방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 14 - 100호

안 건 명 ㈜ 개인정보 유출사고에 대한 시정조치에 관한 건

피 심 인 ㈜

대표이사

(사업자등록번호 : 법인등록번호 :)

의 결 일 2018. 3. 28.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출 등을 방지하기 위하여 ①개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치를 설치·운영을 하여야 하고, ②개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

2. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 어플리케이션에 1주일 이상 게시하여야 한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

3. 피심인은 제1, 2항에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호 책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 분실·도난·유출 등을 방지하기 위한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

4. 피심인에 대하여 다음과 같이 과징금과 과태료를 각 부과한다.

가. 과 징 금 : 112,000,000원

나. 과 태 료 : 10,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

마. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

이 유

Ⅰ. 기초 사실

피심인은 영리를 목적으로 패키지(등) 소프트웨어를 개발·제공하는 웹사이트 ' '( )를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)」 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황과 최근 3년간 매출액은 다음과 같다.

<참고 1> 피심인의 일반현황

대표이사	설립일자	자본금	종업원 수

<참고 2> 피심인의 최근 3년간 매출액

(단위 : 천원)

구 분	2014년	2015년	2016년	합 계	3년 평균*
매출액					

Ⅱ. 사실조사 결과

1. 조사대상

방송통신위원회는 피심인이 보관, 관리하는 이용자의 개인정보가 2017. 12. 중순경 경찰에 검거된 해커(이하 '이 사건 해커'라 한다)에 의해 서비스 대상 사전대입 공격[1] 방식의 해킹으로 ' ' 서비스의 계정정보, 계정에 등록된 정보가 유출되었다는 피심인의 신고('17. 9. 2.)를 접수하였다.

1) 사전대입 공격(Dictionary Attack)이란 공격자가 사전에 확보한 ID/PW 정보 또는 일반적으로 사용되는 정보파일을 가지고 프로그램을 통해 하나씩 모두 대입시켜 보는 공격기법을 말한다.

이에, 방송통신위원회는 한국인터넷진흥원과 함께 피심인을 대상으로 피심인으로부터 넘겨받은 사고 관련 자료와 피심인이 이용자의 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템'이라 한다) 등에 남아있는 접속기록 등을 토대로 해킹경로 파악과 개인정보의 기술적·관리적 보호조치 등 정보통신망법 위반 여부 확인을 위한 개인정보 처리·운영 실태를 조사(2017. 9. 2. ~ 2018. 1. 10.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 유출 규모

이 사건 해커의 서비스에 대한 사전대입 공격으로 피심인이 ' 소프트웨어' 제공 서비스를 운영하면서 수집한 '17. 9. 26. 기준 회원정보(아이디, 비밀번호, 이름, 이메일 등) 총 명(휴면회원 명 포함) 중 명(중복제거)의 이용자 계정에 등록된 정보 건이 유출되었다.

<참고 3> 피심인의 유출 정보 현황

구 분		유출된 항목	건 수	중복제거
사전대입 공격 ('17.2.9.~9.25.)	정보	외부사이트 도메인, 아이디, 비밀번호	건	명***

* 검거된 해커의 PC에 저장('17.2.9. ~ 9.25.)되어 있던 개인정보 유출 자료

<참고 4 > 유출정보의 웹사이트 종류별 유출 계정 건수

합계(건)	포털	공공	가상통화	금융	통신	기타

나. 유출 경로

(1) 2017년 사전대입 공격

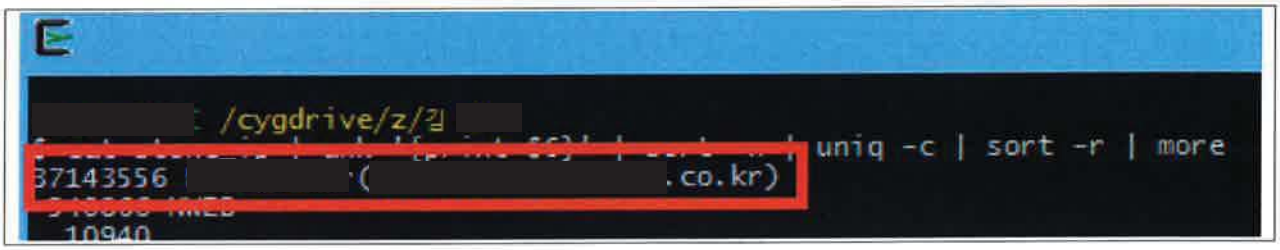
피심인의 데이터베이스(이하 'DB')내 존재하는 2017. 6. 2.부터 2017. 9. 12.까지 기간의 접속기록을 분석한 결과, 피심인의 ' ' 서비스에 총 건의 대량 접속 시도가 있었고, 이 중 %에 해당하는 건이 접속에 실패하였으며, 최소 명의 계정이 이 사건 해커에 의해 접속 성공된 것을 확인하였다.

<참고 5> 해커의 공격내역(IP주소대역, 국가코드, 접속 성공 횟수)

IP주소 대역	국가코드	접속 성공 횟수
180.210 ~ 180.210	KR	
45.64. ~ 45.64.	KR	
180.210.x.x 및 45.64.173.x IP에서 가장 많은 인증실패 발생('17.8.2. 샘플링 기준)		

<참고 6> 해커의 사전대입 공격 시도 및 접속 실패 기록

<참고 7> 해커가 서비스를 대상으로 공격한 기록



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

《 2016. 11.경 사전대입 공격 관련 》

이 사건 조사 과정 중, 피심인의 소명을 통하여 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 계정정보(아이디, 비밀번호)를 이용하여 서비스를 대상으로 54개 IP에서 약 1백만 번의 접속시도*를 하였고, 이 중 부정 접속이 성공한 것으로 의심되는 이용자 계정은 총 건(휴면회원 포함) 중 최소 건**(약 %)으로 확인하였다.

* 이용자인 경우에 대해서만 분석한 자료이며 접속기록을 3개월만 보관하고 있어 정확한 접속시도횟수는 확인 할 수 없음(관련 접속기록 보관기간: '16.08.30 ~ '16.11.10)

** 경의 이용자중 이용자는 명이며 총 개의 등록정보가 DB에 저장되어 있음

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

(2) 개인정보 유출

알패스 이용자는 아이디, 비밀번호를 이용하여 정상적으로 에 접속하는 경우 프로그램에 저장된 외부 사이트 주소, 그 사이트에 대한 아이디 및 비밀번호를 화면으로 볼 수 있다.

이 사건 해커는 해킹프로그램인 ‘ 3.0.exe’와 사전에 대량으로 확보한 이용자의 아이디, 비밀번호를 이용하여 이용자가 에 접속하는

경우와 유사하게 알툴바 서버에 접속하여 이용자 명이 등록한 정보(외부사이트 도메인, 아이디, 비밀번호) 건을 txt파일로 저장하여 외부로 유출하였다.

또한, 이 사건 해커는 2017. 9. 1.부터 2017. 9. 8.까지 피심인으로부터 탈취한 이용자의 계정정보(아이디, 비밀번호) 건(중복제거) 및 정보(외부사이트 도메인, 아이디, 비밀번호) 개가 담겨있는 계정 개(중복제거) 파일과 동영상 파일, 보도자료 등을 제시하며 전화통화 및 전자 우편 등으로 67회(전화 8회, 전자 우편 52회, 게시 글 6회, SMS문자 1회)에 걸쳐 끈질기게 현금 5억원에 해당하는 비트코인을 요구하며 피심인을 협박하였으나, 피심인은 이에 응하지 않았다.

<참고 8> 해커의 사전대입 공격 및 자료 유출 현황

구 분	유출 기간	건 수
사전대입 공격	'16. 8. 30. ~ 11. 10. (접속기록 분석 기간)	최소 건 (부정 접속이 의심되는 계정)
	'17. 6. 2. ~ 9. 12. (접속기록 분석 기간)	최소 건 (접속이 성공한 계정)
해커 협박 메일	'17. 9. 1. ~ 9. 8. (해커 협박 기간)	건 (정보)
		건 (계정)
검거된 해커 PC	'17. 2. 9. ~ 9. 25. (PC에 저장되어 있던 기간)	건 (정보)
		건 (계정)

이 사건 해커가 제시한 건의 계정정보를 DB에 있는 이용자 계정과 비교한 결과, 개가 실제 계정으로 확인되었고, 특히 2016. 11.경 당시 사전대입 공격으로 접속이 성공한 계정 건 중 건이 동일한 계정으로 확인되었다.

<참고 9> 해커의 협박 메일 발송 현황

구분	발송 일시	발송횟수	비 고
1차	2017.09.01. 16:46	1회	임직원
2차	2017.09.01. 16:50	1회	임직원 (이용자 개인정보 포함)
3차	2017.09.04. 15:33~21:05	18회	임직원 (5억 요구)
계	-	52회	

(3) 이용자 2차 피해 발생

이 사건 해커는 유출한 계정의 정보(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 이용자 계정으로는 거래사이트에 부정 접속하여 해당 이용자의 비트코인(당시 시세 : 800만원, 수량 : 2.1코인)을 절취하여 이용자에게 2차 피해가 발생한 것을 검거된 이 사건 해커에 대한 경찰청 조사 결과를 통해 확인하였다.

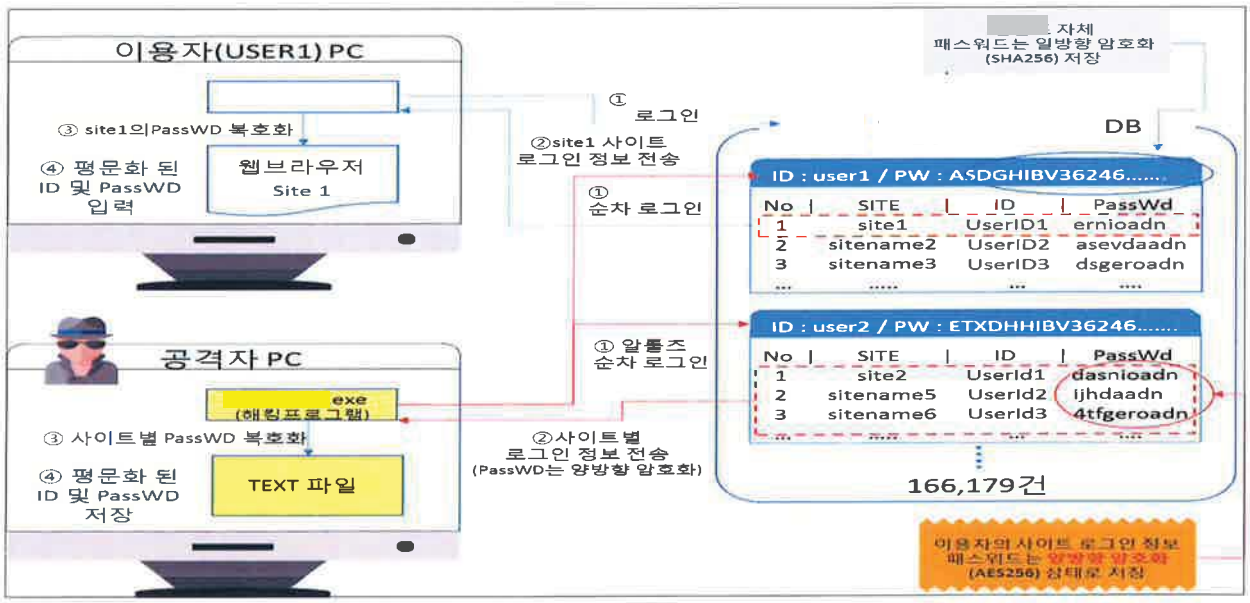
다. 개인정보 유출 경로 요약

이 사건 해킹의 방법 및 절차 등은 크게 2단계로 구분해볼 수 있는데,

1 이 사건 해커는 해킹프로그램인 ' 3.0.exe'와 출처를 알 수 없는 대량의 아이디, 비밀번호를 확보하여, 피심인의 ' ' 서비스에 접속을 시도하는 사전대입 공격(2017. 2. 9. ~ 2017. 9. 25.)을 하였고,

2 이를 통해 접속이 성공한 ' ' 이용자의 계정에 등록된 ' ' 정보를 txt 파일로 저장하여 유출한 것으로 조사되었다.

<참고 10> 개인정보 유출사고 개요도



3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제[정보통신망법 제28조(개인정보의 보호조치) 중 접근통제]

1) **(침입차단시스템 및 침입탐지시스템의 설치·운영)** 피심인은 오픈소스(Snort)를 이용한 침입탐지를 적용하였고, 운영체제(Linux CentOS)에서 제공하는 기본 방화벽(iptables) 및 공개용 웹 방화벽(Webknight)을 사용하고 있었다.

다만, 개인정보에 대한 불법적인 접근을 차단하기 위하여 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템, 방화벽(시큐아이 MF2-6000, 2017. 7.경 도입) 등의 보안장비를 도입하여 설치·운영한 사실은 없었다.

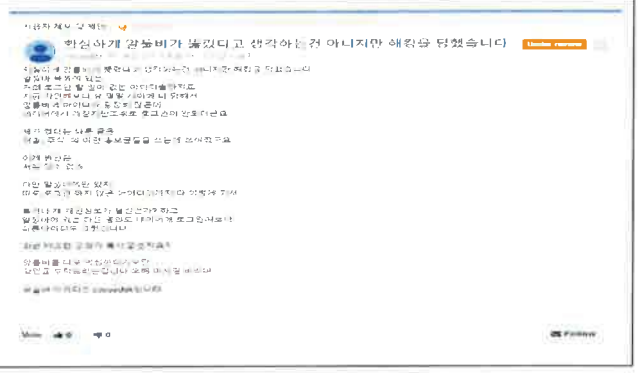
특히, 웹서버에 설치된 웹 방화벽(Webknight)에서 동일 IP에서 1시간 동안 1,000건 이상의 공격에 대하여 탐지하도록 운영정책을 설정하고 있었으나, 동일 IP대역에서 짧은 시간에 대량의 아이디, 비밀번호를 이용한 접속하는 경우에는 공격으로 판단하지 않아 2016. 8. 30. ~ 2016. 11. 10. 기간 동안 최소 54개 IP에서 약 번의 사전대입 공격이 있었음에도 불구하고 2016. 11. 2. 이용자가 해킹 의심 관련 글을 게시하기 전까지 사전대입 공격에 대하여 탐지하지 못하였고 부정 성공이 의심되는 이용자들에게 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 체계적으로 운영·관리하지 않아 2017. 6. 2. ~ 2017. 9. 12. 기간의 건의 사전대입 공격에 대하여도 2017. 9. 1. 16시 46분 이 사건 해커의 협박 전까지 탐지하지 못한 사실이 있다.

<참고 11> 피심인의 웹 방화벽(Webnight) 정책 설정 화면

상시 탐지	위에 언급한 로그 외에 탐지되는 로그	동일 IP 에서 1 시간동안 1,000 건이상의 공격 및 페이지

2) **(개인정보 유·노출 방지 조치)** 피심인은 2016년 11월 해킹 의심 관련 게시글을 확인한 후, 서버 접속기록을 분석하여 서비스에 봇[2]을 이용한 대량의 아이디, 비밀번호를 대입하는 사전대입 공격을 인지하였다.

<참고 12> 이용자 해킹 의심 관련 게시글

뽐뿌 자유게시판 게시	스윙 아지트 게시
	

2) 봇이란 인터넷 상에서 자동화된 작업(스크립트)를 실행하는 응용 소프트웨어이다.

그러나 피심인은 해커가 서비스의 아이디, 비밀번호를 취득하는 경우 이용자에게 심각한 2차 피해가 발생할 수 있음을 알면서도, 피심인은 당시 사전대입 공격으로 부정한 접속 성공이 의심되는 계정 이용자 명에게 비밀번호 변경 안내 메일을 발송한 것 외에 해당 이용자의 비밀번호 초기화, 접속차단 등의 조치를 하지 않아 이 사건 해커의 2017. 2. 9.부터 2017. 9. 25.까지 기간 발생한 사전대입 공격으로 이용자의 정보(외부사이트 도메인, 아이디, 비밀번호)가 유출되었다.

또한, 봇을 이용한 공격을 방지하기 위한 캡차[3] 및 추가적 인증수단 등을 적용하는 조치를 취하지 않아, 해커의 2017. 6. 2.부터 2017. 9. 12.까지 기간의 (접속기록 분석 기준) 사전대입 공격에서 이용자 정보(외부사이트 도메인, 아이디, 비밀번호)가 서비스를 통하여 외부로 유출되는 사고를 방지하지 못한 사실이 있다.

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 2. 23. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2018. 3. 16., 3. 23. 2회에 걸쳐 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령이 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)'을 하여야 한다."라고 규정하고 있다.

3) 캡차(CAPTCHA)란 사람과 컴퓨터를 구별하기 위한 '자동 계정 생성 방지 기술'로 인터넷에서 회원가입 등에서 사용한다.

나. 정보통신망법 시행령 제15조제2항은 "법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

다. 정보통신망법 시행령 제15조제6항에 따라 제2항 등의 구체적인 기준을 정한 고시인 「개인정보의 기술적·관리적 보호조치 기준(이하 '고시'라 한다)」 제4조제5항은 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 '개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)'하는 기능, '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)'하는 기능을 포함한 시스템을 설치·운영하여야 한다."라고,

고시 제4조제9항은 "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 있다.

2. 위법성 판단

○ 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위한 기술적·관리적 보호조치를 아니한 행위(정보통신망법 제28조제1항)

1) 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위

고시 제4조제5항은 "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·운영하여야 한다."라고 규정하고 있다.

고시 해설서는 ▲"정보통신망을 통해 개인정보처리시스템에 불법적으로 접근하는 행위를 방지·차단하기 위해 침입차단기능 및 침입탐지기능을 갖는 시스템 등을 설치·운영함으로써 네트워크 보안을 강화하여야 한다."라고,

▲"침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법으로, 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치·운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다"라고,

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

▲"또한, 공개용(무료) S/W를 사용하여 해당 기능을 구현한 시스템을 설치·운영 할 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 제4조제5항의 입법 목적은 '정보통신망을 통한 불법적인 접근 및 침해사고 방지'인바, 그 내용은 첫째 침입차단 및 침입탐지 기능을 포함한 시스템의 '설치' 의무이고, 둘째 침입차단 및 침입탐지 기능을 포함한 시스템의 '운영'의무이다.

먼저 시스템 '설치' 의무에 대하여 살펴보면, 정보통신서비스 제공자등은 ①접속권한을 IP주소 등으로 제한하여 비인가 접근을 '차단'하는 기능(침입차단기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출 시도를 '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 제1조제2항에 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 사업자'[4]로서 그 사업규모, 개인정보 보유 수를 고려하여 개인정보 보호조치를 취하여야 할 것이다. 또한, 수집·보관 중인 이용자의 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, 운영체

4) '일정 규모 이상 사업자'라 함은 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등을 의미한다.(정보통신망법 시행령 제15조 제2항 참조)

제(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 한번이라도 분석하였다면(DB내 Member_Data 테이블에 존재하는 2017. 6. 2. ~ 2017. 9. 12. 기간 접속기록을 분석한 결과, 전체 접속기록 건의 %에 해당되는 건의 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 접근을 제한하거나 인가자의 비정상적인 행동에 대응), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 차단) 등의 방법을 활용하여 접근 제한 및 유출 탐지

기능이 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 ' ' 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 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 데이터베이스시스템 전체를 의미하는 것으로, 데이터베이스와 연결되어 개인정보의 처리 과정에 관여하는 웹 서버 등을 포함하는 개념으로 보아야 하고, 보호조치 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 사전 대입공격을 탐지하지 못하는 등 침입차단 및 탐지시스템을 소홀히 설치·운영 함으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항, 고시 제4조제5항을 위반하였다.

2) ' ' 서비스 이용자 개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치하지 않은 행위

고시 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 있다.

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

그러나 피심인은 해커가 서비스의 아이디, 비밀번호를 취득하는 경우 이용자에게 심각한 2차 피해가 발생할 수 있음을 알면서도, 당시 사전대입 공격으로 부정한 접속 성공이 의심되는 계정 이용자 명에게 비밀번호 변경 안내 메일을 발송한 것 외에 해당 이용자의 비밀번호 초기화, 접속차단 등의 조치를 하지 않아 이 중 명의 이용자는 2차 사전대입 공격으로 정보(외부

사이트 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 이용자 정보(외부사이트 도메인, 아이디, 비밀번호)가 서비스를 통하여 외부로 유출되는 사고를 방지하지 못한 사실이 있다.

이에 대하여 피심인은 보호조치 기준 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 피심인이 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 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 웹서비스를 가지고 지속적으로 요청", "아마 지속적으로 ip를 바꿔서 접속 시도를 할 것으로 생각된다"는 등의 내용이

담겨있는 것으로 볼 때 피심인의 주장은 근거가 없다.

또한, 피심인은 2016. 11.경 부정접속이 의심되는 사례가 발생한 후 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 5000회 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 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 접속기록(170107.log 파일)을 분석한 결과, 2017. 1. 7. 20:00:38부터 20:59:28까지 223.130. IP에서 번의 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, 정보통신서비스 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 등 백신을 판매하는 국내 대표적인 보안업체로 2016년 매출액이 억 원이고, 2017년 9월 기준 개인정보를 보관하고 있는 건수가 200만 명 이상으로 일정규모 이상의 사업자에 해당하며, 제공하는 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 또다시 발생할 수 있는 봇에 의한 사전대입 공격을 차단할 수 있도록 하였어야 한다.

이러한 부정한 접속 성공이 의심되는 계정에 대한 비밀번호 초기화, 접속차단 조치를 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 서비스에 사전대입 공격이 있었음을 인지한 이후에도 이용자의 비밀번호를 보관하는 서비스 특성상 해커가 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 이용자 정보가 서비스를 통하여 외부로 유출되게 함으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항, 고시 제4조제9항을 위반하였다.

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출 등을 방지하기 위하여 ①개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제 장치를 설치·운영을 하여야 하고, ②개인정보가 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 조치를 취하여야 한다.

나. 피심인은 가항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지와 모바일 어플리케이션에 1주일 이상 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

<참고 13> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

피심인은 1.가항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 분실·도난·유출을 방지하기 위한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

※ 위 사항에서 정하지 않은 시정명령 이행계획 및 이행결과보고 등 추가 세부사항은 방송통신위원회와 협의하여 이행하도록 한다.

V. 과징금 부과

피심인의 개인정보처리시스템에 기술적·관리적 보호조치를 하지 않은 행위에 대하여 정보통신망법 제64조의3제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] 과징금의 산정기준과 산정절차 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(이하 '부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항을 위반한 과징금 상한액은 같은 법 제64조의3제2항, 시행령 제69조의2에 따라 위반행위와 관련된 매출액의 산정이 곤란한 경우로 4억원 이하의 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

'부과기준' 제5조제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따를 때, 피심인은 영리를 목적으로 패키지(등) 소프트웨어를 개발·제공하는 웹사이트 ' '( )를 운영하는 정보통신망법 제2조제1항제3호에 따른 정보통신서비스 제공자로서

▲피심인이 2017. 9. 26. 기준 보관·관리하고 있던 개인정보(계정정보)는 건(휴면회원 포함)이고 계정에 등록된 정보는 수천만 건으로 매우 방대하고, ▲' ' 서비스의 특성상 이용자의 개인정보(외부 사이트, 아이디, 비밀번호)는 유출 시 이용자가 입게 되는 피해 정도가 매우 심각하므로 이에 걸맞게 엄격하고 세밀한 개인정보 관리가 요구됨에도 ▲정보통신망법 제28조 제1항제2호에 따른 접근통제의 기술적·관리적 보호조치 중 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, 개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 행위로 이 사건 해커에 의해 이용자의 개인정보가 유출되게 하는 빌미를 제공하였으므로, 피심인에게 중과실이 있다.

2) 중대성의 판단

'부과기준' 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있고,

'부과기준' 제5조제3항 단서조항은, 위반행위의 결과가 ▲위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우(제1호), ▲위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우(제2호), ▲이용자의 개인정보가 공중에 노출되지 않은 경우(제3호) 중 모두에 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 감경하도록 규정하고 있다.

이에 따를 때, 피심인의 위반행위 결과가 ▲위반행위로 인한 개인정보의 피해규모가 피심인이 보유하고 있는 개인정보의 100분의 5 이상{2017. 9. 26. 기준, 피심인의 이용자 개인정보 총 명(휴면회원 명 포함) 중 명(중복제거)의 이용자 계정과 이용자 계정에 등록된 정보 건 유출}이나, ▲위반행위로 직접적으로 이득을 취득하지 않은 점, ▲이용자의 개인정보가 공중에 노출되지 않은 점 등을 고려할 때, 위반행위의 중대성을 '중대한 위반행위'로 판단하였다.

3) 기준금액 산출

피심인의 서비스는 무료로 이용자들에게 제공하는 서비스로 위반행위 관련 매출액을 산정하기 곤란하므로 정보통신망법 제64조의3제2항, 같은 법 시행령 제69조의2제2항 및 [별표 8] 과징금의 산정기준과 산정절차 2. 가. 2)에 따른 '중대한 위반행위'로서 기준금액을 280,000,000원으로 한다.

<참고 14> 정보통신망법 시행령 제69조의2제2항에 따른 기준금액

위반행위의 중대성	기준금액
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
보통 위반행위	2억원

다. 필수적 가중 및 감경

위반행위의 기간이 1년 이내(2016.11.8. ~ 2017.9.2.)로 '부과기준' 제6조와 제7조에 따른 '단기 위반행위'에 해당하므로 위반행위에 따른 가중은 기준금액인 280,000,000원을 유지하고,

또한, 최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 140,000,000원을 감경한 140,000,000원으로 한다.

라. 추가적 가중 및 감경

'부과기준' 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려한 결과, 이번 개인정보 유출사고 시 자진 신고한 사실 및 방송통신위원회 등 관계기관의 조사에 피심인이 협조하여 이 사건 해커가 검거된

사실 등을 고려하여 '부과기준' 제8조 [별표] Ⅱ. 2.에 따라 필수적 가중·감경을 거친 금액 140,000,000원에서 100분의 20에 해당하는 금액인 28,000,000원을 감경한 112,000,000원으로 한다.

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2, [별표 8] 과징금의 산정기준과 산정절차 및 '부과기준'에 따라 상기와 같이 단계별로 산출한 금액인 112,000,000원을 최종 과징금으로 결정한다.

<참고 15> 과징금 산출내역

<table>
<tr><th>기준금액</th><th colspan="2">필수적 가중·감경</th><th>추가적
가중·감경</th><th>최종 과징금</th></tr>
<tr><td rowspan="2">28,000만원</td><td>가중 없음</td><td rowspan="2">14,000만원</td><td>가중 없음</td><td rowspan="2">11,200만원</td></tr>
<tr><td>기준금액의 50%
(140,000,000원)
감경</td><td>필수적 가중·감경을 거친 금액의 20%
(28,000,000원)
감경</td></tr>
</table>

Ⅵ. 과태료 부과

피심인의 개인정보처리시스템에 기술적·관리적 보호조치를 하지 않은 행위에 대하여 정보통신망법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표 9] '과태료의 부과기준' 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '처리지침')에 따라 다음과 같이 부과한다.

1. 기준금액

정보통신망법 시행령 [별표 9] 2. 개별기준은 최근 3년간 같은 위반행위로 과태료 처분을 받은 경우에 위반 횟수에 따라 기준금액을 달리 적용하도록 규정하고 있고, 이번 피심인의 위반행위는 첫 번째에 해당하여 1회 위반 과태료를 적용한다.

<참고 16> 위반 횟수별 과태료 금액

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조제1항 제3호	1,000	2,000	3,000

2. 과태료의 가중 및 감경

가. 과태료의 가중

처리지침 제9조는 ▲위반행위가 2개 이상인 경우(제1호), ▲위반행위가 2개 이상에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기·정도, 사회·경제적 파급 효과 등을 고려하여 과태료를 가중 부과할 필요가 있다고 인정되는 경우(제2호)에는 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 따를 때, 피심인의 ▲기술적·관리적 보호조치 위반행위는 ①침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 행위 등 위반행위가 1개(제28조제1항제2호)에 해당하고 위반의 동기 등을 종합적으로 고려할 때, 특별히 과태료 금액을 가중할 만한 사유가 없다.

나. 과태료의 감경

처리지침 제8조는 ▲위반행위의 결과가 과실에 의한 경우(제1호), ▲위반행위의 결과가 경미한 경우(제2호), ▲위 두 가지 규정에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우(제3호)에는 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 따를 때, 피심인의 위반행위 결과가 ▲개인정보처리시스템에 대한 접근통제 조치 등을 제대로 하지 아니하여 이용자의 개인정보가 유출된 것이지 과실에 의한 경우에 해당한다고 볼 수 없다는 점, ▲위반행위의 결과로 개인정보 유출의 피해 규모가 경미하지 않다는 점, ▲기타 위반의 동기 등을 종합적으로 고려할 때, 특별히 과태료 금액을 감경할 만한 사유가 없다.

3. 최종 과태료의 결정

이에 따라, 피심인의 기술적·관리적 보호조치를 하지 않은 행위(과태료 1,000만 원)에 대하여 총 1,000만 원의 과태료를 최종적으로 부과한다.

<참고 17> 과태료 산출내역

위반 유형	기준금액	가중금액	감경금액	최종 과태료
기술적·관리적 보호조치 §28①2호	1,000만원	-	-	1,000만원

<참고 18> 위반행위별 과징금·과태료와 시정명령

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2호	112백만원	10백만원	O	122백만원

Ⅶ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조제1항제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

피심인은 이 시정명령 및 과징금 부과 처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 의하여 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조 규정에 의하여 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항 규정에 의하여 그 효력을 상실하고 관할법원(당사자 주소지의 지방법원 또는 그 지원)이 과태료 재판 절차에 따라 결정한다. 이 경우 피심인은 관할법원의 과태료 재판이 확정된 이후 재판 결과에 따라 과태료 납입 의무를 부담한다.

위 원 장　　이 효 성 (인)

부위원장　　허　　욱 (인)

위　　원　　김 석 진 (인)

위　　원　　표 철 수 (인)

위　　원　　고 삼 석 (인)