방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 47 - 444호

안 건 명 의 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 9. 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. 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것

나. 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리할 것

다. 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

2. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날로부터 1개월이내에 4단×10㎝ 또는 5단×9㎝의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 앱에 1주일 이상 게시하여야 한다. 이때, 공표 내용 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 과징금과 과태료를 각 부과한다.

가. 과 징 금 : 283,000,000원

나. 과 태 료 : 15,000,000원

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 생활용품 등을 판매하는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자로서 일반현황 및 최근 3년간 매출액은 다음과 같다.

<참고 1> 피심인의 일반 현황

('17.12. 기준)

대표이사	설립일자	매출액	종업원 수	
			전체	정보보호
			명	

<참고 2> 피심인의 최근 3년간 매출액 현황

(단위 : 천원)

구 분	2015년	2016년	2017년	3년 평균
전체 매출				
관련 매출*				
관련없는 매출				

* 위반행위와 관련된 피심인 쇼핑몰 매출을 관련 있는 매출로 분류

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 피심인이 보관, 관리하는 이용자의 개인정보가 미상의 해커(이하 '이 사건 해커'라 한다)에게 개인정보가 유출되었다는 피심인의 신고('18. 4. 11.)를 접수하였다.

※ 유출 인지 : 피심인은 '18. 4. 9. 의 상품 페이지의 디자인 이상으로 원인을 파악하던 중 '18. 4. 10. 개인정보 유출 가능성을 확인함

2. 행위 사실

가. 유출 규모

피심인이 온라인 생활용품 쇼핑몰 홈페이지(' ',)를 운영하면서 수집한 2018. 4. 17. 기준의 회원정보(아이디, 이름, 연락처, 이메일 등) 총 2,407,895명(휴면회원 포함) 중 2.18Mb('18.5.21.기준 최소 1,952명)의 개인정보(이름, 아이디, 포인트)가 유출된 것으로 확인되었다.

<참고 3> 의 유출된 개인정보 현황

구 분		유 출 항 목	데이터량(건수)	중복제거*
이용자정보	관리자 페이지	아이디, 이름, 권한, 이메일, 휴대전화번호, 적립금, 등록일 등	31Mb(확인불가)	확인불가**
		이름, 아이디, 포인트	2.18Mb(최소 7,707건)***	최소 1,952명
	DB	아이디, 이름, 생년월일, 이메일, 주소, 전화, 휴대전화번호, 성별 등	498Mb(확인불가)	확인불가**

소 계	-	최소 7,707건	**최소 1,952명**

* 유출된 개인정보 중 아이디 기준으로 중복제거

** 개인정보유출 시점('18. 4. 7.~4. 9.) 방화벽 로그 기록이 없어 실제 유출여부는 판단 불가

*** 유출 당시 회원포인정보(pointList.xls)의 데이터량은 2.18Mb 였으나, 조사 시('18. 5. 21. 기준) 회원 포인트 정보를 다운로드한 데이터량은 1.2Mb로 7,707건의 유출 건수가 확인됨

나. 유출 경로

1) 해커의 관리자 계정 탈취

이 사건 해커는 협력업체에게 포장재 제공을 목적으로 피심인이 운영하고 있는 관리자페이지( )의 관리자 계정( ) 및 웹을 통해 ' ' 회원 DB를 관리할 수 있는 DB 관리자페이지( )의 관리자 계정( )을 2018. 4. 7. 23:17경 이전에 알 수 없는 방법으로 탈취하였다.

2) 탈취한 관리자 계정을 이용하여 개인정보처리시스템(관리자페이지, DB관리자페이지) 접속

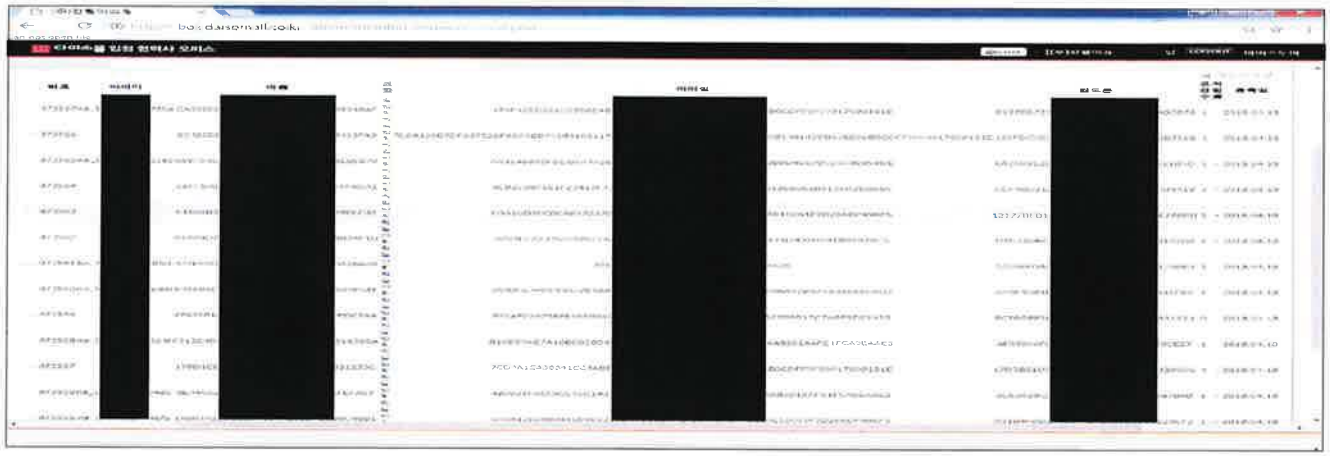
(관리자페이지 접속) 이 사건 해커는 2018. 4. 7. 23:17부터 2018. 4. 9.까지 해외 IP( )에서 탈취한 관리자 계정( )을 이용하여 관리자페이지( )에 지속적으로 접속하였고, 2018. 4. 9. 00:44경 ' '의 유효한 회원정보를 조회할 수 있는 웹페이지( )에서 개인정보 유출(약 30MB)을 시도*한 것으로 확인되었다.

* 웹 로그 외 추가적인 정보(방화벽 로그 기록, 개인정보취급자 접속기록 등)가 없어 외부 유출 여부는 확인 불가

<참고 4> '피심인'의 관리자페이지에 해커가 접속한 이력

```
- - 0 [07/Apr/2018:23:17:49 +0900] "POST HTTP/1.0" 302
20 " " "Mozilla/5.0 (Windows NT 6.1; Win64; x64) Appl
eWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36" 0 13329
- - 6 [07/Apr/2018:23:17:50 +0900] "GET HTTP/1.0" 2
00 14970 " " "Mozilla/5.0 (Windows NT 6.1; Win64; x6
4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36" 6 13337
```

<참고 5> '피심인' 관리자페이지에 접속 시 회원정보에 대한 열람·다운로드 가능



(DB 관리자페이지 접속) 이 사건 해커는 2018. 4. 9. 00:18경 탈취한 관리자 계정( )으로 DB 관리자페이지( )에 접속하였고, 2018. 4. 9. 00:29경 ' ' 회원정보 DB 테이블( )내 암호화된 개인정보(이름, 이메일, 휴대폰번호, 주소 등)를 복호화할 수 있는 key 파일( )을 탈취한 후, 2018. 4. 9. 02:47경 유효 회원정보 DB 테이블( )에 저장되어 있는 개인정보에 대한 유출(약 500Mb)을 시도*한 것이 확인되었다.

* 웹로그 분석결과, 유출 실패로 확인되나 유출 시점과 동일한 환경의 시연이 불가능하고 웹로그 외 추가적인 정보(방화벽 로그 기록 등)도 없어 외부 유출 여부는 확인이 불가

<참고 6> '피심인' DB 관리자페이지에 해커가 접속한 이력

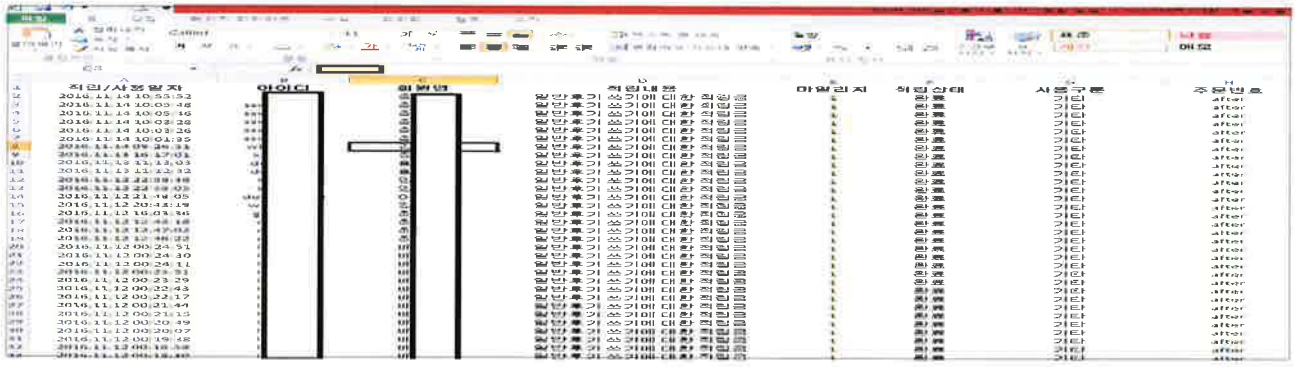
```
-          [09/Apr/2018:00:18:41 +0900] "GET /          / HTTP/1.0" 200 1
060 "-" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/65.0.3325.181 Safari/537.36" 0 9911
-          [09/Apr/2018:00:18:42 +0900] "GET
token=0b9848ad129c03691c0ae98657607289 HTTP/1.0" 200 1363 "
" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/65.0.3325.181 Safari/537.36" 0 16176
```

3) 개인정보 유출

(관리자페이지) 이 사건 해커는 2018. 4. 9. 00:51경 탈취한 관리자 계정( )으로 피심인 관리자페이지에 접속하여, ' '의 유효한 회원정보를 조회할

수 있는 웹페이지에서 아이디, 이름, 포인트 내용 등 개인정보를 다운로드 (, 2.18Mb)하여 유출한 것으로 확인되었다.

<참고 7> 해커의 개인정보 유출 파일



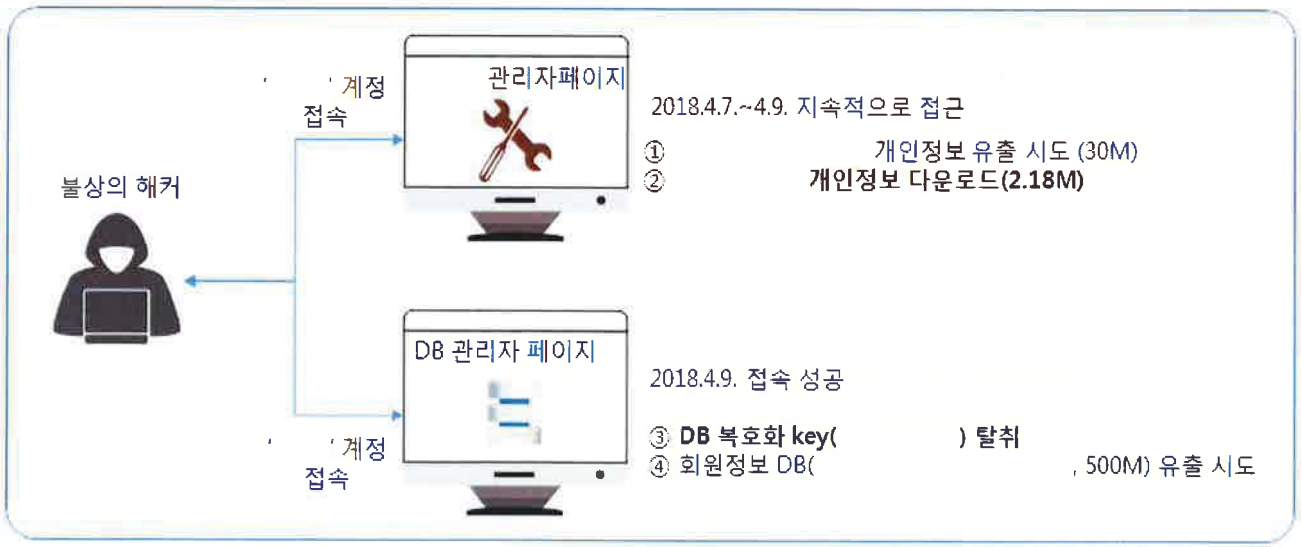
라. 개인정보 유출경로 요약

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

1 이 사건 해커는 알 수 없는 방법으로 관리자페이지 및 DB 관리자페이지의 관리자 계정을 탈취하여

2 관리자페이지에 접속한 후 ' ' 서비스의 유효한 회원정보를 조회하고 다운로드할 수 있는 페이지에서 이용자의 개인정보를 엑셀파일로 다운로드 하여 유출한 것으로 확인되었다.

<참고 8> 개인정보 유출 경로도



3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

가. 개인정보처리시스템에 대한 안전한 인증수단 적용 등 접근통제{「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제28조(개인정보의 보호조치) 중 접근통제}

1) 안전한 인증수단 관련

피심인의 개인정보취급자는 외부에서 협력업체에게 포장재 제공을 목적으로 운영하고 있는 관리자페이지( )와 웹을 통해 ' ' 회원 DB를 관리할 수 있는 DB 관리자페이지( )에 접속하여 회원정보(아이디, 이름, 휴대전화번호 등)를 조회하고 다운로드할 수 있다.

2018. 4. 17. 기준으로 관리자페이지와 DB 관리자페이지에는 별도의 추가적인 인증수단 없이 아이디, 비밀번호만으로 접속이 가능한 사실이 있다.

<참고 9> 안전한 인증수단 미적용 화면

2) 망분리 관련

피심인은 2018. 4. 17. 기준 개인정보가 저장·관리되고 있는 이용자 수가 약 2,407,895명이며, 정보통신서비스 부문 2017년 매출액이 약 222억원인 정보통신서비스 제공자임에도 불구하고, 관리자페이지 등 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리를 한 사실이 없다.

* 2018. 4. 16. 기준 1년 동안 이용내역이 없어 별도로 분리하여 저장·관리하고 있는 휴면 회원 1,433,657명의 개인정보 포함

따라서 이 사건 해커가 외부에서 개인정보처리시스템인 관리자페이지에 접속하여, 개인정보 파일을 다운로드할 수 있는 구조가 유지될 수 있었다.

<참고 10> 망분리 미조치 화면

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

피심인은 개인정보취급자 등이 관리자페이지( )에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 접속기록을 보존·관리하지 않았으며, 따라서 이를 월 1회 이상 정기적으로 확인·감독한 사실도 없다.

※ 피심인이 별도로 운영하고 있는 또 다른 관리자페이지( )의 경우에는 접속기록을 보존·관리하고 있음

다. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 5. 31. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 6. 15. 의견을 제출하였다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)', '접속기록의 위조·변조 방지를 위한 조치(제3호)' 등의 기술적·관리적 조치를 하여야 한다."라고 규정하고 있다.

나. 정보통신망법 시행령 제15조제2항은 "법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단(제3호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)' 등의 조치를 하여야 한다. 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.

정보통신망법 시행령 제15조제3항은 "법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 '개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독(제1호)' 등의 조치를 하여야 한다."라고 규정하고 있다.

다. 「개인정보의 기술적·관리적 보호조치 기준(이하 '고시'라 한다)」 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)', '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 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다."라고 규정하고 있다.

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 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.

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. 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 시 안전한 인증수단을 적용하지 않은 행위

피심인이 협력업체에게 포장재 제공을 목적으로 운영하고 있는 관리자페이지( )와 웹을 통해 ' ' 회원 DB를 관리할 수 있는 DB 관리자페이지( )는 ' ' 서비스를 이용하고 있는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어 이용자의 이름, 이메일, 휴대전화번호 등 개인정보를 조회, 다운로드할 수 있도록 체계적으로 구성한 데이터베이스시스템으로 개인정보처리시스템이다.

따라서 피심인은 고시 제4조제4항에 따라 개인정보취급자가 정보통신망을 통해 외부에서 관리자페이지와 DB 관리자페이지에 접속하는 경우 안전한 인증수단을 적용하여야 한다.

이에 대하여 고시 해설서는 ▲"인터넷 구간 등 외부로부터 개인정보처리시스템에 접속은 원칙적으로 차단하여야 하나, 정보통신서비스 제공자등의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요할 때에는 개인정보처리시스템에 사용자계정과 비밀번호를 입력하여 정당한 개인정보취급자 여부를 식별·인증하는 절차 이외에 추가적인 안전한 인증수단을 적용하고 안전한 인증 수단을 적용할 때에도 보안성 강화를 위하여 VPN, 전용선 등 안전한 접속수단의 적용을 권고한다."라고 설명하고 있다.

피심인은 2018. 4. 17. 기준으로 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템인 관리자페이지와 DB 관리자페이지에 접속하는 경우 별도의 추가적인 인증수단 없이 아이디, 비밀번호만으로 접속이 가능하도록 한 사실이 있다.

또한 이 사건 해커는 외부 인터넷망에서 바로 피심인의 관리자페이지에 접속하여 개인정보 파일을 다운로드하여 유출한 사실이 확인된다.

피심인이 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속할 경우 안전한 인증을 거치도록 적용하였다면, 이 사건 해커는 외부 인터넷망에서 개인정보처리시스템에 쉽게 접속할 수 없었을 것이다.

그러나 피심인은 해당 관리자페이지 및 DB 관리자페이지가 사용되지 않았다고 소명할 뿐 이러한 위반사실에 대하여는 별다른 소명이 없다.

따라서 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속할 경우 필요한 안전한 인증수단 없이 아이디, 비밀번호만으로 접속이 가능하도록 함으로서 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제1호, 고시 제4조제4항을 위반하였다.

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

피심인은 2018. 4. 17. 기준 개인정보가 저장·관리되고 있는 이용자 수가 약 2,407,895명이고, 정보통신서비스 부문 2017년 매출액이 약 222억원인 정보통신서비스 제공자이다.

따라서 피심인은 고시 제4조제6항에 따라 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하여야 한다.

그러나 피심인은 관리자페이지 등 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터를 물리적 또는 논리적으로 망분리한 사실이 없다.

이 사건 해커는 외부 인터넷망에서 바로 피심인의 관리자페이지에 접속하여 개인정보 파일을 다운로드하여 유출한 사실이 확인되었다.

피심인이 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터를 망분리하였다면, 다운로드가 가능한 개인정보취급자의 컴퓨터는 외부 인터넷망이 차단되므로, 이 사건 해커는 외부 인터넷망에서 개인정보처리시스템에 접속할 수 없었거나 접속하더라도 개인정보 파일을 다운로드하는 기능이 비활성화 되는 등 외부에서 개인정보처리시스템에 접속하여 개인정보 파일을 다운로드할 수 있는 구조가 유지될 수 없었을 것이다.

피심인은 이러한 위반사실에 대하여 개인정보취급자의 컴퓨터에서 웹사이트 접속에 필요한 최소한의 포트만을 허용하였다고 주장하나 인터넷 접속이 완전히 차단되지 않은 사실에 대해서는 인정하고 있다.

따라서 피심인이 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 변경할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하지 아니하여 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제3호, 고시 제4조제6항을 위반하였다.

다. 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 시스템 이상 유무의 확인을 위해 6개월 이상 접속기록을 보존·관리하지 않은 행위

피심인은 고시 제5조제1항에 따라 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.

이에 대하여 고시 해설서는 ▲"정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다." 라고 설명하고 있다.

그러나 피심인은 개인정보취급자 등이 관리자페이지에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 접속기록을 보존·관리하지 않았으며, 따라서 이를 월 1회 이상 정기적으로 확인·감독한 사실도 없다.

이에 대해 피심인은 ' ' 서비스를 이용하고 있는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어 있는 또 다른 관리자페이지( )에 대해서는 개인정보취급자가 개인정보처리시스템에 접속한 접속일시 및 처리내역 등 접속기록을 보존·관리하여 관련 고시에서 요구하는 접속기록 관련 의무를 이행하고 있었으나, 협력업체에게 포장재 제공을 목적으로 운영하고 있는 관리자페이지( )에 대해서는 피심인이 실제로 사용하지 않아 그 동안 접속이 이루어지지 않았기 때문에 접속기록 자체가 존재하지 않았다고 주장한다. 그러나 해당 관리자페이지가 실사용 여부와 관계없이 피심인의 관리하에 있다는 것은 명백하고 애초부터 접속기록은 넘길 수 있도록 설계디지 아니한 사실도 인정된다.

결국 피심인은 개인정보취급자가 관리자페이지에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않고, 시스템 이상 유무의 확인 등을 위해 최소 6개월

이상 접속기록을 보존·관리하지 아니하여 정보통신망법 제28조제1항제3호(기술적·관리적 보호조치 중 접속기록의 위조·변조방지), 같은 법 시행령 제15조제3항, 고시 제5조제1항을 위반하였다.

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) 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용할 것

2) 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리할 것

3) 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리할 것

나. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날로부터 1개월이내에 4단×10㎝ 또는 5단×9㎝의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지 및 모바일 어플리케이션에 1주일 이상 게시하여야 한다. 이때, 공표 내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

<참고 11> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①개인정보처리시스템 접속시 안전한 인증수단을 적용하지 않은 행위, ②개인정보취급자의 컴퓨터를 망분리 하지 않은 행위, ③개인정보처리시스템 접속기록을 보존·관리하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

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 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조3의 제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정기준과 산정절차) 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(이하 '과징금 부과기준'이라 한다)' 따라 다음과 같이 부과한다.

1. 과징금 상한액과 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금 상한액은 같은 법 제64조3의제1항, 같은 법 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

과징금 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 생활용품 등을 판매하는 정보통신서비스 제공자로서 ▲피심인이 '18.4.17. 기준 보관·관리하고 있던 개인정보량이 2,407895명으로 매우 방대하고, ▲정보통신망법 제28조제1항제2호에 따른 접근통제 중 기술적·관리적 보호조치 중 안전한 인증수단을 소홀히 한 행위, ▲개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하지 아니한 행위, ▲정보통신망법 제28조제1항제3호에 따른 개인정보취급자의 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 아니하고, 시스템 이상 유무의 확인을 위해 최소 6개월 이상 접속기록을 보존·관리하지 않은 행위 등으로 이 사건 해커에 의해 이용자의 개인정보가 유출되는 빌미를 제공하였으므로, 피심인에게 중과실이 있다고 판단한다.

2) 중대성의 판단

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

과징금 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 규정하고 있다.

이에 따를 때, 피심인의 위반행위의 결과가 ▲개인정보 유출로 피심인이 직접적인 이득을 취하지 않은 점, ▲유출된 개인정보가 피심인이 보유하고 있는 개인정보의 100분의 5 이내(2018. 4. 17. 기준, 피심인의 서비스인 '다이소몰' 이용자의 개인정보 2,407,895명으로 1,952명 유출)인 점, ▲공중에 노출되지 않은 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 '보통 위반행위'로 판단하였다.

3) 기준금액 산출

피심인의 '다이소몰' 서비스 관련 매출을 위반행위 관련 매출로 하고, 직전 3개 사업년도의 연평균 매출액을 환산하여 위반행위와 관련된 매출액을 원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '보통 위반행위'의 부과기준율 1천분의 15를 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

과징금 부과기준 제6조와 제7조에 따라 위반행위의 기간이 2년 초과( )이므로 기준금액의 100분의 50에 해당하는 금액인 원을 가중한 원이나,

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

특별히 가중·감경할 사유가 없어 기준금액을 유지한다.

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 과징금부 과기준에 따라 상기와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 이상 10억원 미만에 해당하여 백만원 미만을 절사한 원을 최종 과징금으로 결정한다.

〈참고 13〉 과징금 산출내역

기준금액	필수적 가중·감경	추가적 가중·감경	**최종 과징금***
원	필수적 가중 (50%, 원) 필수적 감경 (50%, 원)	추가적 가중 없음 추가적 감경 없음	**283백만원**
	→ 283백만원	→ 283백만원	

* '전기통신사업법 금지행위 위반에 대한 과징금 산정 실무요령'에 따라 최종 과징금 산출액이 1억원 미만은 십만원 미만 절사, 1억원 이상은 백만원 미만 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(법 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

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.

이에 따라 피심인의 정보통신망법 제28조제1항 위반 행위가 2개 이상인 경우에 해당하므로 기준 금액의 50%를 가중한다.

〈참고 15〉 과태료 산출내역

위반조문	기준금액	가중	감경	최종 과태료
§28①2·3호	1,000만원	500만원	없음	**1,500만원**

3. 최종 과태료

이에 따라 피심인의 정보통신망법 제28조제1항 위반행위에 대해 1,500만원의 과태료를 부과한다.

<참고 16> 위반행위별 과징금·과태료와 시정명령

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2·3호	**283백만원**	**15백만원**	O	**298백만원**

Ⅶ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금) 및 제76조(과태료)제1항제3호에 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)

(국회 참석 관계로 회의 불참)

위　　원　　김 석 진 (인)

위　　원　　표 철 수 (인)

위　　원　　고 삼 석 (인)