방 송 통 신 위 원 회
심의 · 의결

안건번호 제2019 - 57 - 304호

안 건 명 통신사 영업점 등 개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2019. 11. 22.

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. 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.

나. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 한다.

2. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

3. 피심인은 제1항부터 제2항까지의 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 과태료를 부과한다.

가. 금　　액 : 13,000,000원

나. 납부기한 : 고지서에 명시된 납부기한 이내

다. 납부장소 : 한국은행 국고수납 대리점

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

이　　유

Ⅰ. 기초 사실

(이하 '피심인'이라 한다)는 영리를 목적으로 홈페이지를 통해 온라인 교육서비스를 제공하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황과 최근 3년간 매출액은 다음과 같다.

< 피심인의 일반현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수('18.3.2.기준)

< 피심인의 최근 3년간 매출액 >

(단위 : 백만원)

구 분	2016년	2017년	2018년	3년 평균
전체 매출				
관련 매출				
관련없는 매출*				

※ 자료 출처 : 피심인이 제출한 재무제표 등 회계자료를 토대로 작성

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 피심인이 보관, 관리하는 이용자의 개인정보가 미상의 해커(이하 '이 사건 해커'라 한다)에 의해 약 125만명의 회원정보가 유출되었다는 피심인의 신고(2018. 3. 2.)를 접수하였다.

※ 유출인지 : 보안관제 서비스 업체 로부터 웹셸 업로드 및 개인정보 유출 추정 관련 내용을 통보받아 인지('18.3.1. 17:00)

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(2018. 3. 2. ~ 2018. 4. 26.)한 바, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 온라인 교육 서비스 를 제공하면서 2018. 3. 2. 기준 건의 개인정보를 수집하여 보관하고 있다.

< 피심인의 개인정보 수집현황 >

구 분	항 목	수집일	건수
이용자 정보 (휴면 포함)	아이디(전화번호), 이름, 이메일, 비밀번호, 주소, 생년월일, 성별, 학부모전화번호, 학부모이름		건

나. 유출 규모

피심인이 온라인 교육 서비스를 제공하기 위해 웹페이지 를 운영하면서 수집한 2018. 3. 2. 기준의 회원정보(아이디, 이름, 성별, 생년월일, 전화번호, 핸드폰번호, 이메일, 주소 등) 총 건*의 개인정보가 외부에 유출된 것으로 추정된다.

* 피심인의 웹서버 기록을 분석(2018.3.15.)한 결과, 2018.3.1. 11:00:37경 웹셸 업로드를 통하여 외부에서 파일(, 382Mbyte)을 다운로드한 것은 확인되나, 다운로드 파일에 개인정보가 포함되어 있는지는 확인 불가

다. 유출 경로

1) 파일업로드 취약점을 이용한 웹셸 업로드

이 사건 해커는 2018. 2. 28. 09:01:36부터 2018. 3. 1. 11:09:33까지 IP(221.157.125.)에서 홈페이지에 접속한 후, 이용후기를 작성하는 게시판의 파일업로드 취약점을 이용하여 총 7개의 웹셸(WeShell) 등을

업로드하였다.

< 해커가 업로드한 웹셸 등의 파일명 및 생성일시 >

	파일명	위치	생성일시	비고
1			2018.02.28. 09:46:53	웹쉘
2			2018.02.28.09:48:01	
3			2018.03.01.10:17:00	생성
4			2018.03.01.10:17:32	한줄 웹쉘
5			2018.03.01.10:46:12(추정)	웹쉘
6			2018.03.01.10:54:11(추정)	개인정보 유출에 사용
7			2018.03.01. 11:09:33(추정)	웹쉘

2) 업로드한 웹셸을 이용하여 개인정보 조회

이 사건 해커는 2018. 3. 1. 10:56:05에 업로드한 웹셸(로 추정)을 이용하여 개인정보를 조회하는 명령어를 입력하였다.

< 해커가 입력한 명령어 >

3) 개인정보 추정되는 파일 생성 후 다운로드

이 사건 해커는 조회한 개인정보로 파일을 생성하여 2018. 3. 1.

11:00:37경 특정 IP(221.157.125.)에서 다운로드하였다.

< 해커의 유출 파일 화면 >

라. 개인정보의 기술적·관리적 보호조치 등 사실 관계

1) 개인정보의 불법적인 접근차단을 위한 침입차단·탐지시스템{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**운영을 소홀히 한 행위**

피심인은 에스케이인포섹㈜와 2014. 3. 1.부터 보안관제서비스 계약을 체결하고 방화벽 , IPS시스템 , 웹쉘 및 악성코드 탐지 서비스를 제공받고 있었으나, 2018. 3. 1. 11:09분경 파일 실행을 탐지한 것 외에 6개 웹쉘에 대해서 탐지·차단하지 못한 사실이 있다.

2) 악성 프로그램 등을 방지, 치료{정보통신망법 제28조(개인정보의 보호조치) 중 백신소프트웨어 설치·운영 보호조치}**할 수 있는 보안 프로그램을 설치·운영하지 않는 행위**

피심인은 2018. 3. 1. 당시 홈페이지에서 이용후기를 작성하는 경우 SmartEditor Basic(2.8.2)버전을 통해 작성하도록 하였으나 해당 SmartEditor Basic(2.8.2)는 2016. 7월경 파일 업로드 기능을 통한 WebShell 업로드 및 시스템 명령어 사용이 가능한 취약점이 발견되어 제조사인 네이버, 인터넷침해대응센터

(KISA)에서 2.8.2.1.로 보안 업데이트를 공지(2016. 7. 19.)하였으나 업데이트를 하지 않고 사용한 사실이 있다.

3) 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리{정보통신망법 제29조(개인정보의 파기) 중 유효기간제}하지 않은 행위

피심인은 온라인 교육 서비스 를 제공하면서 해당 서비스 등을 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보(2018. 4. 26. 기준, 563,935건)를 파기하거나 서비스를 이용하는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2019. 4. 18. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2019. 5. 7. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 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)', '백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해방지 조치(제5호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단

하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 등을 조치하여야 한다"고 규정하고 있고, 제5항은 "정보통신서비스 제공자 등은 개인정보처리시스템 및 개인정보취급자가 개인정보에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다"라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적 · 관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '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 제7조는 "정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하고, 제1호에 보안프로그램의 자동 업데이트 기능을 사용하거나, 도는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지, 제2호에는 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 한다. "라고 규정하고 있다.

'고시 해설서'는 고시 제7조에 대해 "정보통신서비스 제공자등은 개인정보처리시스템, 컴퓨터 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치하여야 하며, 보안 프로그램은 그 목적과 기능에 따라 다양한 종류의 제품이 있으므로, 정보통신서비스 제공자등은 스스로의 환경에 맞는 보안 프로그램을 설치하도록 한다."라고 해설하고 있다.

나. 정보통신망법 제29조제2항은 "정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다."라고 규정하고 있고, 같은 법 시행령(대통령령 제27510호, 2016.9.22.) 제16조제2항은 "정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간(1년) 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다."라고 규정하고 있다.

다. 정보통신망법 제64조제3항은 "방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반한 사실이 있다고 인정되면 소속공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다."라고 규정하고 있다.

2. 위법성 판단

가. 개인정보의 불법적인 접근차단을 위한 침입차단·탐지시스템{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**운영을 소홀히 한 행위**

피심인이 2017. 4월경부터 웹셸 및 웹 악성코드 탐지를 수행하고 있었으나, 2018. 3. 1. 11:09 파일 실행을 탐지한 것 외에 6개 웹쉘에 대해서 침입탐지·차단하지 못한 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항, 고시 제4조제5항을 위반한 것이다.

나. 악성 프로그램 등을 방지, 치료{정보통신망법 제28조(개인정보의 보호조치) 중 백신소프트웨어 설치·운영 보호조치}**할 수 있는 보안 프로그램을 설치·운영하지 않는 행위**

피심인이 SmartEditor Basic(2.8.2)에 대하여 2016. 7월경 파일 업로드 기능을 통한 WebShell 업로드 및 시스템 명령어 사용이 가능한 취약점 해결을 위한 보안 업데이트(2.8.2.1.버전)를 하지 않은 행위는 정보통신망법 제28조제1항제5호, 같은 법 시행령 제15조제5항, 고시 제7조를 위반한 것이다.

3) 서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리{정보통신망법 제29조(개인정보의 파기) 중 유효기간제}**하지 않은 행위**

정보통신서비스 제공자 등은 정보통신망법 제29조제2항에 따라 2015. 8. 18.부터 이용자가 정보통신서비스를 1년 동안 이용하지 아니한 경우 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도 저장·관리하여야 하나,

피심인이 2017. 4. 26. 이후에 온라인 교육 서비스( )를 1년 이상 이용하지 않은 이용자의 개인정보(이름, 성별, 생년월일, 이메일, 주소, 연락처 등) 총 563,932건을 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않아, 개인정보 유효기간제를 적용하지 않은 행위는 정보통신망법 제29조제2항, 같은 법 시행령 제16조제2항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 운영을 소홀히 한 행위(고시§4⑤)
	악성프로그램 방지	§28①5호	§15⑤	개인정보를 안전하게 관리하기 위해 백신소프트웨어의 설치·운영에 대한 보호조치를 하지 않은 행위(고시§7)
	유효 기간제	§29②	§16②	서비스를 이용하지 않는 이용자의 개인정보를 파기 또는 별도로 저장·관리하지 않은 행위

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) 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. 2) 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 한다.

나. 피심인은 이용자가 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.

2. 시정명령 이행결과의 보고

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.

Ⅴ. 과징금 부과

피심인의 위반행위는 정보통신망법 제64조의3제1항제6호에 따라 이용자의 개인정보가 분실·유출된 경우로서 개인정보 보호조치(제28조제1항)를 하지 않은 경우에 해당하여, 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과할

수 있으나,

피심인의 경우 개인정보 유출사실을 확인할 수 없는 점을 고려하여 과징금 부과를 시정명령으로 갈음하되, 차후 수사기관에서 해커를 검거하여 유출이 확인될 경우, 과징금을 부과 재처분한다.

Ⅵ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항, 제29조(개인정보의 파기)제2항에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 같은 법 시행령 제74조의 [별표9] 및 「개인정보 및 위치정보의 보호 위반행위에 대한 과태료 부과지침」(이하 '과태료 부과지침'이라 한다)에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과지침 제6조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 각 적용한다.

〈 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
더. 법 제29조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조 제1항제4호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** 과태료 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보 제공 등 조사방해, ▲위반의 정도, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 가중할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위가 2개에 해당하는 경우이므로 기준금액의 100분의 30인 300만원을 가중하고, 같은 법 제29조제2항 위반행위에 대해서는 특별히 해당사항이 없으므로 과태료를 가중하지 않는다.

< 과태료 부과지침 [별표2] '과태료의 가중기준' >

위반의 정도	나. 제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우	기준금액의 30% 이내
	제3호 정보통신망법 시행령 제74조 별표 9 제2호 너목	
	가. 정보통신망법 제28조제1항제1호에 따른 개인정보를 안전하게 취급하기 위한 내부 관리계획의 수립·시행을 하지 않은 경우	
	나. 정보통신망법 제28조제1항제2호에 따른 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 하지 않은 경우	
	다. 정보통신망법 제28조제1항제3호에 따른 접속기록의 위조·변조 방지를 위한 조치를 하지 않은 경우	
	라. 정보통신망법 제28조제1항제4호에 따른 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하지 않은 경우	
	마. 정보통신망법 제28조제1항제5호에 따른 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치를 하지 않은 경우	
	바. 정보통신망법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하지 않은 경우	

2) **(과태료의 감경)** 과태료 부과지침 제7조는 ▲당사자 환경, ▲사업규모와 자금사정, ▲개인(위치)정보보호 노력정도, ▲조사협조 및 자진시정, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우에는, 기준금액의 2분의 1까지 감경할 수 있다고 규정하고 있다.

이에 따라 피심인의 정보통신망법 제28조제1항 및 제29조제2항 위반행위에 대해 시정조치(안) 사전통지 및 의견제출 기간 내에 시정이 완료된 점을 고려하여 기준금액의 100분의 50인 500만원을 각 감경한다.

< 과태료 산출내역 >

위반조문	기준금액	가중	감경	최종 과태료
§28①2·5호	1,000만원	300만원	500만원	**800만원**
§29②	1,000만원	없음	500만원	**500만원**
계				**1,300만원**

다. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항, 제29조제2항 위반행위에 대해 1,300만원의 과태료를 부과한다.

Ⅶ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 및 제76조제1항제3호·제4호(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 서면

으로 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.

이에 주문과 같이 의결한다.

2019년 11월 22일

위 원 장 한 상 혁 (인)

부위원장 김 석 진 (인)

위 원 허 욱 (인)

위 원 표 철 수 (인)

위 원 김 창 룡 (인)