방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 30 - 162호

안 건 명 ㈜ 의 개인정보 유출사고에 대한 시정조치에 관한 건

피 심 인 ㈜

대표이사
(사업자등록번호 : , 법인등록번호 :)

의 결 일 2017. 9. 8.

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, ②접속기록의 위조·변조 방지를 위한 조치를 하여야 하며, ③개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 기술적·관리적 보호조치를 하여야 하고, ④정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 위 1년이 경과한 후 위 이용자의 개인정보를 즉시 파기하거나 정보통신서비스를 이용하고 있는 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하는 등 필요한 조치를 하여야 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 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

3. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 분실·도난·유출 등을 방지하기 위한 재발방지 대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

4. 피심인에 대하여 다음과 같이 과징금과 과태료를 각 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 25,000,000원

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

5. 피심인에 대하여 정보통신망법 제69조의2제2항에 따라 개인정보 유출 및 정보통신망법 위반과 관련하여 피심인의 대표자 및 책임 있는 임원을 포함한 책임자에 대해 징계할 것을 권고한다. 피심인은 이를 존중하여야 하며 그 결과를 처분통지를 받은 날로부터 90일 이내에 방송통신위원회에 통보하여야 한다.

이 유

Ⅰ. 기초 사실

㈜ (이하 '피심인'이라 한다)은 영리를 목적으로 숙박O2O[1] 어플리케이션인 ' ' 등을 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	
			전체	정보보호
		원	명	명(0.5%)

<참고 2> 피심인의 최근 3년간 매출액

(단위 : 천원)

구 분	2014년	2015년	2016년	합 계	3년 평균*
전체 매출					
관련 매출					
관련 없는 매출**					

※ 자료 출처 : ㈜ 이 제출한 재무제표 등 회계자료를 토대로 작성

* 사업개시 후 3년이 되지 않아, 정보통신망법 시행령 제69조의2제1항 단서에 따라 사업개시 후 '16년 말까지의 매출액을 연평균 매출액으로 환산

** ' ' 수수료 매출 등은 관련 없는 매출로 분류

1) O2O(Online to Offline)란 온라인과 오프라인이 결합하는 현상을 의미하는 말로, 최근에는 주로 전자상거래 혹은 마케팅 분야에서 온라인과 오프라인이 연결되는 현상을 말하는 데 사용된다. ' '는 이용자가 모바일 어플리케이션(온라인)을 통해 다양한 숙박 장소(오프라인)를 예약할 수 있도록 연결해주는 서비스를 제공한다.

Ⅱ. 사실조사 결과

1. 조사대상

피심인이 보관, 관리하는 이용자의 개인정보가 .경부터 .경까지 중국인 해커[2](이하 '이 사건 해커'라 한다)에 의한 SQL-Injection[3] 공격방식의 해킹으로 외부로 유출됨에 따라,

방송통신위원회는 과학기술정보통신부(舊 미래창조과학부)와 합동으로 구성한 민관합동조사단[4]과 함께 피심인을 대상으로 피심인으로부터 넘겨받은 사고관련 자료{피해시스템 총 대(서비스 웹서버 대, 서비스 관리 웹서버 대, 공격 시스템 대, 숙박이용 내역 문자 발송 악용 서버 대) 등}와 개인정보취급자가 피심인의 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. 3. 23. ~ 5. 11.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 유출 규모

피심인이 ' ' 서비스를 운영하면서 수집한 기준의 숙박 예약정보 총 건(중복제거 시 명)과 회원정보 건(식별정보

2) 경찰청 사이버수사과는 중국인 해커(26세) 등 피의자 4명을 검거하고 해외 체류 중인 피의자 1명을 추적하고 있음

3) SQL(Structured query language) Injection 이란 데이터베이스에 대한 질의 값(SQL 구문)을 조작하여 정상적인 자료 이외에 공격자가 원하는 자료까지 데이터베이스로부터 유출 가능한 공격기법을 말한다.

4) 정보통신망법 제48조의4제2항 : 미래창조과학부 장관은 중대한 침해사고 발생 시 피해확산 방지 및 사고 대응, 복구 및 재발방지를 위하여 민관합동조사단을 구성하여 침해사고 원인 분석을 수행
* 민관합동조사단(12명) : 미래부 정보보호정책관(단장) 등 공무원 5명, 민간 2명, · KISA 5명으로 구성

명)이 외부로 유출되었다.

<참고 3> ㈜ 의 유출 정보 현황

구 분		유 출 항 목	건수	명수
이용자 정보	숙박 예약 정보	숙박수(구분), 제휴점명, 객실명, 예약일시, 예약자, 회원번호, 휴대전화번호, 결제방법, 결제금액, 원금액, 입금가, 예약현황, 입·퇴실(가능)시간 등	건	명*
	회원 정보	회원번호, 회원ID(이메일주소), 이름(또는 닉네임), 가입일자, 가입수단, 회원등급, 가입환경(OS정보) 등	건	명**
소 계		-	건	명***
사업자(제휴점) 정보****		업체번호, 업체명, 은행명, 계좌번호, 예금주, 연락처(휴대전화번호), 생년월일(사업자번호), 영업담당자, 회원등록상태, 등록일	건	명
합 계		-	건	명

* 숙박예약정보 건을 휴대전화번호 기준으로 중복 제거

** 회원정보 중 이메일주소가 저장되어 있어 특정 개인을 식별할 수 있는 회원 수

*** 숙박예약정보와 회원정보 중 회원번호 등을 기준으로 동일인으로 파악된 명 제외

**** ㈜ 과 계약관계에 있는 사업자의 정보로 정보통신망법 상 이용자의 개인정보로 보기는 어려움

나. 유출 경로

1) DB자료 수집

이 사건 해커는 IP주소( )에서 부터 피심인이 운영하고 있는 ' ' 서비스와 관련한 DB 내 자료 중 공격에 유효한 정보를 파악하기 위하여 서비스 관련 웹페이지 중 하나인 마케팅센터의 일부 경로 (https://)에 SQL-Injection 공격을 수행하여 IP주소( )에서 부터 까지 ' ' 서비스의 DB자료(DB 구조, 테이블, 테이블 스키마)를 유출하여 수집하였다.

2) 관리자 인증 세션 탈취

이 사건 해커는 IP주소(　　)에서　　부터　　까지 SQL-Injection 공격으로 '　　' 서비스 관리자페이지(이하 '관리자 페이지'라 한다.)(https://　　)에 접속하기 위한 정보가 저장되는 DB내　　테이블의 구조를 파악하였다.

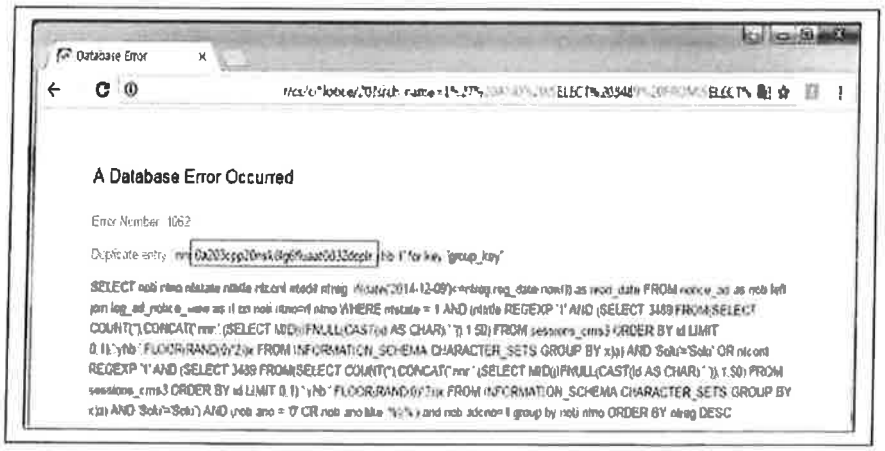
<참고 4>　　테이블 구조

구분	필드명	설명	공격자 악용
1			관리자 권한 접속에 악용
2			
3			
4			

<참고 5>　　테이블 내 데이터 예시

그리고 이 사건 해커는 IP주소(　　)에서　　부터　　까지 SQL-Injection 공격으로 관리자페이지에 접속하기 위한 정보(관리자 인증 세션 값)를　회 조회 및 유출하였다.

<참고 6> SQL-Injection 공격(관리자 인증 세션 값 유출 재연)



참고로 이 사건 해커는 총 7개의 IP주소(포함)에서 부터 까지 SQL-Injection 공격으로 관리자페이지의 관리자 권한 접속 정보(관리자 인증 세션 값 포함)를 회 조회 및 유출하였다.

<참고 7> SQL-Injection 공격(관리자 인증 세션 값 유출 IP주소, 시간, 횟수)

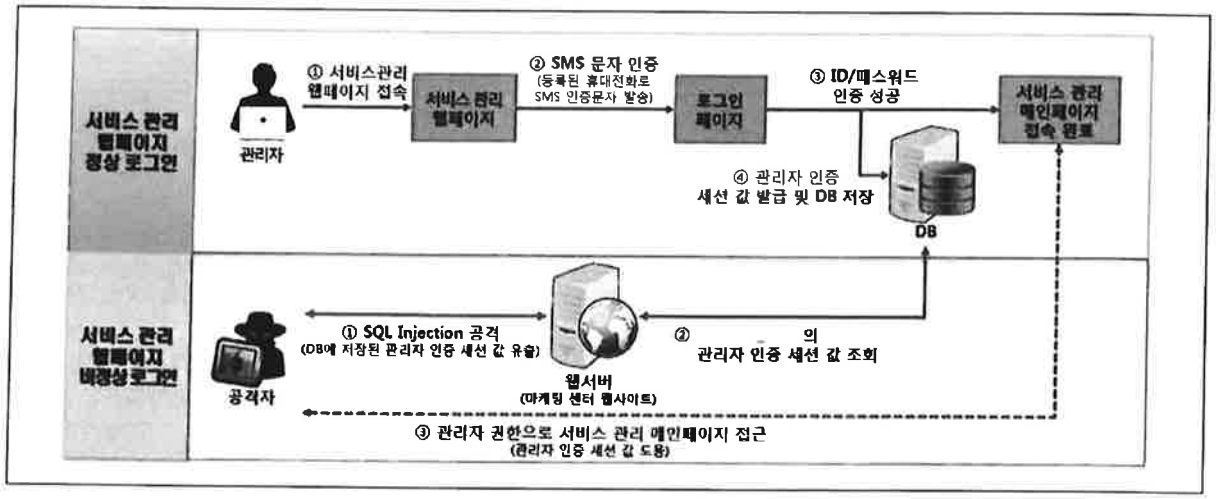
구분	IP주소	국가 코드	유출 시간	유출 횟수
1		KR	2017.03.06. 23:11:41 ~ 2017.03.07. 00:16:57	63
2		KR	2017.03.07. 03:49:28 ~ 2017.03.07. 04:05:59	188
3		KR	2017.03.09. 23:12:12 ~ 2017.03.09. 23:27:03	325
4		CN	2017.03.17. 13:46:55 ~ 2017.03.17. 13:47:06	7
5		KR	2017.03.17. 13:48:16 ~ 2017.03.17. 14:00:41	143
6		CN	2017.03.21. 21:21:50 ~ 2017.03.21. 21:21:59	18
7		KR	2017.03.21. 21:23:06 ~ 2017.03.21. 21:23:43	44

3) ' ' 서비스 관리자페이지 접속

피심인은 관리자페이지에 개인정보취급자가 접속하는 경우 회사 내부에서는 아이디, 비밀번호로 접속을 할 수 있고, 외부에서는 아이디, 비밀번호 외 휴대전화 인증을 거친 후 접속이 가능하도록 하였으나, 이 사건 해커는 IP주소 ( )에서 에 SQL-Injection 공격으로 탈취한 관리자 인증 세션 값을 도용하여 외부에서 아이디, 비밀번호, 휴대전화인증을 우회하여 관리자페이지에 접속하는 데 성공하였다.

이때 이 사건 해커가 IP주소( )에서 관리자페이지에 접속 시 도용한 관리자 인증 세션 값은 피심인의 직원인 의 인증 세션 값으로 확인되었으며, 이후 IP주소( )에서 에 피심인의 직원인 의 인증 세션 값을 도용하여 관리자페이지에 접속하였다.

<참고 8> 해커의 관리자 인증 세션 값 유출 및 도용 개요도



<참고 9> ‘ ’ 서비스 관리자페이지에 해커가 접근한 이력

구분	IP주소	국가	접속 시간
1		KR	2017.03.06. 23:19:18 ~ 2017.03.08. 20:57:11
2		KR	2017.03.07. 00:58:38 ~ 2017.03.07. 15:00:32
3		KR	2017.03.08. 22:24:26 ~ 2017.03.10. 15:31:13
4		KR	2017.03.17. 13:48:16 ~ 2017.03.17. 13:56:57
5		KR	2017.03.21. 21:29:44 ~ 2017.03.21. 21:33:11

4) 개인정보 유출

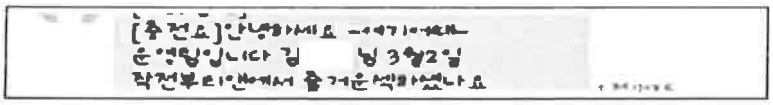
이 사건 해커는 IP주소( )에서 에 의 인증 세션 값을 도용하여 관리자페이지에 접속한 후 부터 까지 “예약” 메뉴에서 파일 다운로드 기능(“CSV 다운로드” 버튼)을 이용하여 이용자 명의 숙박 예약정보 건을 CSV파일로 유출하였고, IP주소( )에서 부터 까지 “회원관리” 메뉴에서 이용자 건의 회원정보를 조회 및 유출하였으며, IP주소( )에서 에 “자동이체 등록 제휴점 관리” 메뉴에서 파일 다운로드 기능(“Excel 다운로드” 버튼)을 이용하여 숙박업소 사업자 명의 정보를 xls파일로 유출하였다.

<참고 10> 해커의 자료 유출 현황

구분	IP주소	유출 시간	유출 정보
1		2017.03.07. 01:12:39 ~ 03:40:59	숙박예약정보
2		2017.03.10. 00:48:29 ~ 15:19:54	회원정보
3		2017.03.17. 13:54:25	제휴점정보

이 사건 해커는 피심인으로부터 탈취한 이용자의 개인정보를 활용하여 부터 까지 3차례 총 명의 이용자들에게 숙박 이용내역에 대한 문자를 발송하였고, 페이스 북에 탈취한 이용자의 개인정보 중 건을 게시하였다.

<참고 11> 해커가 발송한 문자 내용



<참고 12> 해커의 문자 발송 현황

구분	발송 일시	발송 건수
1차	2017.03.21. 07:15	건
2차	2017.03.22. 00:40	건
3차	2017.03.23. 16:50	건
합계	-	건

이 사건 해킹사고로 인하여 피심인이 저장·관리하던 총 건의 개인정보가 유출되었는데 유출항목은 숙박예약정보의 숙박수(구분), 제휴점명, 객실명, 예약일시, 예약자, 회원번호, 휴대전화번호, 결제방법, 결제금액, 원금액, 입금가, 예약현황, 입·퇴실(가능)시간 등이고, 회원정보의 회원번호, 회원ID(이메일주소), 이름(또는 닉네임), 가입일자, 가입수단, 회원등급, 가입환경(OS정보) 등이며, 제휴점의 업체명, 은행명, 계좌번호, 예금주, 연락처(휴대전화번호), 생년월일

(사업자번호), 영업담당자, 회원등록상태, 등록일 등이다.

다. 개인정보 유출 경로 요약

이 사건 해킹의 방법 및 절차 등은 크게 4단계로 구분해볼 수 있는데,

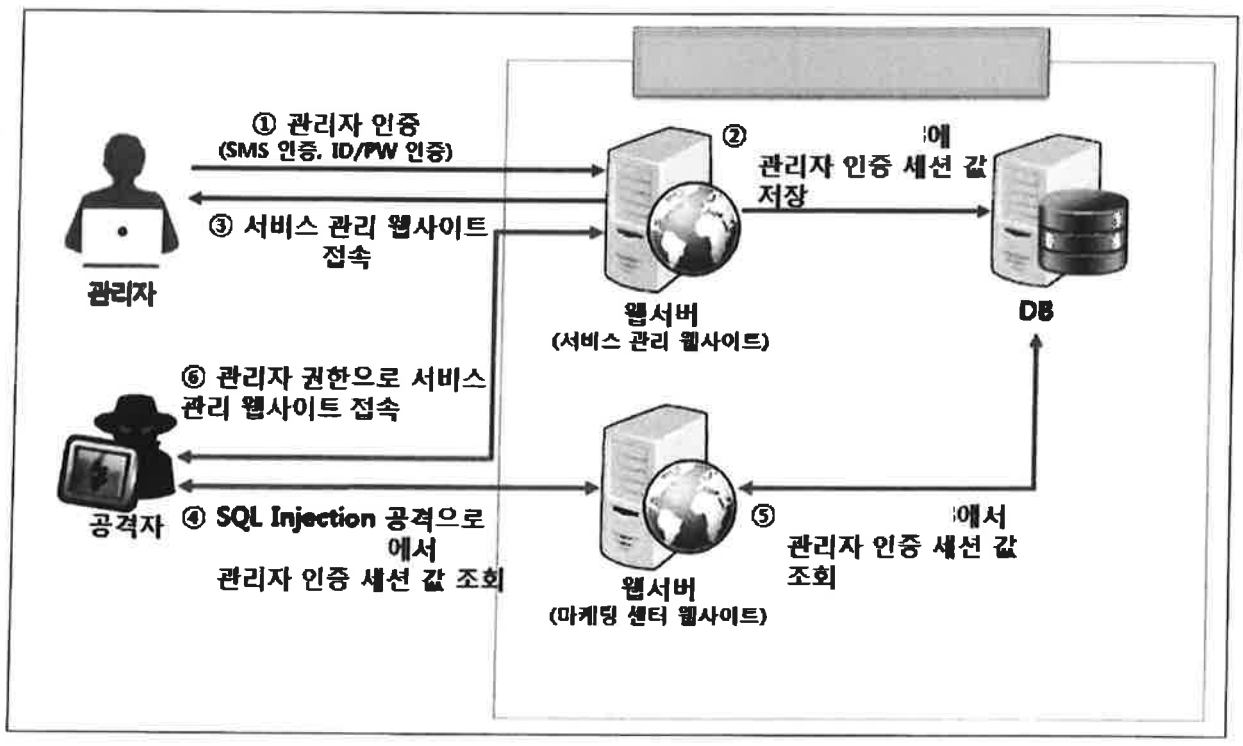
1 해커는 SQL-Injection 공격으로 ' ' 서비스의 DB정보를 수집하고,

2 DB의 테이블에서 관리자 인증 세션 정보를 탈취하여,

3 ' ' 서비스 관리자페이지에 최고관리자 권한으로 접속한 후,

4 ' ' 서비스 관리자페이지의 파일 다운로드 기능을 이용하여 개인정보를 다운로드 받아 유출한 것으로 조사되었다.

<참고 13> 사고 개요도



3. 개인정보의 기술적·관리적 보호조치 등 사실 관계

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

1) 접근권한 부여

피심인의 관리자페이지의 접근권한은 99번, 98번, 95번, 90번, 85번, 80번, 79번, 75번, 74번, 73번, 71번, 70번, 69번, 65번, 61번, 50번, 41번, 39번, 35번, 31번, 5번, 2번, 1번 등 총 24개로 Level로 분류하고 있고, 각 권한에 대하여 상태1은 이용할 수 있는 상태, 상태2는 이용할 수 없는 상태로 관리하고 있었으며, 이중 개인정보 파일을 다운로드 할 수 있는 접근권한 Level은 99번, 98번, 95번, 90번, 39번, 35번, 33번, 31번으로 총 8개이다.

피심인은 당시 관리자페이지(https://)의 파일 다운로드 권한을 99번(최고관리자) 27명, 98번(개발팀) 20명, 90번(운영자) 36명, 39번(고객센터 관리자) 2명, 35번(고객센터 조장) 8명, 31번(고객센터 상담사) 35명 등 총 128명에게 부여하고 있었다.

피심인의 직원인 는 입사하여 까지 사업부 운영본부에서 (이하 ' '라 한다) 개선업무를 담당하였으나, 조직개편으로 TF 부문에서 업무를 담당하게 되었으며, 는 TF로 발령이 난 후 에도 개선 업무를 위해 관리자페이지에 접속하여 관련 업무를 수행하고 있었다.

피심인과 는 개선업무를 위해서는 관리자페이지의 모든 메뉴에 대한 확인이 필요하기 때문에 99번(최고관리자) 권한이 필요하다고 소명하고 있다.

한편, 피심인의 직원으로 31번(고객센터 상담사) 권한을 부여받은 은 입사

후부터 까지 야간 고객센터 상담사로서 고객의 예약확인, 환불 등 응대 업무를 담당하고 있었기 때문에 관리자페이지에서 파일 다운로드 권한이 필요하지 않았으며, 실제 파일 다운로드 기능을 사용한 사실도 없었다.

피심인이 후 까지 관리자페이지의 접근권한을 변경한 내역은 확인되지 않았고, 의 경우 사고이후인 99번(최고관리자) 권한에서 69번(마케팅관리자) 권한으로 변경된 사실이 있으며, 이후 관리자페이지에서 파일 다운로드 기능을 전면 차단한 사실이 있다.

2) 침입차단시스템 및 침입탐지시스템의 설치·운영

피심인은 오픈소스( )를 이용한 침입탐지를 적용하였고, 운영체제( )에서 제공하는 기본 방화벽( )을 사용하고 있었다.

다만 개인정보에 대한 불법적인 접근을 차단하기 위하여 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템, 웹 방화벽 등의 보안장비를 도입하여 운영한 사실은 없었다.

특히 피심인의 개인정보취급자가 ' ' 서비스 이용자의 숙박예약정보 등 개인정보 파일을 외부에서 상시적으로 다운로드 받을 수 있는 기능을 만들어 놓았음에도 불구하고, 숙박예약정보 등 개인정보 파일이 외부로 전송되는 것을 탐지하도록 개인정보처리시스템에 접속한 IP주소 등을 재분석하지 않은 사실이 있다.

참고로 피심인의 개인정보취급자가 해커가 다운로드한 것 외에 외부에서 관리자 페이지로부터 숙박예약정보 등 개인정보를 다운로드 한 사실은 없다.

3) 웹페이지 취약점

* 기준 이전에 가입한 회원 수를 조회한 것으로, 조회 시점 이전에 탈퇴한 회원 수는 집계되지 않음

따라서 외부에서 개인정보처리시스템인 관리자페이지에 접속하여, 개인정보 파일을 다운로드 할 수 있는 구조가 까지 유지될 수 있었다.

5) 안전한 인증수단

피심인의 제휴점은 ' ' 서비스의 마케팅센터 웹페이지(https://:)에 접속하여 예약내역 메뉴에서 해당 제휴점에 예약한 예약자의 이름(또는 닉네임)과 연락처를 조회할 수 있으며 다운로드 또한 할 수 있다.

기준 ' ' 마케팅센터 웹페이지에 접속이 가능한 피심인의 제휴점은 총 개이며, 제휴점은 마케팅센터 웹페이지에 별도의 추가적 인증수단 없이 아이디, 비밀번호만으로 접속이 가능하다.

나. 개인정보처리시스템에 접속한 기록의 보관 및 점검 등[정보통신망법 제28조(개인정보의 보호조치) 중 접속기록의 위·변조방지]

피심인은 관리자페이지의 웹 로그 중 POST 로그[6]에 대해서는 부터 개인정보취급자를 알 수 있도록 별도로 DB에 보관하고 있었으나, GET 로그[7]는 부터 접속일시 및 수행업무만 보관하고 있어 개인정보취급자가 관리자페이지에서 개인정보를 조회, 다운로드 등 처리하는 경우 해당 개인정보취급자를 확인할 수 없다.

6) POST 방식은 URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송하는 방식으로, 게시판 등에서 파일 업로드를 하는 경우가 이에 해당한다.

7) GET 방식은 가장 일반적인 HTTP Request 형태이며, 웹 브라우저에 요청 데이터에 대한 인수를 URL을 통해 전송하는 방식으로 메신저로 알려준 URL을 클릭하여 특정 웹 페이지를 똑같이 확인할 수 있는 경우가 이에 해당한다.

특히 개인정보취급자가 직접 ‘ ’ 서비스 관련 DB에 접속하여 개인정보를 조회하는 등의 업무를 하는 경우에 대한 접속기록은 부터 보관하기 시작하였다.

피심인은 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독한 사실이 없었으며, 개인정보취급자 등이 개인정보 파일을 대량으로 다운로드 받는 경우에 대하여 별도로 점검하지는 않았다. 다만, 자체 개발 모니터링 툴을 이용하여 트래픽이 증가하는 등 하드웨어적인 이상 징후를 감지할 수 있는 통제장치는 있었다.

다. 개인정보취급자·이용자 비밀번호 및 개인정보 파일 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}

1) 비밀번호 암호화

피심인은 DB내에 저장·관리되고 있는 회원의 비밀번호 및 관리자 계정의 비밀번호 암호화 알고리즘은 PHP(ver 7.0)에서 기본으로 제공하는 SHA-1 함수를 사용하고 있었고, 관리자페이지의 접근권한을 변경한 기록에 개인정보취급자의 비밀번호를 암호화하지 않고 평문으로 저장하고 있었으며, .php 파일 내에 DB 접속계정의 비밀번호를 암호화하지 않고 평문으로 저장한 사실이 있다.

한편, 피심인은 DB내 저장·관리되고 있는 회원의 비밀번호 및 관리자 계정의 비밀번호 암호화 알고리즘에 함수를 추가로 적용하였고, DB에 보관되어 있는 이용자의 이름, 휴대전화번호에 대한 암호화 조치를 하였다.

2) 개인정보 파일 암호화

개인정보취급자의 업무용PC에 대하여 점검을 한 결과 최고관리자 권한이 있던 의 컴퓨터에 이용자의 개인정보(이름, 휴대전화번호, 숙박 장소,

숙박 일시, 숙박 유형, 결제금액 등 숙박이용자 정보 건)가 담긴 암호화되지 않은 엑셀파일(( ) 당일예약(예약내역) .xlsx)이 저장되어 있었다.

한편, 피심인은 내부관리계획 중 비밀번호 작성규칙을 통해 개인정보 취급자가 개인정보파일을 컴퓨터 등에 저장하는 경우 암호화를 하도록 하였다.

라. 개인정보 보호조직의 구성·운영{정보통신망법 제28조(개인정보의 보호조치) 중 내부관리계획 수립}

피심인은 담당자 1명이 보안업무를 병행하여 운영하는 등 사내 보안 및 운영 서비스에 대한 일관되고 지속적인 정책 수립 및 보안 조직이 부재하였으며, 이전 개인정보 처리방침을 확인하였을 때, 사업부 운영본부장인 이 개인정보보호책임자로 지정되어 있고 사업부 운영본부의 , 가 개인정보보호담당자로 지정되어 있을 뿐, 실질적인 개인정보 보호업무를 전담하는 직원은 없었다.

마. 서비스를 이용하지 않는 이용자의 개인정보에 대한 파기 등{정보통신망법 제29조(개인정보의 파기) 중 개인정보 유효기간제}

피심인은 2017. 3. 30. 기준으로 ' ' 서비스를 1년 이상(마지막 접속이력이 2016. 3. 30. 이전) 이용하지 않은 이용자의 개인정보 건을 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하지 않은 사실이 있다.

바. 처분의 사전통지 및 의견수렴

방송통신위원회는 2017. 6. 5. '개인정보보호 법규 위반사업자 시정조치(안) 사전통지 및 의견수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였고, 피심인은 2차례(1차 : 2017. 6. 19. 2차 : 2017. 8. 22.) 의견을 제출하였으며, 방송통신위원회 전체회의에서 한차례(2017. 9. 8.) 의견을 진술하였다.

정보통신망법 시행령 제15조제4항은 "법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '그 밖에 암호화 기술을 이용한 보안조치(제4호)' 등의 보안조치를 하여야 한다."라고 규정하고 있다.

다. 「개인정보의 기술적·관리적 보호조치 기준(이하 '고시'라 한다)」 고시 제2조 "이 기준에서 사용하는 용어의 뜻은 '개인정보취급자란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.(제2호)', '개인정보처리시스템이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.(제4호)', '망분리라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.(제5호)', '비밀번호라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.(제6호), '접속기록이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.(제7호)'라고 규정하고 있다.

고시 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다."라고,

고시 제4조제2항은 "정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다."라고,

고시 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다."라고,

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

1) ' ' 서비스 관리자페이지(https://)의 파일 다운로드 권한을 고객센터 상담사 35명에게 부여한 행위

고시 제4조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다."라고 규정하고 있다.

정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 '서비스 제공을 위하여 필요한' 개인정보취급자에게만 부여하여야 하는바, 보호조치 기준의 목적이 개인정보 유출 등을 방지하기 위한 '최소한의 기준'을 정하는 데 있는 점, 고시 제4조제2항에서 접근권한의 '말소' 뿐 아니라 '변경'도 규정하고 있는 점, 고시 제4조제6항에서 다운로드, 파기 등으로 접근권한을 나누고 있는 점, 개인정보취급자의 업무별 접근권한의 범위 역시 차등적으로 부여하는 것이 일반적인 현실인 점, 실제 피심인의 시스템에서도 쉽게 접근권한을 차등적으로 부여할 수 있는 점 등을 고려할 때, 접근권한의 범위는 단순히 有無의 차원이 아니라 그 질적 범위까지 따져야 하는 것으로 해석된다.

피심인의 관리자페이지는 ' ' 서비스를 이용하고 있는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어, 피심인이 접근권한을 부여한 직원 등이

접속해 데이터베이스의 이용자의 개인정보를 조회, 수정, 다운로드 등 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템으로 개인정보처리시스템에 해당한다.

앞서 살펴본 바와 같이 피심인의 관리자페이지의 접근권한은 99번, 98번, 95번, 90번, 85번, 80번, 79번, 75번, 74번, 73번, 71번, 70번, 69번, 65번, 61번, 50번, 41번, 39번, 35번, 31번, 5번, 2번, 1번 등 총 24개로 Level로 분류하고 있고, 각 권한에 대하여 상태1은 이용할 수 있는 상태, 상태2는 이용할 수 없는 상태로 관리하고 있었으며, 이중 개인정보 파일을 다운로드 할 수 있는 접근권한 Level은 99번, 98번, 95번, 90번, 39번, 35번, 33번, 31번으로 총 8개이다.

피심인은 당시 관리자페이지의 파일 다운로드 권한을 99번(최고관리자) 27명, 98번(개발팀) 20명, 90번(운영자) 36명, 39번(고객센터 관리자) 2명, 35번(고객센터 조장) 8명, 31번(고객센터 상담사) 35명 등 총 128명에게 부여하고 있었다.

그런데 피심인의 고객센터 상담사는 고객의 예약확인, 환불 등 응대 업무를 담당하고 있었기 때문에 ' ' 서비스 관리자페이지에서 파일 다운로드 권한이 필요하지 않았으며, 실제 파일 다운로드 기능을 사용한 사실도 없었다.

이에 대해 피심인은 상담사들에게 관리자페이지의 파일 다운로드 권한을 부여한 것은, 상담사들이 고객상담 및 예약상담 시 예약 세부 내역 및 취소사유를 확인하고 제휴점 업주들의 정산내역 요청 업무를 처리하기 위해서는 CSV 파일을 다운로드 받아서 확인하는 것 이외에 다른 방법이 없는 등 피심인의 업무 처리 필요성 때문이라고 주장하고 있으나,

이 사건 해커가 인증 세션 값을 도용한 관리자 중 한 사람인 은 입사 후부터 까지 야간 고객센터 상담사로서 고객의 예약확인, 환불 등 응대 업무를 담당하기 위해 31번 권한을 부여받았고, '17. 4. 21. 방송통신위원회 조사 과정에서 "업체에서 정산내역을 요청하게 되면 CMS(관리자페이지)가 아닌 마케팅

센터 페이지를 통해 CSV파일을 다운로드 받아서 보내주며, 별도로 CMS에서는 다운로드 받을 일이 없었다."라고 진술한 사실이 있으며, 실제 관리자페이지의 파일 다운로드 기능을 사용한 사실이 없는 점 등에 비추어 볼 때, 상담사에게 관리자 페이지의 파일 다운로드 권한을 부여한 것은 필요한 범위를 넘어 접근권한을 과다 부여 한 것이 된다.

따라서 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보취급자에게만 부여'하여야 하나 개인정보 조회 권한만으로 서비스 제공이 가능한 고객센터 상담사 35명 등에게 파일 다운로드 권한을 과도하게 부여함으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제1항을 위반하였다.

2) '　　' 서비스 관리자페이지 접근권한을 조직개편에 따른 인사이동 후 2주 이상 변경 또는 말소하지 않은 행위

고시 제4조제2항은 "정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다."라고 규정하고 있다. 여기서 '지체 없이'란 정당하거나 합리적인 이유가 없는 한 즉시 해야 한다는 뜻이다.

고시 해설서는 ▲"조직 내의 임직원 전보 또는 퇴직 등 인사이동을 통해 사용자 계정의 변경·삭제가 필요한 경우에는 공식적인 사용자 계정 관리절차에 따라 통제될 수 있도록 한다."라고 설명하고 있다.

피심인은　　조직개편에 따라　명을 전보 조치하였으나,　　이 되어서야　　의 접근권한을 변경,　　의 접근권한을 변경하였고, 사고를 인지하기 전까지 위 2명 외 다른 직원들의 접근권한을 변경 또는 말소한 사실이 없으며, 사고를 인지한　　이후인　　불필요한 권한을

삭제하는 등 일괄 변경한 것을 보면 조직개편에 따른 접근권한을 변경 또는 말소하지 않은 사실이 인정된다.

<참고 14> ' ' 서비스 관리자페이지의 접근권한 변경 전후 비교

권한 Level	변경 전(명)		변경 후(명)
	전체	상태1*	
99	36	27	2
98	24	20	5
95	3	-	-
90	57	36	11
85	2	-	-
80	1	-	-
79	1	1	-
75	1	1	-
74	1	1	-
73	1	-	-
71	89	54	-
70	3	2	-

권한 Level	변경 전(명)		변경 후(명)
	전체	상태1*	
69	10	8	95
65	1	1	-
61	7	4	-
50	6	-	1
41	5	5	-
39	2	2	2
35	10	8	8
33	1	-	-
31	94	35	34
5	2	-	-
2	2	-	-
1	72	61	-
합계			

* 피심인의 관리자페이지 권한 중 이용이 가능한 상태는 상태1로 구분하고 있음

특히 이 사건 해커가 유출에 사용한 의 접근권한은 파일 다운로드 권한이 있는 99번에서 파일 다운로드 권한이 없는 69번으로 변경되었으므로, 조직개편에 따라 지체 없이 접근권한을 변경 또는 말소하였다면 해당 접근권한을 이용한 개인정보 유출은 일어나지 않았을 것이다.

피심인은 는 조직개편 전후에 걸쳐 개선 업무를 담당하고 있었고, 에 조직개편으로 TF로 이동하였으나 에도 개선 업무를 하였으며, 에도 장비를 구매하는 기안을 작성하는 등 지속적으로 개선 업무를 하였기 때문에 의 접근권한을 변경·말소하지 않았다고 주장하고 있다.

그러나 피심인은 조직개편을 하면서 를 비롯한 어느 누구의 접근권한도 변경 또는 말소한 사실이 없는 점을 미루어볼 때, 피심인이 개선 업무를 위해 의 접근권한을 변경·말소하지 않았다고 보기는 어렵다. 만약 에게 해당 접근권한이 필요한 경우라면 피심인은 인사이동에 따른 접근권한을 변경하면서 공식적인 사용자 계정 관리절차에 따라 관련 접근권한을 추가로 부여하는 등의 조치를 하였어야 할 것이다.

따라서 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하나, 조직개편에 따라 명을 전보 조치하면서 관리자페이지의 접근권한을 변경하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제2항을 위반하였다.

3) 제휴점이 정보통신망을 통해 외부에서 ' ' 서비스의 마케팅센터 웹페이지(https://) 접속 시 안전한 인증수단을 적용하지 않은 행위

고시 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다."라고 규정하고 있다.

고시 해설서는 ▲"외부에서 개인정보처리시스템 접속 시 단순히 아이디와 비밀번호만을 이용할 경우, 키로깅 등에 의해 아이디와 비밀번호만 유출되어도 개인정보처리시스템이 위험에 노출되게 된다. 이러한 위험성을 감소시키기 위해 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서 등을 활용한 추가적인 인증 수단의 적용이 필요하다."라고 설명하고 있다.

피심인이 운영하고 있는 ' ' 서비스의 마케팅센터 웹페이지는 관리자

페이지와 마찬가지로 ' ' 서비스를 이용하고 있는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어 피심인의 제휴점이 해당 제휴점에 예약한 피심인의 이용자의 이름(또는 닉네임)과 연락처를 조회, 다운로드 할 수 있도록 체계적으로 구성한 데이터베이스시스템으로 개인정보처리시스템이다.

기준 ' ' 마케팅센터 웹페이지에 접속이 가능한 피심인의 제휴점은 총 개이며, 제휴점은 마케팅센터 웹페이지에 추가적인 인증수단 없이 아이디, 비밀번호만으로 접속이 가능하다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

따라서 피심인은 가맹점 직원 등이 외부에서 피심인의 개인정보처리시스템에 접속 시 단순히 아이디와 비밀번호만으로 접속할 수 있도록 하고 추가적으로 안전한 인증수단을 적용하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제4항을 위반하였다.

4) 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), 웹 방화벽 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.

피심인은 오픈소스(　　)를 이용한 침입탐지를 적용하였고, 운영체제(　　)에서 제공하는 기본 방화벽(　　)을 사용하고 있었으나, 별도로 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하거나 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템, 웹 방화벽 등의 보안장비를 도입하여 운영한 사실은 없었다.

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.

고시 제4조제5항의 입법 목적은 '정보통신망을 통한 불법적인 접근 및 침해사고 방지'이고, 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(침입차단 기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출 시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

피심인은 개인정보가 저장·관리되고 있는 이용자 수가 100만명 이상이고, 전년도 정보통신서비스 부문 매출액이 100억원 이상으로 '일정 규모 이상 사업자'[8]로서 그 사업규모, 개인정보 보유 수를 고려하여 개인정보 보호조치를 취하여야 할 것이다. 그런데 원고는 전문기업의 시스템을 설치한 것이 아니라 SOHO 등 소기업 사업자가 설치·운영할 수 있는 오픈소스( )를 이용한 침입탐지를 적용하였고 운영체제( )에서 제공하는 기본 방화벽( )을 사용하였다.

피심인의 사업 규모, 개인정보 보유 수 등을 고려할 때, 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치하지 않아 이 사건 해커의 SQL-Injection 공격을 탐지하지 못한 것은 설치의 의무를 소홀히 한 것으로 볼 수 있다.

8) '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)

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 공격을 재현하여 피심인이 적용한 오픈소스(　　)에서 해당 공격을 탐지하는지 확인한 결과, 2014. 업데이트된 오픈소스(　　) 룰을 적용한 경우에도 탐지되는 사실을 비추어 볼 때, 피심인은 오픈소스(　　)에서 해당 룰을 적용하거나 모니터링 하는 등 오픈소스(　　)를 '운영'하였다고 판단할 수 없다.

특히 피심인의 개인정보취급자가 '　　' 서비스 이용자의 숙박예약정보 등 개인정보 파일을 외부에서 상시적으로 다운로드 받을 수 있는 기능을 만들어 놓았음에도 불구하고, 숙박예약정보 등 개인정보 파일이 외부로 전송되는 것을 탐지하도록 개인정보처리시스템에 접속한 IP주소 등을 재분석하지 않은 점에서도 마찬가지로 해당 기능을 포함한 시스템을 '운영'하였다고 볼 수 없다.

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 침입탐지 시스템을 설치하지 않았고, 오픈소스(　　)를 이용한 침입탐지를 통해서도 이 사건 해커의 SQL-Injection 공격을 탐지하지 않았고, 관리자페이지의 다운로드 기능을 통해 개인정보 파일이 외부로 유출되는 것을 탐지하도록 IP주소 등을 재분석하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제5항을 위반하였다.

5) 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 망분리를 하지 않은 행위

정보통신망법 시행령 제15조제2항제3호는 '법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단' 조치를 하도록 규정하고 있다. 다만, 제3호의 조치는 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 제공자등만 해당한다.'라고 규정하고 있다.

이에 대해 고시 제4조제6항은 "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 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다."라고 규정하고 있다.

고시 해설서는 업무망과 외부 인터넷망을 분리하는 방법으로 ▲"업무망과 외부 인터넷망은 서로의 영역에 접근할 수 없도록 차단되어야 한다."라고 설명하고 있다.

피심인은 조회 시점 이전에 탈퇴한 회원 수를 제외하고 기준으로 개인정보가 저장·관리되고 있는 이용자 수가 약 명이고, 정보통신서비스 부문 매출액이 약 원인 정보통신서비스 제공자임에도 불구하고, 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 한 사실은 없다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

이 사건 해커는 외부 인터넷망에서 바로 피심인의 관리자페이지에 접속하여 개인정보 파일을 다운로드하여 유출한 사실이 있다. 만약 피심인이 개인정보처리시스템에서 개인정보를 다운로드 할 수 있는 개인정보취급자의 컴퓨터를 망분리 하였다면, 다운로드가 가능한 개인정보취급자의 컴퓨터는 외부 인터넷망이 차단되므로, 이 사건 해커는 외부 인터넷망에서 개인정보처리시스템에 접속할 수 없었거나 접속하더라도 개인정보 파일을 다운로드 받는 기능이 비활성화 되는 등 외부에서 개인정보처리시스템에 접속하여 개인정보 파일을 다운로드 할 수 있는 구조가 유지될 수 없었을 것이다. 이러한 점은 피심인도 확인서를 통해 인정하고 있다.

따라서 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 하나, 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제6항을 위반하였다.

6) ' ' 서비스의 마케팅센터 웹페이지의 취약점을 점검하지 않는 등 개인정보가 인터넷 홈페이지를 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 조치하지 않은 행위

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.

고시 해설서는 ▲"인터넷 홈페이지 취약점으로 인한 노출 방지 즉, 인터넷 홈페이지 개발 시 보안기준을 따르지 않아서 발생하는 취약점으로 인해 개인정보 DB가

노출되는 사례가 발생하지 않도록 수시로 인터넷 홈페이지 취약점을 점검하여 조치하도록 한다."라고 설명하고 있다.

이에 따라 '모든' 웹 취약점이 발생하지 않도록 조치를 하는 것은 현실적으로 불가능하나, 적어도 '잘 알려진' 웹 취약점에 대한 점검 및 조치를 하여야 한다. '잘 알려진' 웹 취약점은 이 사건 해킹사고에 사용된 SQL 인젝션 취약점 및 Cross Site Script 취약점, File Upload 취약점 등을 비롯하여 행정안전부, OWSAP(The Open Web Application Security Project, 국제웹보안표준기구), 국가사이버안전센터(NCSC) 등에서 발표하는 항목이 있다.

피심인은 웹페이지 개발 시 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 외부에 유출되지 않도록 SQL-Injection 공격 등을 방지할 수 있는 시큐어 코딩을 수행하지 않았으며, 웹 방화벽 등의 전문보안장비를 설치·운영하지 않은 사실을 확인서를 통해 인정하고 있다.

또한 피심인은 말부터 초까지 부터 운영하고 있는 ' ' 웹페이지(https://)에 대해서는 ㈜ 과 한국인터넷진흥원에서 무료로 제공하는 취약점 점검을 받은 후, 발견된 취약점(SQL-Injection, XSS, 전송구간 미암호화 등)에 대하여 에 소스코드를 수정하는 등의 조치를 취하였으나, 부터 마케팅센터 웹페이지 운영을 시작하면서 취약점 점검을 받은 사실은 없다.

즉 피심인은 ' ' 마케팅센터 웹페이지에 대하여 SQL-Injection을 방지할 수 있는 제작·점검이 미흡하였으며, 해당 웹페이지에 대한 지속적인 공격이 있었으나 탐지 및 차단할 수 있는 체계가 부재하였다.

피심인은 SQL-Injection 공격 등을 방지할 수 있는 제작·점검이 필요한 "개인정보처리시스템"은 DB서버를 의미하며 DB서버에 연동되어 있는 시스템이나 웹서버는 포함되지 않는다고 주장하고 있으나, 피심인이 SQL-Injection 공격 등을

방지하기 위해 DB서버 등에 어떠한 조치를 하였는지에 대해서 조차 아무것도 소명하지 못하고 있으며, 앞서 살펴본 바와 같이 피심인이 운영하고 있는 '
' 서비스의 마케팅센터 웹페이지는 관리자페이지와 마찬가지로 '
' 서비스를 이용하고 있는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어 피심인의 제휴점이 해당 제휴점에 예약한 피심인의 이용자의 이름(또는 닉네임)과 연락처를 조회, 다운로드 할 수 있도록 체계적으로 구성한 데이터베이스시스템으로 개인정보처리시스템에 해당한다.

따라서 피심인은 취급중인 개인정보가 인터넷 홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 하나, 마케팅센터 웹페이지에 SQL-Injection 공격 등을 방지할 수 있는 시큐어 코딩을 수행하지 않았고, 마케팅센터 웹페이지에 대해서는 취약점 점검을 하지 않았으며, 웹 방화벽 등의 전문 보안장비를 설치·운영하지 않는 등 취급중인 개인정보가 인터넷홈페이지 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템에 어떠한 조치도 취하지 않음으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제9항을 위반하였다.

나. 개인정보처리시스템에 접속한 기록을 정기적으로 확인·감독하지 않고, 일부 접속기록을 6개월 이상 보존·관리하지 않은 행위(정보통신망법 제28조제1항)

고시 제5조제1항은 "정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다."라고 규정하고 있다.

피심인은 관리자페이지의 웹 로그 중 POST 로그에 대해서는 부터 개인정보취급자를 알 수 있도록 별도로 DB에 보관하고 있었으나, GET 로그는

부터 접속일시 및 수행업무만 보관하고 있어 개인정보취급자가 관리자페이지에서 개인정보를 조회, 다운로드 등 처리하는 경우 해당 개인정보취급자를 확인할 수 없었다.

특히 피심인은 개인정보취급자가 직접 ' ' 서비스 관련 데이터베이스(DB)에 접속하여 개인정보를 조회하는 등의 업무를 하는 경우에 대한 접속기록은 부터 보관하기 시작하였다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

따라서 피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 하나,

개인정보취급자가 관리자페이지에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 개인정보를 조회, 다운로드 등 처리하는 경우 해당 개인정보취급자가 누구인지 확인할 수 없었으며, 개인정보취급자가 직접 ' ' 서비스 관련 DB에 접속하여 개인정보를 조회하는 등의 업무를 하는 경우에 대해서는 접속기록을 보존·관리하지 않음으로써 정보통신망법 제28조제1항제3호(기술적·관리적 보호조치 중 접속기록의 위조·변조방지), 시행령 제15조제3항, 고시 제5조제1항을 위반하였다.

다. 개인정보취급자·이용자 비밀번호 및 개인정보 파일을 암호화 하지 않은 행위(정보통신망법 제28조제1항)

1) 비밀번호 암호화

정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 '개인정보를 안전하게 저장·전송할 수 있는

암호화기술 등을 이용한 보안조치(제4호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제4항은 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 '비밀번호의 일방향 암호화 저장(제1호)'을 하도록 규정하고 있다.

고시 제2조제6호는 "비밀번호라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다."라고 규정하고 있다.

고시 해설서는 ▲"이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 사용하는 식별자는 소유자 식별을 위한 목적의 ID, 사용자이름, 사용자 계정명 등을 말한다."라고

▲"「타인에게 공개되지 않는 정보」의 의미는 개인정보취급자 중 계정관리자라 할지라도 이용자 및 개인정보취급자의 비밀번호를 알 수 있는 형태로 관리되어서는 안 된다는 것이다. 비밀번호가 알 수 있는 형태로 관리되는 경우 해당 정보에 접근할 수 있는 관리 담당자에 의한 도용이 가능하기 때문이다."라고 설명하고 있다.

앞서 살펴 본 바와 같이, 개인정보의 암호화 취지는 비밀번호 등과 같은 개인정보가 암호화되지 않고 저장 및 전송되는 경우, 노출 및 위·변조 등의 위험이 있으므로, 개인정보처리시스템에 저장하거나 네트워크를 통해 전송할 때에는 해당정보의 불법적인 노출 또는 위·변조 방지를 위한 암호화가 제공되어야 한다는 것이다.

이와 관련하여 고시 제6조제1항은 "정보통신서비스 제공자등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장한다."라고 규정하고 있다.

이 경우 정보통신서비스 제공자등은 개인정보취급자 및 이용자의 비밀번호 등이 노출 또는 위·변조되지 않도록 일방향 함수(해쉬함수)를 이용하여 저장하여야 한다. 즉 사용자가 입력한 인증과 관련된 정보는 평문 형태로 저장되지 않고, 일방향 함수를 통해 얻은 결과 값이 시스템에 저장되어야 한다.

그러나 피심인은 관리자페이지의 접근권한을 변경한 기록에 개인정보취급자의 비밀번호를 암호화하지 않고 평문으로 저장하고 있었으며, .php 파일 내에 DB 접속계정의 비밀번호를 암호화하지 않고 평문으로 저장하였다. 또한 피심인은 DB내에 저장관리되고 있는 회원의 비밀번호 및 관리자 계정의 비밀번호를 현재 권고하고 있지 않은 암호화 알고리즘인 PHP(ver 7.0)에서 기본으로 제공하는 SHA-1 함수를 사용하고 있어, 외부로 유출되는 경우 복호화 되어 이용자의 피해가 발생할 가능성이 크다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

따라서 피심인이 개인정보취급자 및 개인정보처리시스템의 비밀번호를 일방향 암호화하지 않고 평문으로 저장하고, 이용자의 비밀번호를 안전하지 않은 암호화 알고리즘으로 암호화한 것은 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제3항, 고시 제6조제1항을 위반한 것이다.

2) 개인정보 파일 암호화

고시 제6조제4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다."라고 규정하고 있다.

이에 대해 고시 해설서는 ▲"고객의 개인정보를 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려 받아 저장할 때에는 파일암호화 제품 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다."라고 설명하고 있다.

피심인의 개인정보취급자의 업무용PC에 대하여 점검을 한 결과 최고관리자 권한이 있던 의 컴퓨터에 이용자의 개인정보(이름, 휴대전화 번호, 숙박 장소, 숙박 일시, 숙박 유형, 결제금액 등 숙박이용자 정보 건)가 담긴 암호화되지 않은 엑셀파일(( ) 당일예약(예약내역) .xlsx)이 저장되어 있었으며, 관리자페이지에서 CSV 파일을 다운로드 하였을 때에도 해당 파일은 암호화가 되어 있지 않았다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

개인정보처리시스템에서 CSV, EXCEL 등 파일을 생성하는 시점에 비밀번호를 설정하여 개인정보취급자의 PC에 내려 받도록 하는 것은 어려운 기술, 비용을 요하지는 않는다. 만약 해당 기능이 적용되었다면 이 사건 해커는 지금과 같은 방식으로 개인정보 파일을 유출하였더라도 해당 파일을 쉽게 열어보지 못하였을 것이다.

따라서 피심인이 이용자의 개인정보를 개인정보취급자의 업무용PC에 저장할 때 암호화되지 않은 행위는 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제3항, 고시 제6조제4항을 위반한 것이다.

라. 정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위(정보통신망법 제29조제2항)

피심인은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 그 개인정보를 파기하거나 또는 별도로 저장·관리하여야 하나, ' ' 서비스를 1년 이상 이용하지 않은 이용자의 개인정보 건을 파기하지도 않고 서비스를 이용하고 있는 이용자의 개인정보와 분리하여 별도로 저장·관리하지도 않음으로써 정보통신망법 제29조제2항(개인정보의 파기 중 개인정보 유효기간제), 시행령 제16조제2항을 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 장치의 설치·운영을 하여야 하고, ②접속기록의 위조·변조 방지를 위한 조치를 하여야 하며, ③개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 등 기술적·관리적 보호조치를 하여야 하고, ④정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 위 1년이 경과한 후 위 이용자의 개인정보를 즉시 파기하거나 정보통신서비스를 이용하고 있는 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하는 등 필요한 조치를 하여야 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 15> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①개인정보처리시스템에 대한 접근권한을 과도하게 부여한 행위, ②개인정보처리시스템에 대한 접근권한을 변경·말소하지 않은 행위, ③외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위, ④침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ⑤개인정보취급자의 컴퓨터 등을 망분리를 하지 않은 행위, ⑥인터넷 홈페이지 등을 통해 개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 행위, ⑦개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 최소 6개월 이상 접속기록을 보존·관리하지 않은 행위, ⑧개인정보취급자·이용자의 비밀번호를

암호화 하지 않은 행위, ⑨이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 행위, ⑩정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 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 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, 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 의할 때, 피심인은 영리를 목적으로 숙박O2O 어플리케이션인 ' ' 등을 운영하는 정보통신망법 제2조제1항제3호에 따른 정보통신서비스 제공자로서 ▲피심인이 기준 보관·관리하고 있던 개인정보량이 건(중복제거 시 명)으로 매우 방대하고, ▲숙박O2O 서비스의 특성상 이용자의 개인정보가 민감할 수 있는 정보이기 때문에 이에 걸맞은 엄격하고 세밀한 개인

정보 관리가 요구됨에도 ▲정보통신망법 제28조제1항제2호에 따른 접근통제의 기술적·관리적 보호조치 중 개인정보처리시스템에 대한 접근권한을 과도하게 부여한 행위, 개인정보처리시스템에 대한 접근권한을 변경·말소하지 않은 행위, 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, 개인정보 취급자의 컴퓨터 등을 망분리를 하지 않은 행위, 인터넷 홈페이지 등을 통해 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 의할 때, 피심인의 위반행위의 결과가 ▲개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영을 소홀히 하는 등 안전하고 체계적인 개인정보 관리를 위한 정보보호에 대한 투자를 게을리 하여 이용자의 개인정보가 유출된 점, ▲위반행위로 인한 개인정보의 피해규모가 피심인이 보유하고 있는 개인정보*의 100분의 5 이상{ 기준, 피심인의 서비스인 ' '를 이용하여 숙박을 예약한 '전체' 이용자의 개인정보 건(중복제거 시 명) 및 회원정보 건(특정 개인을 식별할 수 있는 정보 명)건, 총 건(중복제거 시 명) 유출}인 점, ▲이용자의 개인

정보가 공중에 노출된 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 감경할 만한 사유가 없으므로 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하였다.

* 시 기준으로 피심인이 보유하고 있는 이용자의 개인정보는 숙박 예약정보 건, 회원정보 건임

3) 기준금액 산출

피심인의 위반행위와 관련된 ' ' 서비스의 사업개시( ) 이후 매출액을 연평균 매출액으로 환산한 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '매우 중대한 위반행위'의 부과기준율 1천분의 27을 적용하여 기준금액을 원으로 한다.

<참고 16> 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 초과 2년 이내인 (까지) '중기 위반행위'에 해당하므로 기준금액에 100분의 25에 해당하는 금액인 원을 가중한 원이나,

최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액에 100분의 50에 해당하는 금액인 원을 감경한 원으로 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 해커가 검거된 사실 등을 고려하여 '부과기준' 제8조 [별표] Ⅱ. 2.에 따라 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 상기와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 이상 10억원 미만에 해당하여 백만원 미만은 절사한 원을 최종 과징금으로 결정한다.

<참고 17> 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">원</td><td>기준금액의 25%
가중</td><td rowspan="2">원</td><td>가중 없음</td><td rowspan="2">원</td></tr>
<tr><td>기준금액의 50%
감경</td><td>필수적 가중·감경을 거친 금액의 10%
감경</td></tr>
</table>

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

Ⅵ. 징계 권고

피심인이 개인정보 보호와 관련하여 이 법을 위반한 행위가 ①개인정보처리시스템에 대한 접근권한을 과도하게 부여한 행위, ②개인정보처리시스템에 대한 접근권한을 변경·말소하지 않은 행위, ③외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위, ④침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ⑤개인정보취급자의 컴퓨터 등을 망분리를 하지 않은 행위, ⑥인터넷 홈페이지 등을 통해 개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 행위, ⑦개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 최소 6개월 이상 접속기록을 보존·관리하지 않은 행위, ⑧개인정보취급자·이용자의 비밀번호를 암호화 하지 않은 행위, ⑨이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 행위, ⑩정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위 등으로, 안전하고 체계적인 개인정보 관리를 위한 정보보호에 대한 투자를 게을리 하여 이용자의 개인정보를 유출한 책임은 피심인의 최고 경영자 등 임원에게 있다.

이에 피심인에 대하여 정보통신망법 제69조의2제2항에 따라 개인정보 유출 및 정보통신망법 위반과 관련하여 피심인의 대표자 및 책임 있는 임원을 포함한 책임자에 대해 징계할 것을 권고한다. 피심인은 이를 존중하여야 하며 그 결과를 방송통신위원회에 통보하여야 한다.

Ⅶ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 및 제29조(개인정보의 파기)제2항 위반에 대한 과태료는 같은 법 제76조제1항제3호·제4호, 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 각 위반행위는 첫 번째에 해당하여 1회 위반 과태료를 각 적용한다.

<참고 18> 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
더. 법 제29조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조제1항 제4호	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 의할 때, 피심인의 ▲기술적·관리적 보호조치 위반행위는 ①개인정보처리시스템에 대한 접근권한을 과도하게 부여한 점, ②개인정보처리시스템에 대한 접근권한을 변경·말소하지 않은 점, ③외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 점, ④침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 점, ⑤개인정보취급자의 컴퓨터 등을 망분리를 하지 않은 점, ⑥인터넷 홈페이지 등을 통해 개인정보가 유출되지 않도록 개인정보처리시스템에 조치를 취하지 않은 점, ⑦개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 최소 6개월 이상 접속기록을 보존·관리하지 않은 점, ⑧개인정보취급자·이용자의 비밀번호를 암호화 하지 않은 점, ⑨이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 점 등 2개 이상(제28조제1항 제2호와 제4호)에 해당하므로 기준금액의 50%를 가중하고,

▲정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위는 가중할 만한 사유가 없으므로 기준금액을 유지한다.

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 의할 때, 피심인의 위반행위의 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 피해규모가 경미하지 않다는 점, ▲사업규모도 처리지침 제10조제1항제2호에 따른 운영중인 웹사이트(모바일 어플리케이션 포함)에 대한 일일 평균 이용자 수가 5만명 미만인 정보통신서비스 제공자등(기간·별정통신사업자 제외)에 해당하지 않는 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 1,500만원) 및 정보통신서비스를 1년 동안 이용하지 아니하는 이용자의 개인정보를 즉시 파기 또는 별도로 저장·관리하지 아니한 행위(과태료 1,000만원)에 대하여 총 2,500만원의 과태료를 최종적으로 부과한다.

<참고 19> 과태료 산출내역

위반 유형	기준금액	가중금액	감경금액	최종 과태료
기술적·관리적 보호조치 §28①2·3·4호	1,000만원	500만원	-	1,500만원
개인정보 유효기간제 §29②	1,000만원	-	-	1,000만원
계	2,000만원	500만원	-	2,500만원

<참고 20> 위반행위별 과징금·과태료와 시정명령

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2·3·4호	원	15백만원	O	원
개인정보 유효기간제 §29②	-	10백만원	O	

Ⅷ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금), 제69조의2(고발)제2항 및 제76조제1항 제3호와 제4호(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

부위원장　　허　　욱

위　　원　　김 석 진

위 원 표 철 수

위 원 고 삼 석