방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 33 - 377호

안 건 명 의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 7. 4.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

가. 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·운영할 것

나. 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취할 것

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 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

4. 피심인에 대하여 다음과 같이 과징금 및 과태료를 부과한다.

가. 과 징 금 : 219,000,000원

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 홈페이지( )를 통해 온라인 교육 서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황과 최근 3년간 매출액은 다음과 같다.

<참고 1> 피심인의 일반현황

대표이사	설립일자	자본금	종업원 수	
			전체	정보보호

<참고 2> 피심인의 최근 3년간 매출액

(단위 : 백만원)

구 분	2014년	2015년	2016년	3년 평균
전체 매출				
관련 매출				
관련없는 매출*				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

* ‘ ’ 수수료와 교재 매출 등은 관련 없는 매출로 분류

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 피심인이 주 2회 실시하는 웹 로그분석 등을 통해 2017. 7. 18. 유출 징후를 인지하고, 보관·관리하는 이용자의 개인정보가 인적사항을 알 수 없는 해커(이하 ‘이 사건의 해커’라 한다)에게 9,873명의 회원정보가 유출되었다는 피심인의 신고(‘17. 7. 19.)를 접수하였다.

이에, 방송통신위원회는 한국인터넷진흥원과 함께 피심인으로부터 넘겨받은 사고 관련 자료와 개인정보처리시스템 등에 남아있는 접속기록 등을 토대로 해킹 경로 파악과 정보통신망법 위반 여부 확인을 위한 개인정보 처리·운영 실태를 조사(2017. 7. 19. ~ 2018. 2. 22.)한 바, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 유출 규모

피심인이 초·중등 온라인 교육 서비스를 제공하기 위해 웹페이지(,)를 운영하면서 수집한 2017. 7. 25. 기준의 회원정보(아이디, 이름, 연락처, 이메일 등) 총 1,539,137명 중 1,233,859건(중복제거 1,117,227명)의 개인정보가 외부로 유출된 것으로 확인되었다.

<참고 3> 피심인의 개인정보 유출 현황

구 분		유 출 항 목	건수	중복제거*
이용자 정보	정상 회원	아이디, 이름, 생년월일, 휴대전화번호, 전화번호, 주소, 이메일 등	7,297건	7,140명
	휴면·탈퇴 회원	아이디, 이름, 휴대전화번호	1,226,562건	1,110,087명
소 계		-	1,233,859건	**1,117,227명**

* 이용자 정보 1,233,859건을 아이디 기준으로 중복 제거

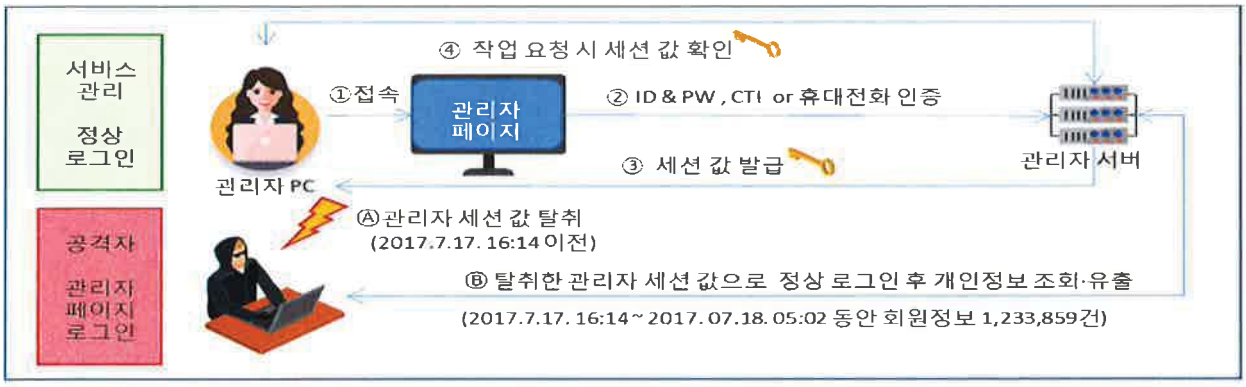
나. 유출 경로

1) 해커의 관리자 인증 세션ID 탈취

이 사건 해커는 피심인의 직원 신○○이 2017. 7. 17. 10:43경부터 피심인 관리자 페이지( )에 접속하여 사용 중인 세션ID*를 2017. 7. 17. 16:14경 이전에 알 수 없는 방법으로 탈취하였다.

* 세션ID :

<참고 4> 해커의 관리자 인증 세션 값 탈취 개요도



2) 탈취한 세션ID를 이용하여 공격 스크립트 작성·업로드

이 사건 해커는 신○○으로부터 탈취한 세션ID를 이용하여 관리자페이지에서 개인정보를 조회 및 유출할 수 있는 공격 스크립트*(　　)를 작성하였고, 이호스트데이터센터 등 5개의 IP를 이용하고 있는 서버에 업로드 한 것으로 확인되었다.

* 해커가 업로드 한 공격스크립트 기능 : 회원정보를 자동으로 조회하여 다운로드 할 수 있는 기능

<참고 5> 온라인교육서비스 관리자페이지에 해커가 접근한 이력

구분	IP주소	국가코드	접속 시간
1	139.162.115.	JP	2017.07.17. 16:14 ~ 2017.07.18. 05:02
2	223.130.89.	KR (SDS)	
3	211.220.195.	KR (KT)	
4	27.255.64.	KR (이호스트)	
5	211.32.53.	KR (LGU+)	

<참고 6> 해커의 공격 스크립트(　　) 작성 화면

3) 공격 스크립트를 이용한 개인정보 유출

이 사건 해커는 탈취한 세션ID(CS팀장 신○○)로 관리자 페이지에 2017. 7. 17. 16:00경 5개 IP에서 접속하였고, 업로드한 공격 스크립트를 이용하여 2017. 7. 17. 16:14부터 7. 18. 05:02까지 관리자페이지( )에 아이디, 이름 등 개인정보를 최대 1초당 35회 조회하는 질의* 방법으로 1,233,859건(중복제거 1,117,227명)의 개인정보를 txt파일로 저장, 외부로 유출하였다.

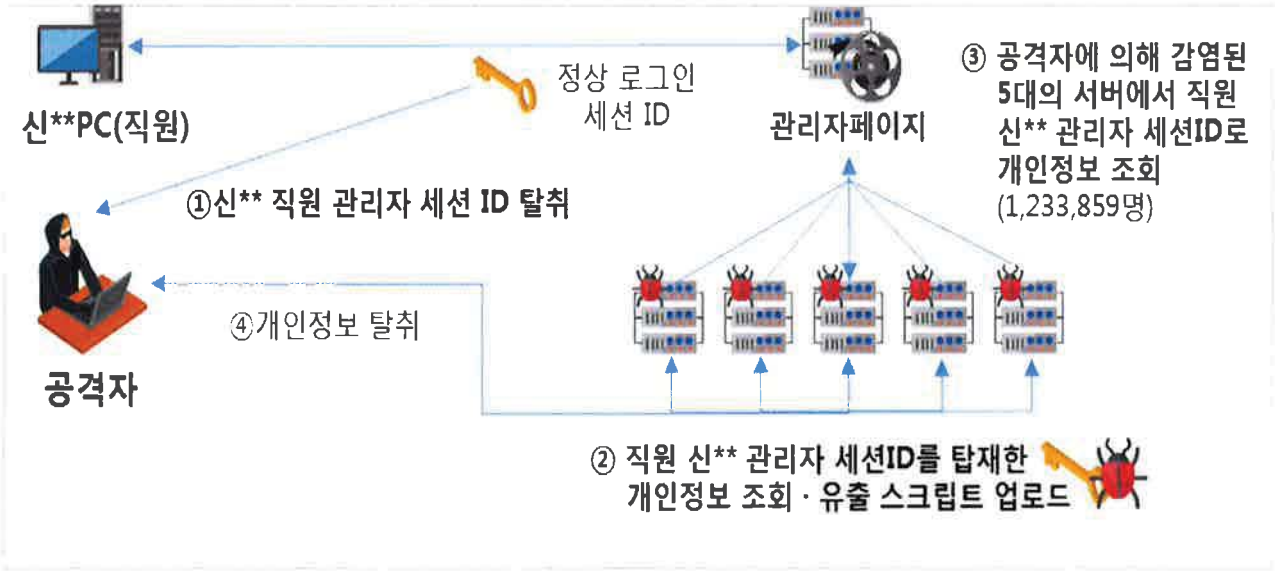
* 개인정보를 조회하는 질의(detail_type=1&mem_key= 회원고유번호)

<참고 7> 해커의 자료 유출 파일

'220000-140001.txt' 파일내용

220000	탈퇴(ydc	탈퇴회원	2006-12-07오전8:11: --	탈퇴탈퇴		--
219999	휴면(hae	탈퇴회원	2006-12-07오전6:04: --	휴면휴면	이	010--
219998	휴면(chc	탈퇴회원	2006-12-07오전5:16: --	휴면휴면	이	016-9
219997	휴면(tkd	탈퇴회원	2006-12-07오전2:50: --	휴면휴면	신	011-7
219996	탈퇴(al0	탈퇴회원	2006-12-07오전2:00: --	탈퇴탈퇴		--
219995	탈퇴(pin	탈퇴회원	2006-12-07오전1:42: --	탈퇴탈퇴		--
219994	휴면(nar	탈퇴회원	2006-12-07오전12:42 --	휴면휴면		
219993	탈퇴(fre	탈퇴회원	2006-12-07오전12:34 --	탈퇴탈퇴		--
219992	휴면(sur	탈퇴회원	2006-12-07오전12:25 --	휴면휴면		
-						
140008	휴면(kim	탈퇴회원	2005-12-22오후6:37: --	휴면휴면	백	018-7
140007	휴면(znh	탈퇴회원	2005-12-22오후6:37: --	휴면휴면	강	010-9
140006	휴면(tjd	탈퇴회원	2005-12-22오후6:32: --	휴면휴면	김	010-9
140005	휴면(juji	탈퇴회원	2005-12-22오후6:31: --	휴면휴면	문	011-3
140004	휴면(van	탈퇴회원	2005-12-22오후6:31: --	휴면휴면	유	016-4
140003	휴면(ghk	탈퇴회원	2005-12-22오후6:31: --	휴면휴면	구	010-9
140002	휴면(mil	탈퇴회원	2005-12-22오후6:30: --	휴면휴면	김	010-9
140001	휴면(boy	탈퇴회원	2005-12-22오후6:28: --	휴면휴면	정	010-3

<참고 8> 개인정보 유출 경로도



3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}

1) **(침입차단 및 침입탐지시스템의 설치·운영)** 피심인은 개인정보에 대한 불법적인 접근을 차단하기 위하여 웹 방화벽(펜타시큐리티시스템, WAPPLES-2200)을 설치·운영하였고, DDOS 공격을 탐지·차단하기 위한 Anti DDOS 보안 관제 서비스(시큐아이, SECUI MFI 2100)를 이용하여 하나의 출발지 IP에서 1초 동안 500회의 HTTP Requst 패킷이 발생하면 해당 IP를 공격자로 간주하고 20초 동안 격리하도록 운영하고 있었다.

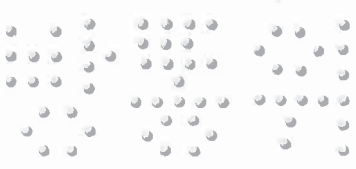
그러나 피심인은 개인정보처리시스템인 관리자페이지( )에 접속한 개인정보취급자 또는 IP주소 등의 개인정보 조회 행위에 대한 재분석을 통해 불법적인 개인정보 유출 시도를 탐지하도록 시스템을 설치·운영한 사실이 없었다.

이로 인해, 이 사건의 해커가 2017. 7. 17. 16:14부터 2017. 7. 18. 05:02경까지 5개 IP에서 관리자페이지에 동일한 계정(CS팀장 신○○)으로 접속하여 총 1,233,859건(중복제거 1,117,227명)의 개인정보를 조회(최대 초당 35회), 유출하였음에도 피심인은 이를 탐지하지 못한 사실이 있다.

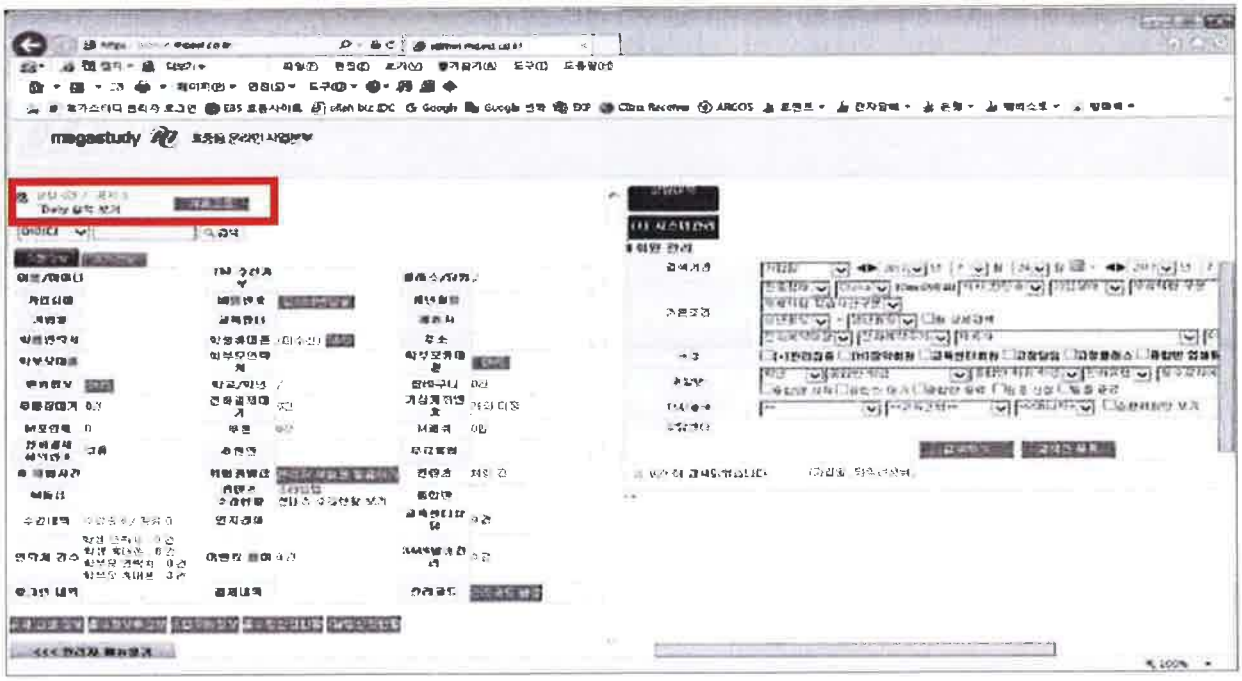
※ 세션ID를 탈취당한 신○○ 팀장의 평상 시 근무 시간(평균 10:00경 출근 ~ 20:00경 퇴근)

2) **(최대 접속시간 제한)** 피심인은 개인정보취급시스템인 관리자페이지의 최대 접속시간 제한은 60분으로 설정하였으나, 해커에게 세션ID를 탈취당한 신○○(CS팀장)이 속해있는 CS 부서는 고객의 실시간 요청 건을 파악하기 위해 1분 단위로 자동 로딩되도록 시스템이 사전 설정되어 있어 세션 종료가 이루어지지 않은 사실이 있다.

이로 인해, 이 사건의 해커는 탈취한 관리자 인증 세션을 이용하여 아이디, 비밀번호, 휴대전화 인증 없이 온라인 교육 서비스의 관리자 페이지에 접속할 수 있었다.



<참고 9> CS부서 어드민 사용자의 자동 페이지 로딩 화면



※ 빨간 박스 안에 iFrame으로 해당 페이지에 1분 단위로 자동 페이지 로딩 됨

나. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 4. 11. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 4. 30. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영(제2호) 등의 기술적·관리적 보호조치"를 하도록 규정하고 있다.

나. 정보통신망법 시행령 제15조제2항은 "정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템')에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)과 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호) 등의 조치"를 하도록 규정하고 있다.

다. 「개인정보의 기술적·관리적 보호조치 기준」(이하 '고시'라 한다) 제4조제5항은 제2호에서 "정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위하여 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지할 수 있는 시스템을 설치·운영"하도록 규정하고, 같은 조 제10항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 동안만 최대 접속시간 제한 등의 조치"를 하도록 규정하고 있다.

2. 위법성 판단

가. 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위 관련

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.

조사결과, 피심인은 웹 방화벽(펜타시큐리티시스템, WAPPLES-2200), 침입탐지 및 차단 기능이 포함된 침입방지시스템(시큐아이, SECUI MFI 2100)을 설치하였다.

다만 시스템의 '운영'은 단순히 시스템의 전원을 켜 놓은 상태를 의미하는 것이 아니라 침입차단 및 침입탐지 목적 달성에 필요한 기능을 활용하는 것을 의미하고, 단순히 시스템의 전원을 켜 놓은 상태나 침입차단 및 침입탐지에 필요한 기능을 활용하지 못한 상태 등은 '운영'이라고 할 수 없다.

피심인은 침입방지시스템을 이용하여 초당 500회 이상의 HTTP request 발생에 대한 탐지 차단 정책을 시행하였다고 하나, 이는 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하기 위한 정책으로 보기 어렵다.

또한 피심인은 데이터베이스에서 쿼리당 100건 이상을 조회하는 경우 경고를 보내도록 정책설정이 되어 있다고 주장하고 있으나, 이는 내부 데이터베이스에서 한 번에 다량의 개인정보를 조회하는 것을 탐지하기 위한 것으로 본 건 유출사고와 같이 외부로부터의 비정상 조회 등의 공격행위를 탐지하는 조치로 볼 수 없다.

피심인은 고시 및 해설서에 구체적으로 초당 몇 회 이상의 조회 건수가 발생할 경우 이를 탐지할 수 있어야 한다는 요구사항이 포함되어 있지 않다고 주장하고 있으나, 외부 IP 또는 한 개의 ID에서 초당 35회 이상 개인정보를 조회하는 행위는 명백히 사람이 할 수 없는 비정상 행위이고, 피심인의 업무 특성을 파악하여 외부 IP에서 개인정보취급자가 통상적으로 개인정보를 조회하는 횟수 이상의 조회가 발생하는 경우 탐지·차단이 될 수 있도록 침입탐지시스템을 운영하였다면 대량의 개인정보 유출을 충분히 방지할 수 있었다.

따라서 이 사건의 해커가 외부 IP에서 통상적인 업무 시간 이후(20:00~05:02)에 피심인의 관리자페이지에 접속하여 초당 최대 35회, 총 1,233,859건(1,117,227명)의 개인정보를 조회하여 유출하였음에도 피심인이 이를 탐지하지 못하는 등 침입차단 및 탐지시스템 운영을 소홀히 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

나. 개인정보처리시스템인 관리자페이지의 최대 접속시간 제한조치를 하지 않은 행위 관련

피심인은 개인정보처리시스템인 관리자페이지(　　)의 최대 접속시간이 60분으로 설정되어 있었으나, CS 상담원의 업무 특성상 원할한 상담을 위하여 관리자 페이지 중 일부인 공지사항 부분을 1분 간격으로 로딩되도록 설정하는 것이 불가피하였다고 주장하고 있다.

고시 해설서는 "최대 접속시간 제한 조치는 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속을 차단하는 것을 의미하며, 최대 접속시간이 경과하면 개인정보처리시스템과 연결이 완전히 차단되어 정보의 송·수신이 불가능한 상태가 되어야 한다."라고 설명하고 있는바,

피심인은 개인정보처리시스템에 대한 개인정보취급자의 최대 접속시간을 60분으로 설정하였으나 1분 간격으로 자동 로딩이 이루어지도록 함으로써, 결과적으로 60분이 경과하더라도 개인정보처리시스템과 계속 연결되어 정보의 송·수신이 가능하도록 하였다.

이는 피심인이 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취하지 않은 것으로 볼 수 있다.

따라서 피심인이 위와 같은 행위를 통해 해커가 신○○의 세션ID를 탈취하고 관리자페이지에 접속할 수 있는 빌미를 제공하여 이용자의 개인정보가 유출되게 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제5호 및 고시 제4조제10항을 위반한 것이다.

<참고 10> 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 탐지시스템 설치·운영을 소홀히 한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②5호	개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취하지 않은 행위(고시§4⑩)

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 다음과 같은 기술적·관리적 보호조치를 취하여야 한다.

① 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·운영할 것

② 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취할 것

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 11> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

피심인은 시정조치 명령 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하여야 하며, 그 실시결과를 포함한 재발방지대책을 수립하여 처분 통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

Ⅴ. 과징금 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항제6호, 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 제64조의3제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업년도의 연평균 매출액의 100분의 3 이하에 해당하는 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 학원 및 온라인 교육서비스( )를 운영하는 정보통신망법 제2조제1항제3호에 따른 정보통신서비스 제공자로서 ▲피심인이 2017. 7. 25. 기준 보관·관리하고 있던 개인정보량이 1,539,137명으로 매우 방대하고, ▲정보통신망법 제28조제1항제2호에 따른 접근통제의 기술적·관리적 보호조치 중 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ▲개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 유지되도록 최대 접속시간을 제한하는 조치를 취하지 않은 행위로 이 사건의 해커에 의해 이용자의 개인정보가 유출되게 하는 빌미를 제공하였으므로, 피심인에게 중과실이 있다고 판단한다.

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 따라, 피심인의 위반행위의 결과가 ▲위반행위로 인한 개인정보의 피해규모가 피심인이 보유하고 있는 개인정보의 100분의 5 이상{2017. 7. 18. 기준, 피심인의 온라인 교육서비스인 ' ' 이용자의 개인정보 1,233,859건(중복제거 1,117,227명)}이나, ▲위반행위로 직접적으로 이득을 취득하지 않은 점, ▲이용자의 개인정보가 공중에 노출되지 않은 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 감경하여 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

피심인의 위반행위와 관련된 온라인교육서비스( )의 직전 3개 사업년도의 연평균 매출액으로 환산한 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 원으로 한다.

<참고 12> 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 부과기준율

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

다. 필수적 가중 및 감경

'부과기준' 제6조와 제7조에 따라 위반행위의 기간이 1년 이내(2017. 2. 28. ~ 2017. 9. 2.까지)인 '단기 위반행위'에 해당하므로 가중 없이 기준금액을 유지한 금액인 원으로 하고,

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

라. 추가적 가중 및 감경

'부과기준' 제8조에 따라 이번 개인정보 유출사고 시 자진 신고한 사실 및 방송통신위원회 등 관계기관의 조사에 피심인이 적극 협조한 점 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액 원에서 100분의 10에 해당하는 금액인 원을 감경한 원으로 한다.

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 '부과기준'에 따라 위에서 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 이상 10억원 미만에 해당하여 백만원 미만을 절사한 **219,000,000**원을 최종 과징금으로 결정한다.

<참고 13> 과징금 산출내역

기준금액	필수적 가중·감경	추가적 가중·감경	**최종 과징금***
원	필수적 가중 없음 필수적 감경 (50%, 원)	추가적 가중 없음 추가적 감경 (10%, 원)	**219백만원**
	→ 원	→ 원	

* 최종 과징금 산출액이 1억원 이상 10억원 미만에 해당하여 백만원 미만은 절사함

Ⅵ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '과태료 부과 등 처리지침'이라 한다)에 따라 다음과 같이 부과한다.

1. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과 등 처리지침 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 적용한다.

<참고 14> 위반 횟수별 과태료 금액

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조 제1항제3호	1,000	2,000	3,000

2. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과 등 처리지침 제9조는 ▲위반행위가 2개 이상인 경우, ▲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 경우에는, 과태료 부과 등 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

그러나 피심인의 정보통신망법 제28조제1항 위반행위는 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

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

그러나 피심인의 정보통신망법 제28조제1항 위반행위는 이와 관련하여 특별히 해당사항이 없으므로 과태료를 감경하지 않는다.

<참고 15> 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§28①2호	1,000만원	없음	없음	**1,000만원**
계				**1,000만원**

3. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,000만원의 과태료를 부과한다.

Ⅴ. 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 부과처분에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 방송통신위원회에 행정심판청구 또는 관할법원에 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 방송통신위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 방송통신위원회의 과태료 부과처분은 「질서위반행위규제법」 제20조제2항의 규정에 따라 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)