 2차 사전대입공격 기간 중 접속시도 건수와 접속실패율은 평상시와 현저히 다른 양상을 보였다.

2017. 6. 2.부터 2017. 9. 25.까지 총 접속기록 202,612,768건의 대량접속 시도가 있었고, 이 중 81%에 해당되는 165,049,639건이 접속에 실패하였으며, 해커에 의하여 최소 522,532건의 접속 성공이 확인되었다.

반면, 원고가 피고의 요청으로 피고에게 제출한 최근 알툴즈 접속 로그(최근 3개월치 로그인 평균 횟수) 총/성공/실패내역 자료에 따르면, 2차 사전대입공격이 끝난 이후인 2017. 10. 1.부터 2018. 1. 9.까지 총 시도 6,169,794건, 성공 5,806,160건, 실패 363,634건, 성공률 94%(실패율 6%)로 확인되어 사전대입공격이 없던 시기와 비교하여 접속건수와 접속성공률에 현저한 차이가 있었다.

㉡ 앞서 본 바와 같이 원고가 피고에게 제출한 2017. 8. 6.자 로그기록을 보면 별도의 분석을 거치지 않더라도 여러 IP에서 원고의 DB에 없는 아이디(사용자번호 0)로 로그인을 집중적으로 시도하여 다량으로 로그인이 실패하였고, 사람이 하기 어려운 속도로 하나의 IP에서 여러 아이디로 같은 시각 또는 지나치게 짧은 시각에 동시에 로그인을 시도하는 이상 징후를 쉽게 확인할 수 있다(이는 2차 사전대입공격이 1차 사전대입공격에 비하여 사용된 IP개수가 늘어났을 뿐 하나의 IP에서 여러 아이디로 로그인 시도를 하는 공격방식이 동일하다). 대기업이나 큰 규모의 기관에서 동일한 IP로 접속하는 사례도 생각해 볼 수 있으나, 이는 정상적인 이용자들이 접속에 성공하는 것을 전제로 하는데, 단시간 내 대량의 접속실패를 동반하는 것은 이러한 사용형태가 아님을 충분히 의심할 수 있다.

2017. 8. 6. 14시 33분 36초에서 16시 59분 27초 사이에 약 100만 번의 로그인 시도가 확인된다.

앞서 본 대로 사전대입공격이 없었던 2017. 10. 1.부터 2018. 1. 9.까지 기간 총 로그인 시도가 6,169,794건(하루 평균 약 6만 건)에 그친 것과 비교하면 로그인 시도 건수가 현저히 비정상적인 이상 징후를 보였음을 알 수 있다.

또한, 해당 로그파일에서 2시간 26분 동안 930번으로 가장 로그인 시도가 많았던 (IP 주소 2 생략) IP주소의 경우에는 사람이 할 수 없는 속도로 14시 36분에 76회, 15시 00분에 198회, 15시 02분에 181회, 16시 13분에 67회, 16시 28분에 151회, 16시 44분에 257회 로그인 시도가 있었고, 15시 00분 198회의 경우에도 39초에 19회, 40초에 27회, 41초에 27회, 42초에 28회, 43초에 29회, 44초에 18회, 45초에 14회, 46초에 23회, 47초에 13회로 9초 사이에 집중적으로 로그인을 시도하였음을 알 수 있다.

2017. 8. 6.자 15시 00분 43초의 로그기록(갑 제17호증)은 아래와 같다.

생략

③ VPN 업체의 서비스는 익명성이 있어 추적이 어려운 반면, 접속이 번거롭고 서비스 이용 속도가 느려지므로, 기업이 아닌 일반 이용자가 일부러 VPN을 이용하는 것이 일반적이라고 볼 수 없다.

특정 IP의 접속이 많거나 로그인 실패가 많은데, 그 특정 IP가 VPN이라면 이상 징후로 의심해 볼 수 있다.

원고의 경영기획실장 겸 최고 정보 보호책임자(CISO) 소외 3이 2017. 6. 2.부터 2017. 9. 12.까지 알툴즈 접속기록 DB(ALToolsMember)를 조회・분석한 결과(갑 제16, 27호증)에 의하면 아래 와 같이 14,762개의 IP주소를 통한 전체 접속시도 건수 148,171,735건 중 퍼플스톤즈, 트루네트웍스, 네트로피 등 VPN 업체(순번 7내지 24)의 IP주소를 이용한 접속시도 건수는 145,112,529건으로 약 98%를 차지하고 KT, LG, 에스케이브로드밴드를 통한 접속(순번 1 내지 6)은 약 2%에 불과하다.

알툴즈에 접속을 시도한 IP 개수는 총 890,719개이고, 접속시도 횟수가 많은 IP에 대하여 WHOIS 조회를 통해 VPN 업체가 사용하는 IP주소 대역을 확인하고 해당 VPN 업체가 속한 IP주소 대역의 접속시도 횟수가 현저히 저하되는 경계점 이상을 해킹 시도로 추정해 보면, 전체 24개 IP주소 대역 5,754개 IP주소에서 147,165,525번의 접속을 시도하였고 아래 순번 1 내지 6 기재 국내 이통통신3사 KT, LG유플러스, 에스케이브로드밴드의 104개를 제외하면 18개 IP주소 대역 5,650개 IP에서 144,329,564번의 접속시도(약 98%)가 해킹에 사용되었다고 추정하였다.

생략

④ 2017. 6. 24.자 접속 로그를 사후적으로 엑셀로 통계를 낸 자료(갑 제37호증, 일부는 아래 표와 같다)에 의하면 이 사건 해커는 미리 확보해 둔 아이디/비밀번호를 가지고 원고가 룰 세팅한 임계치를 회피하여 IP가 막히지 않는 범위(500회 로그인시도 내)에서 접속을 시도한 것으로 보인다.

생략

⑤ 원고는 2016년 1차 사전대입공격을 경험하고 로그분석을 통해 사전대입공격이 접속자수가 늘어나고 접속실패율이 높아지는 이상징후를 보이는 사실을 알고 있었으므로, 동일 내지 유사한 2차 사전대입공격이 발생할 것을 예상하여 로그분석 등을 통해 2차 사전대입공격의 발생 여부를 탐지하여야 한다.

㉠ DB의 로그파일은 아이디, IP주소, 로그인시간, 성공/실패, 접속URL 등 다양한 정보를 담고 있고 이를 실시간으로 파악하는 것은 기술적으로 구현 가능하다.

전체 사용자의 로그인 시도 횟수, 성공된 로그인 횟수, 실패한 로그인 횟수, 로그인 성공/실패율을 실시간으로 확인하는 것은 기술적으로 구현이 가능하다.

사용자가 탐지 룰을 설정하는 방법에 따라 설정한 임계치를 넘어가는 각종 IP주소(다수 아이디로 로그인하는 IP, 동일 아이디가 로그인하는 다수의 IP, 다수 기기에서 동일 아이디로 로그인이나 로그인 실패가 빈번한 IP, 해외에서 로그인하는 IP 등)를 실시간으로 보여주도록 구현하는 것도 기술적으로 가능하다.

㉡ 주기적으로 로그를 사후 확인・분석하여 보다 심층적으로 분석하는 것도 가능하다.

DB가 로그파일 정보를 실시간으로 보안담당 인력이 확인할 수 있는 영역으로 보내주도록 하고, 보안담당 인력이 '엑셀작업' 내지 'sorting'을 통해서 어떤 IP, URL이 많은 접속을 시도하였는지, 다수의 접속시도를 한 IP가 로그인에 이용한 아이디의 실패율은 어떠한지를 따져보는 사후분석이 가능하다.

기술적으로 룰을 설정하는 방법에 따라, 초・분・시간・일・주・월 등 다양한 시간단위로 로그에 나타난 접속시도 건수, 접속자 수, 접속의 성공 및 실패 등의 분석이 가능하고, 특정 IP 또는 특정 계정 단위로 나누어 해당 IP나 계정에 누적하여 몇 번의 로그인이 성공하였고 실패하였는지 여부도 분석할 수 있다.

분석작업의 간격은 DB서버의 부하에 문제가 없으면 일일단위, 주간단위, 그보다 작은 단위도 가능하다.

㉢ 로그기록을 보면 별다른 분석을 거치지 않더라도 공격 징후가 의심되므로, 로그인 실패율, 접속경로 등에 대한 보다 심층적인 사후 로그분석 작업이 필요하다고 할 것이다.

2차 사전대입공격에 동원되었다고 의심되어 조사할 수 있었던 IP주소가 14,762개가 이르나, 하루나 그 보다 작은 시간단위로 조사를 할 경우 조사대상 IP주소는 현저히 줄어들 뿐만 아니라, '엑셀작업' 내지 'sorting'을 하면 14,762개의 IP주소는 24개 정도의 IP주소 대역으로 분류됨을 쉽게 확인가능하였을 것으로 보인다.

해당 IP 대역에 속하는 몇 개의 IP주소를 샘플로 하여 WHOIS 등을 통해 조회해보면 IP주소 대역이 어떠한 접속경로를 거쳤는지를 쉽게 확인가능하고 이러한 분석작업에 많은 시간을 소요되지 않는다.

㉣ 원고가 2016년 1차 사전대입공격을 인지한 이후 하루 최대 정상적인 로그인 시도 건수를 분석하고, 동일 IP에서 초당 또는 분당 정상 접속하는 최대 건수를 확인하여, 그에 맞는 탐지 룰을 침입탐지시스템에 설정할 수 있었다.

⑥ 원고는 침입탐지시스템 등의 로그를 분석하였다면 VPN 업체의 특정 IP대역 주소에 의한 대량의 접속시도, 반복적인 대량의 접속실패가 일어나는 이상 징후를 쉽게 발견할 수 있었고, 원고가 설정한 룰(500회 이상)을 회피하여 로그인을 비정상적으로 시도한다는 사정을 파악할 수 있었다.

VPN을 이용한 IP주소 대역에서 다량의 접속 실패가 발생하는 것은 정상적인 이용이 아니다.

VPN을 이용한 IP 공격의 경우 IP를 바꾸어 공격이 계속될 수 있고, 1차 사전대입공격 당시 예상하였던 사항이므로, 원고로서는 1차 사전대입공격과 같은 여러 특정 IP주소가 아닌 2차 사전대입공격과 같이 IP주소 대역에서 여러 IP를 재할당받아 공격이 이루어질 수 있음을 예상할 수 있었다.

홈페이지에 접속하여 다량의 접속실패를 가진 IP가 VPN에서 들어온 IP라면 해킹 시도를 의심하는 것이 합리적이고, 로그분석을 통해 VPN 업체의 IP가 대량 확인되면 해당 VPN 업체의 IP를 분석하여 해킹시도 및 성공 여부를 확인하여야 한다.

⑦ 지속적인 모니터링 및 로그분석을 통해 비정상적인 로그인 접속 상황을 파악하고 해커에 의한 공격 IP주소 대역을 확인한 다음 가령 1시간 내 500번 시도를 500번 이하로 줄이거나 초당 또는 분당 일정 건수 이상 로그인 시도를 차단(사람이 할 수 없는 속력의 로그인 시도를 차단)하는 등으로 룰 세팅을 강화하고, 해당 IP주소 대역을 침입탐지시스템(IDS)에 등록하여 관리하며, 로그분석에서 봇에 의한 공격이 의심되는 IP주소나 IP주소 대역을 수동으로 방화벽에 지정하여 차단하는 룰 세팅을 하는 등 방법으로 해당 VPN 업체의 IP주소 대역을 차단하는 정책을 설정하는 조치

를 취함으로써 사전대입공격을 이용한 해커의 침입을 탐지하고 차단할 수 있었을 것으로 보인다.

㉠ 특정 IP주소에서 접속량이 크게 증가하고 로그인 실패가 집중된다면 해당 IP를 차단하는 것은 가능하다.

방화벽은 운영자가 블랙리스트 IP를 등록함에 따라 IP주소의 접근을 허용/차단하는 방식이므로 IP주소 대역 역시 특정한 값을 입력하는 차단 등록 설정을 통해 차단을 할 수 있다.

IDS, IPS는 일정한 공격징후에 대하여 임계치 룰을 세팅하면 그러한 룰에 따라 임계치를 넘는 IP에 대하여 실시간 대응을 할 수 있다.

원고가 운영한 기존 시스템(Snort)에서 관련 IP나 IP주소 대역을 지정(수동으로 등록)하여 차단하도록 설정하는 것은 가능하다.

Snort에서 탐지할 IP주소 대역을 먼저 설정하고, 그 뒤에 해당 IP주소 대역에서 공격이 발생할 경우, 이를 탐지할 수 있다.

원고는 기존 시스템에서 룰 설정을 통해 VPN 업체의 동일 IP대역에 대한 탐지 및 차단이 가능하였다.

㉡ 침입・탐지시스템의 적정한 운영을 위해서는 보안 담당자의 적절한 모니터링, 로그분석과 그에 따른 정책 설정, 차단 조치 판단이 중요하다.

IP주소 대역 내 여러 개별 IP에서 이상징후를 탐지한 경우, IP주소 대역에 대해서 대응할지 여부는 담당자가 판단하여 룰 세팅을 함으로써 차단된다.

IP주소 대역에 대하여 룰 세팅을 강화하면서 정상적인 이용까지 공격으로 잘못 탐지하는 경우가 발생할 여지가 있으나, 이는 보안 담당자의 판단을 거쳐 룰 세팅을 하고 차단하도록 함으로써 어느 정도 오탐지로 인한 부작용을 시정할 수 있다.

㉢ 비록 해커가 VPN 업체의 IP주소를 변경해 가면서 공격을 하는 경우, 원고가 특정 IP를 차단하면 해커는 곧바로 다른 IP를 이용해 공격을 시도할 수 있으나, 알패스 정보의 중요성에 비추어 볼 때 그러한 공격 형태에 대하여 침입탐지, 차단조치를 포기할 수는 없고, 계속적이고 즉각적인 사후 로그 분석을 통해 공격 IP주소 대역을 파악하고 차단하려는 노력을 기울여야 한다.

만일 이러한 조치에 한계를 느낀다면 아래에서 보는 바와 같은 비밀번호 초기화 등 보다 적극적인 조치를 병행하여야 하고, 그럼에도 공격을 탐지, 차단하는 것이 어렵다고 판단한다면 대처방법이 강구할 수 있을 때까지 알패스 서비스 제공 자체를 일시적으로 정지할 필요가 있다.

도저히 공격을 방어할 수 없다고 하여 공격이 가능한 상태로 방치할 수는 없고, 이 경우 원고로서는 알툴즈 프로그램 가운데 최소한 알패스 정보를 제공하는 서비스 부분에 한정하여 이를 중단하여야 할 것이다.

⑧ 원고는 2차 사전대입공격이 7개월 넘게 이어지는 동안 한 번도 로그분석을 하지 않았고, 2차 사전대입공격 당시 룰 세팅이 되어있던 '1시간 내 500번 시도'를 넘지 않는 IP의 접속시도를 공격 징후로 탐지하지 않았다.

원고는 전체 접속시도 중 약 98%에 달하는 VPN 업체의 IP주소 대역을 이용한 2차 사전대입공격 자체를 인식하지 못하였다.

원고는 전체 서비스에서 발생하는 테이터 전송량(네트워크 트래픽)만 모니터링을 하였고 알패스 서비스 관련 방문자 수 증가를 모니터링하지 않아 이상징후를 파악하지 못하였다.

원고가 이글루시큐리티에 동일 IP주소 대역 접속 관제나 주기적 로그인 접속 실패 분석(공격자의 IP 대역 및 접속정보, 특정 IP의 과도한 로그인 시도, VPN 사용 여부, 기업의 공인 IP 등 오탐 여부 등)을 요구하였다면 이상 징후를 파악하고 이 사건 해킹으로 인한 피해를 방지할 수 있었을 가능성이 크다.

알패스 정보의 중요성에 비추어 볼 때, 원고가 이글루시큐리티에 위와 같은 사항을 의뢰할 수 없다면 자체적으로 시행했어야 한다.

접근 제한 및 유출 탐지 기능이 충족되도록 침입탐지시스템을 체계적으로 운영·관리하였다면 2차 사전대입공격을 상당부분 방지할 수 있었다고 할 것이므로, 침입탐지시스템을 적정하게 운영하였다고 할 수 없다.

(바) 기타 사항

① 원고는 동일 IP주소에서 접속하는 횟수를 대폭 줄여 엄격한 룰 세팅을 할 경우 회사가 동일 IP로 다수의 접속시도를 하는 것과 같이 정상 접속까지도 임시차단하여 원고의 서비스 수준을 떨어뜨리므로 보안만을 이유로 룰 세팅을 엄격하게 하도록 요구하는 것은 정상 접속자의 이용까지 차단하므로 타당하지 못하다고 주장한다.

그러나, 사전대입공격이 충분히 예상되는 상황에서 서비스 품질 저하를 이유로 방어가 곤란하도록 룰 세팅을 포기하는 것은 부당하다.

원고는 엄격한 룰 세팅을 하더라도 정상적인 접속으로 확인되는 회사에 대하여 신속하게 차단의 예외를 설정하는 룰 세팅을 통해 사전대입공격을 방어하면서도 서비스 제공이 가능한 절충점을 찾을 수 있다.

원고는 2019. 9. 30. 에스케이브로드밴드에 할당된 몇 개의 IP에서 불과 몇 초 사이에 다량의 접속시도가 발생하여 급하게 접속을 차단하였는데, 확인결과 □□병원의 임직원 1,800여명이 정상적으로 동시에 접속하였다.

룰 세팅에 따라 동일 IP에서 짧은 순간 다량의 접속시도에 대한 탐지 및 차단이 가능함을 알 수 있다.

원고는 2019. 10. 2. 내부적으로 고객사인 □□병원이 소수의 아웃바운드 IP로 1,800여명이 이용하는 과정에서 IPS에 의해 차단되지 않도록 예외 처리를 하였는데, 예외처리 대상 IP는 메디플렉스 □□병원, 부천 □□병원, 부천 시립노인복지시설의 IP 3건이었다.

② 원고는 2차 사전대입공격 이후 해외 IP에 한하여 악성공격 차단로그에 단일 IP가 연속으로 식별될 때 보안을 위해 방화벽 설정을 통하여 동일 IP주소 대역에 대하여 방화벽을 이용한 차단을 하고 있다.

③ 원고는 2017. 7. 유료 방화벽인 시큐아이 MF2-6000을 도입하여 분석된 시간별로 IP를 분석한 다음 이상이 발생하는 경우 경보알림을 받는 등으로 개인정보 노출방지를 위한 조치를 시행하였다고 주장하나, 2차 사전대입공격 당시 이에 대비한 IDS, IPS의 룰 세팅을 하지 아니한 상태였다.

MF2-6000에서는 기본적으로 개별 IP주소에 대해 룰 세팅을 하는데, IP주소 대역에 대한 탐지 효과를 얻기 위해 개별 IP를 다수 등록해서 IP주소 대역에 대한 탐지와 동일한 효과를 얻을 수 있는 기능을 보유하고 있다.

④ 원고는 2017. 5. 19. KISA로부터 '해외 IP의 무차별 대입공격에 따른 모니터링 강화 요청'을 받고 이미 해외IP에 대해서는 이글루시큐리티의 보안관제를 받아 이를 차단하고 있었다고 하나, 이글루시큐리티에게 1차 사전대입공격사실을 알리고 해당 사전대입공격 유형에 특화된 관제를 요청하였다고 볼 만한 사정을 찾아볼 수 없다.

⑤ 원고는 2020. 7. 8.자 준비서면에서 현재는 크리덴셜 스터핑에 대한 관련 모니터링을 하고 있다고 밝혔다.

3) 이 사건 제2 처분사유

가) 관련 규정의 내용 및 적용범위

(1) 구 정보통신망법 제28조 제1항 제2호는 개인정보의 안전성을 확보하기 위한 기술적·관리적 조치의 하나로 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영'을 규정하고 있고, 정보통신망법 시행령 제15조 제2항 제5호는 개인정보에 대한 불법적인 접근을 차단하기 위하여 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치'를 규정하고 있다.

보호조치의 구체적 기준을 정한 이 사건 보호조치 기준 제4조 제9항은 '정보통신서비스 제공자 등은 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) 피고와 KISA가 2012. 9. 발행한 개인정보의 기술적·관리적 보호조치 기준 해설서에 의하면 개인정보취급자의 부주의로 고객 개인정보가 열람 권한이 없는 자에게 공개되는 사례가 많이 발견되고 있다고 하면서 과실로 인한 인터넷 홈페이지에서 노출 방지, 인터넷 홈페이지 취약점으로 인한 노출 방지, P2P 프로그램에서의 노출, 공유설정을 통한 노출 방지를 설명하고 있고, 구체적인 내용을 보면 취약점으로 인해 구글 등의 검색엔진을 통해 개인정보 DB가 노출되는 사례가 발생하고, 회사 홈페이지를 개발할 때 KISA가 권고하는 웹 보안 서비스를 따르도록 하여 취약점을 최소화한다고 되어 있다.

행정자치부와 KISA가 2017. 1. 발행한 개인정보의 안정성 확보조치 기준 해설서는 개인정보취급자의 업무상 부주의 등으로 개인정보가 노출되지 않도록 필요한 조치를 취해야 한다는 점에 주안점을 두면서도 인터넷 홈페이지를 통하여 개인정보가 유출될 수 있는 위험성을 줄이기 위하여 정기적으로 웹 취약점 점검을 권고하고 있다.

피고와 KISA가 2017. 12. 발간한 개인정보의 기술적·관리적 보호조치 기준 해설서에 의하면 정보통신서비스 제공자 등은 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.

인터넷 홈페이지를 통한 개인정보 유·노출 유형으로는 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·노출을 들고 있다.

구체적인 내용을 보면, 인터넷 홈페이지 설계 시 개인정보 유・노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하여야 한다.

보안대책 예시의 하나로 인증, 접근통제 등의 보호조치 적용을 들고 있다.

인터넷 홈페이지 운영・관리 시 개인정보 유・노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다.

운영 및 관리 예시의 하나로 공격패턴, 위험분석, 침투 테스트 등을 수행하고 발견되는 결함에 따른 개선 조치를 들고 있다.

(3) 위와 같은 규정내용에다가, 위 인정사실과 갑 제11호증, 을 제11, 45호증의 기재에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면, 이 사건 보호조치 기준 제4조 제9항을 내부적인 부주의로 인한 개인정보의 노출방지만을 위한 규정으로 한정하여 해석할 수 없다.

① 이 사건 보호조치 기준 제4조 제9항은 '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치'를 규정한 정보통신망법 시행령 제15조 제2항 제5호에 근거하여 이를 구체화하여 기준을 정하고 있으므로, 접근통제에 필요한 조치를 내부적 부주의에만 한정한다고 볼 수 없다.

② 이 사건 보호조치 기준 제4조 제9항은 정보통신서비스 제공자 등이 취급 중인 개인정보가 열람권한이 없는 자에게 공개되거나 외부 유출되는 것을 방지하고자 하는 것이고, 공개나 유출의 통로를 인터넷 홈페이지, P2P, 공유설정 등으로 상정하고 있으므로, 문언 내용상 열람권한이 없는 자가 정당한 이용자인 것처럼 불법적으로 접근하여 공개, 유출하는 행위를 적용대상에서 배제한다고 볼 수 없다.

즉 내부적 요인(개인정보취급자의 부주의, 인터넷 홈페이지 운영자나 자료 게시 담당 직원의 과실, 인터넷 홈페이지 개발 시 간과하여 발생한 취약점 등)에 따라 개인정보가 유출된 경우에만 위 기준을 적용하겠다는 취지로 보기 어렵다.

③ 이 사건 보호조치 기준 제4조 제9항도 제1항 내지 제5항 등과 마찬가지로 개인정보처리시스템의 접근통제를 위한 규정이라고 볼 수 있고, 외부의 불법적 접근에 따른 개인정보 유출을 방지할 필요성이 있다.

④ 이 사건 보호조치 기준 제4조 제5항은 개인정보에 대한 부정한 접근을 차단하기 위하여 침입탐지시스템을 적정하게 설치하고 운영하는 조치를 취하도록 규정하는 반면, 제4조 제9항은 열람권한이 없는 자에게 개인정보가 공개, 유출되지 않도록 필요한 조치를 취하도록 규정하고 있으므로, 제4조 제9항은 침입탐지시스템의 설치, 운영에 속하지 않는 별도의 필요한 조치를 의미한다고 볼 수 있다.

⑤ 피고와 KISA가 2012. 9. 발행한 개인정보의 기술적・관리적 보호조치 기준 해설서 및 행정자치부와 KISA가 2017. 1. 발행한 개인정보의 안정성 확보조치 기준 해설서가 위반사례로 정보통신서비스 제공자 측의 부주의, 과실로 인한 정보노출에 주안점을 두고 있다고 하여 이를 이용한 외부의 불법접근, 침해의 가능성을 배제하지 아니하므로, 개인정보처리자의 접근통제 등 조치내용이 내부적인 부주의로 인한 개인정보의 노출방지에만 적용하는 입장이라고 보

기 어렵다.

이 사건 이후 피고와 KISA가 2017. 12. 발간한 개인정보의 기술적·관리적 보호조치 기준 해설서는 외부의 불법적 접근에 따른 개인정보 유출 방지에도 적용하는 입장을 명확히 하고 있다.

나) 개인정보 노출방지 조치의 시행 여부

이 사건 보호조치 기준 제4조 제9항에 규정된 정보통신서비스 제공자 등이 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 참조).

위와 같은 법리에다가, 위 인정사실과 갑 제13호증, 을 제1 내지 4, 8, 15, 33, 41, 44, 53호증의 기재에 변론 전체의 취지를 종합하여 인정되는 다음 사정들을 고려하면, 원고가 1차 사전대입공격 이후 개인정보처리시스템의 일부를 구성하는 알툴즈의 알툴바 프로그램에 취약점이 있음을 알고도 2차 사전대입공격에 대비하여 개인정보처리시스템에 부정 접속된 이용자의 비밀번호 초기화, 접속차단 등 조치를 하지 않고, 봇을 이용한 사전대입공격을 방지하기 위한 캡차 또는 추가적 인증수단 적용 등의 조치를 취하지 아니하여 알패스 정보가 외부로 유출되었으므로, 원고는 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 하였다고 볼 수 없다.

따라서 원고는 구 정보통신망법 제28조 제1항 제2호, 정보통신망법 시행령 제15조 제2항 제5호, 이 사건 보호조치 기준 제4조 제9항을 위반하였다.

(1) 해커는 권한 없이 알툴즈의 알툴바에 로그인하여 알툴즈(알툴바) DB에 등록된 개인정보를 조회, 유출하였다.

원고는 해커에 의한 비정상적인 로그인 및 이를 통한 개인정보의 취득을 허용하지 아니하였으므로, 원고의 의사에 반하여 열람권한이 없는 해커에 의하여 인터넷 홈페이지 등을 통해 개인정보가 외부로 공개, 유출된 경우에 해당한다.

(2) 원고는 봇을 이용한 1차 사전대입공격을 인지하고 있었고, 로그분석 등을 통해 2차 사전대입공격을 인식하고 그에 걸맞게 침입차단·탐지시스템을 운영하여야 함에도 이를 소홀히 하였다.

① 원고는, 1차 사전대입공격이 이루어진 후인 2016. 11. 부정접속이 의심되는 계정의 이용자들에게 비밀번호 변경을 요청하였고, 알패스 단독프로그램의 운영을 종료하였다.

원고가 부정접속이 의심되는 계정의 이용자에게 비밀번호의 변경을 요청하더라도, 이용자가 비밀번호를 변경하지 아니할 경우 해킹 방지에 아무런 효과가 없다.

해커가 원고를 협박하면서 제시한 알툴즈 계정 254,614개는 2016. 11.경 당시 사전대입공격으로 로그인 성공이 의심되는 계정 384,758개 중 155,049개와 동일하였다.

② 알패스 단독프로그램의 운영을 종료하였더라도 스윙 브라우저와 알툴바 프로그램을 통한 알패스 서비스를 유지하였으므로, 스윙 브라우저와 알툴바 프로그램 접속을 통한 사전대입공격을 방지하기 위한 조치를 취할 필요성이 남아 있다.

(3) 2차 사전대입공격은 해커가 공격 IP주소를 바꿔가면서 로그인을 시도하는 형태이므로, 로그분석 등을 통해 공격 IP주소 대역을 확인하고 룰 세팅을 강화하는 정책 설정을 통해 이를 차단하는 조치로는 충분하지 아니하고, 개인정보처리시스템 일부를 구성하는 알툴바 프로그램 등에 이를 방어하기 위한 보다 적극적인 조치를 취하여야 한다.

원고는 1차 사전대입공격 이후에는 부정한 접속 성공이 의심되는 계정에 대해서는 비밀번호 초기화 또는 접속차단 조치를 통해 추가로 발생할 수 있는 이용자의 개인정보 유출 피해를 최소화하고, 알패스 정보에 대한 로그인에 있어서는 캡차 및 추가적인 인증수단 등을 적용하는 조치를 통하여 봇에 의한 자동화된 2차 사전대입공격을 차단할 수 있는 조치 등을 취하였어야 한다.

이러한 조치는 당시 기술수준으로 구현이 가능하고 보편적으로 알려져 있는 정보보안 기술수준에 속한다.

① 2016. 11. 사전대입공격에 의하여 다수 계정의 부정 접속 성공이 의심되었으므로, 해커가 부정접속한 아이디, 비밀번호로 다시 사전대입공격을 가할 수 있다.

이용자의 비밀번호 변경 안내에도 불구하고 변경을 하지 아니한 이용자에 대한 사전대입공격으로 이용자의 개인정보가 유출될 수 있음을 예상할 수 있으므로, 보다 근원적 조치로 이용자의 비밀번호를 초기화하거나 접속을 차단하는 조치가 필요하다.

비밀번호 초기화에는 비용이 들지 않는다.

비밀번호를 초기화하면 기존 비밀번호를 이용한 접속이 차단되는 효과가 있다.

비밀번호 초기화와 같은 적극적인 조치가 없는 사이 2차 사전대입공격이 이루어져 해커에 의하여 비밀번호를 변경하지 아니한 실제 이용자의 계정에 있던 알패스 정보가 유출되었을 가능성이 충분히 존재한다.

② 원고는 1차 사전대입공격이 봇에 의한 공격임을 알고 있었으므로, 봇에 의한 공격을 방지하기 위해 조치를 취할 필요가 있었다.

'자동화된 툴'은 웹 페이지에서 매번 바뀌는 문자, 부호, 음성 등을 쉽게 인식할 수 없다.

그러한 조치의 하나인 캡차(CAPTCHA)는 자동입력 방지문자를 입력하도록 하는 방법 등으로 사람인지, 컴퓨터(기계)인지 구분해주어 특정 자동화 툴(스팸, 봇)에 의한 공격을 방지하기 위한 기술로서 인터넷 회원 가입 등에 사용된다.

캡차는 1999년 개발된 기술로서 2010년 들어 대중화되었다.

캡차는 오픈소스 소프트웨어로서 비용이 발생하지 않거나 적게 든다.

③ 또 다른 조치의 하나인 2차 인증수단은 지식기반인증(아이디, 비밀번호)에 소유기반인증을 추가하여 해당 접속기기와는 별도의 기기인 휴대전화, 이메일, 백업 코드, OTP, 보안키, 기기 등 인증을 요구함으로써 봇의 공격을 막는 기술이다.

해커가 아이디와 비밀번호를 알고 알툴바에 접속하였다고 하더라도, 2차 인증수단 단계에서 원고가 관리하고 있는 알패스 정보가 열람되지 않도록 조치할 수 있다.

알패스 정보와 같은 중요한 개인정보를 열람하는 특정한 경우에만 인증을 받도록 한다면, 추가인증으로 인한 비용을 절감할 수 있고 이용자의 편의도 기대할 수 있다.

이 사건의 경우에도 알툴바에 로그인하는 경우에도 알패스 정보를 조회하는 단계에서만 추가 인증을 받도록 하는 방법으로 비용절감 및 이용자의 편의성을 고려할 수 있다.

캡차와 2차 인증수단은 최초 로그인 단계, 접속환경 변경 시 로그인 단계에서 일반적으로 사용되고 있다.

(4) 원고는 알약 등 백신을 판매하는 자회사 이스트시큐리티를 자회사로 두고 있는 국내 대표적인 보안업체이다.

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, 해커가 알패스 정보를 취득하는 경우 이용자에게 심각한 2차 피해가 발생할 수 있는 점 등에 비추어 보면, 이 사건의 경우 원고에게 요구되는 사회통념상 합리적으로 기대 가능한 정도의 보호조치는 일반적인 정보통신서비스 제공자보다 높다.

(5) 원고는 비밀번호 초기화, 접속차단 조치, 2차적 인증수단 등이 이용자에게 상당한 불편을 초래하여 이용자의 이탈을 야기할 수 있는 조치라고 주장하나, 원고는 이용자가 금융기관 등 각종 사이트에 로그인할 수 있는 아이디와 비밀번호를 관리하는 프로그램을 제공하고 있었고, 사전대입공격을 통하여 이용자의 아이디와 비밀번호가 유출되는 경우 단순한 개인정보의 노출을 넘어 금전적인 피해까지 이용자가 입게 될 가능성이 있는 중요 개인정보라고 할 수 있으므로, 개인정보의 내용상 높은 수준의 보안수준이 유지되도록 보호조치를 취할 필요가 있었다.

비밀번호 초기화 등 조치가 이용자의 이용 불편을 초래하는 측면이 있더라도, 2차 사전대입공격에 효과적으로 방지할 수 있는 다른 대체수단을 확보할 수 없는 이상 다소 이용의 불편을 감수하더라도 보안의 안전성을 확보할 수 있는 비밀번호 초기화 등 수단의 도입은 필요하다.

특히 원고는 1차 사전대입공격 직후 개인정보 유출을 의심하고 있었던 상황이었으므로, 1차 사전대입공격 이후 유출의 위험에 대비하여 위와 같은 수단을 도입할 필요성이 더욱 크다.

(6) 원고는 2차 사전대입공격 이후 비밀번호 초기화, 접속차단 조치를 취하였고, SMS를 통한 2차 인증을 도입하여 사용한 적이 있다.

2020. 4. 현재 원고의 알툴즈 사이트에는 캡차 기능이 도입되어 있는 것으로 보인다.

4) 이 사건 처분의 적법 여부

가) 시정명령

앞서 본 바와 같이 이 사건 처분사유 중 접근통제장치의 운영의무위반(침입차단 및 탐지시스템을 소홀히 운영하였다는 부분), 개인정보처리시스템에 필요한 조치를 불이행한 위반행위(개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하지 아니하였다는 부분)는 인정되나, 접근통제장치의 설치의무위반(전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템 등의 보안장비를 도입하여 운영하지 아니하였다는 처분사유)은 인정되지 아니한다.

원고는 알툴즈 프로그램을 운영하는 보안업체로서 향후 서비스 제공과정에서 이용자의 개인정보를 보관하는 상황에서 유사한 위반행위를 반복하지 아니하도록 시정명령을 할 필요성이 인정되므로, 위와 같이 처분사유가 인정되는 범위 안에서 위반행위에 대한 시정명령은 정당하다.

나) 공표명령

구 정보통신망법 제64조, 정보통신망법 시행령 제69조에 따르면, 방송통신위원회는 시정조치의 명령을 받은 정보통신서비스 제공자 등에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다.

그 규정의 문언과 공표명령 제도의 취지 등을 고려하면, 방송통신위원회는 그 공표명령을 할 것인지 여부와 공표를 명할 경우에 어떠한 방법으로 공표하도록 할 것인지 등에 관하여 재량을 가진다고 볼 것이다.

구 정보통신망법 제64조가 시정조치의 하나로서 시정명령을 받은 사실의 공표를 규정하고 있는 목적은 일반 공중이나 정보통신서비스 제공자 등이 법위반 여부에 대한 정보와 인식의 부족으로 피고의 시정조치에도 불구하고 위법사실의 효과가 지속되고 피해가 계속되는 사례가 발생할 수 있으므로 조속히 법위반에 관한 중요 정보를 공개하는 등의 방법으로 일반 공중이나 관련 정보통신서비스 제공자 등에게 널리 경고함으로써 계속되는 공공의 손해를 종식시키고 위법행위가 재발하는 것을 방지하고자 함에 있다.

이러한 제도목적과 함께, 사전대입공격이 사전에 확보한 이용자의 아이디와 비밀번호정보 또는 일반적으로 사용되는 정보를 가지고 이를 대입하여 공격하는 해킹기법으로서 이용자에게 커다란 피해를 입힐 수 있고 비교적 최근의 해킹기법이므로 일반 공중에게 아이디나 비밀번호의 보관 및 사용에 주의를 일깨우고 관련 정보통신서비스 제공자 등에게 사전대입공격을 방어하기 위한 보안조치를 강화하도록 경고할 필요가 있는 점, 위반행위로 인한 알패스 정보의 유출규모가 상당한 점, 일간지에 공표하도록 한 크기가 통상적인 수준이고 게재횟수도 1회에 그친 점, 원고의 홈페이지 및 모바일 어플리케이션에 게재하도록 한 기간도 1주일 정도로 장기간이라고 볼 수 없고 비용이 크게 소요될 것으로 보이지 않는 점 등 기록에 나타난 여러 사정에 비추어 보면, 피고의 공표명령이 위 인정범위 안에서 비례원칙에 위배된다거나 재량권을 일탈·남용하였다고 볼 수 없다.

다만, 접근통제장치의 설치의무위반 부분에 대한 시정명령은 위법하므로, 위 행위로 인하여 피고로부터 시정명령을 받은 사실에 대한 공표명령 부분 역시 위법하다.

다) 교육 및 대책수립, 보고

원고는 위 인정범위 안에서 위반행위에 대하여 시정명령을 이행하고 개인정보보호 책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하며, 재발방지대책을 수립하고 이를 피고에게 보고할 필요가 있으므로, 위와 같은 시정조치는 적법하다.

다만, 접근통제장치의 설치의무위반 부분에 대한 시정명령은 위법하므로, 위 행위로 인하여 교육 및 대책수립, 보고를 명한 시정조치 부분 역시 위법하다.

라) 과징금

구 정보통신망법 제64조의3, 정보통신망법 시행령 제69조의2 등 규정을 종합하여 보면, 방송통신위원회는 법 위반행위에 대하여 과징금을 부과할 것인지 여부와 만일 과징금을 부과할 경우 법과 시행령이 정하고 있는 일정한 범위 안

에서 과징금의 액수를 구체적으로 얼마로 정할 것인지에 관하여 재량을 가지고 있다고 할 것이므로, 방송통신위원회의 법 위반행위자에 대한 과징금 부과처분은 재량행위라 할 것이고, 다만, 이러한 재량을 행사함에 있어 과징금 부과의 기초가 되는 사실을 오인하였거나, 비례·평등의 원칙에 위배하는 등의 사유가 있다면 이는 재량권의 일탈·남용으로서 위법하다고 할 것이다.

갑 제1호증의 기재에 변론 전체의 취지를 종합하면 피고는 이 사건 제1, 2처분사유가 모두 인정되는 것을 전제로 과징금을 산정하였으나, 이 사건 제1처분사유 중 접근통제장치의 설치의무위반행위는 인정되지 아니하므로, 이를 위반행위에서 제외하고 나머지 위반행위에 대하여 과징금을 산정할 필요가 있다.

따라서 이 사건 과징금납부명령은 과징금부과 재량행사의 기초가 되는 사실인정에 오류가 있어 재량권 일탈·남용의 위법이 있다 할 것이다.

(과징금의 액수를 산정함에 있어서는, ① 원고가 해커로부터 협박을 받아 2차 사전대입공격을 인지한 직후 스스로 관계 당국에 2차 사전대입공격 사실을 신고한 점, ② 원고는 2차 사전대입공격 이후 사전대입공격에 대한 모니터링, SMS를 통한 2차 인증, 캡차 기능 도입 등 조치를 취한 것으로 보이는 점, ③ 원고는 2차 사전대입공격 이후 보안강화조치로 인한 사용자 이탈의 가속화, 무료 서비스에 따른 사업성 하락을 이유로 이 사건 처분 직전에 알패스 서비스를 종료한 점, ④ 원고는 알패스 서비스 종료 전까지 이용자에게 무료로 알패스 서비스를 이용하도록 하였던 점, ⑤ 원고가 2차 사전대입공격에 대비한 로그분석, 강화된 룰 세팅 등 면에서 운영을 소홀히 한 측면이 있었으나, 사전대입공격이 관련 업계에서 해커에 의한 부정한 접근방법으로 충분하게 인식되지 않았던 측면이 있었고, 원고가 2차 사전대입공격에 대한 사전 보안조치를 취하였더라도 이를 완벽하게 방어하는 데 어려움이 있었을 것으로 보이며, 2차 사전대입공격이 가능하였던 데에는 이용자가 아이디와 비밀번호를 부주의하게 취급한 측면도 있었던 점 등을 고려할 필요가 있다).

3. 결론

그렇다면 원고의 청구는 위 인정범위 안에서 이유 있으므로, 이 사건 처분 중 별지2 처분 내역 기재 시정조치 및 공표명령 부분을 초과하는 부분을 취소하고, 원고의 나머지 청구는 이유 없어 이를 기각한다(원고와 경정 전 피고 방송통신위원회 사이의 제1심판결은 이 법원의 피고경정허가에 따른 소 취하 간주로 실효되었다).

(별지 생략)

판사 이창형(재판장) 최한순 홍기만