방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 26 - 350호

안 건 명 개인정보 유출사업자 법규 위반사항 시정조치에 관한 건

피 심 인 **(사업자등록번호 :)**

대표이사

의 결 일 2018. 5. 30.

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

2. 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.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 금　　액 : 15,000,000원

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

피심인은 영리를 목적으로 온라인 게임서비스를 제공하는 홈페이지(　　)를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 최근 3년간 매출액은 다음과 같다.

〈　　의 매출액 현황 〉

구　분	2015년	2016년	2017년	평 균
매출액 (단위 : 백만원)				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사대상

방송통신위원회는 개인정보 유출 신고(2017. 12. 12.)한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 조사하였고, 피심인에 대한 현장조사(2018. 1. 25.~2018. 1. 26.) 결과 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 개인정보 수집현황

피심인은 게임서비스( )를 운영하면서 2018. 1. 25. 기준으로 799,679건의 회원정보를 수집·보유하고 있다.

< 의 개인정보 수집현황 >

구 분	항 목	수집일	건수
회원정보	아이디, 비밀번호, 닉네임, 이메일, 전화번호	'00. 1. 1. ~	799,679 (휴면회원 617,913건)

나. 개인정보 유출규모 및 경로

(1) 개인정보 유출규모

피심인이 게임서비스( )를 운영하면서 수집한 개인정보 약 6,000여 건이 미상의 해커에 의해 2017. 11. 2 ~ 12. 6. 기간 동안 유출되었다.

※ 정확한 피해규모는 파악하기 어려우며 미상의 해커에 의해 변조된 파일을 에서 삭제하기까지의 기간('17. 11. 2. ~ 12. 6.) 동안 로그인 한 이용자 전체 건수로 추산

< 의 유출정보 현황 >

구 분	유 출 항 목	건 수	중복제거
회원정보	아이디, 비밀번호	약 6,000여 건	약 6,000여 명

(2) 유출경로

미상의 해커가 피심인이 사용 중인 스마트에디터(2.0)의 파일업로드 취약점을 이용해 웹쉘파일을 홈페이지 게시판에 업로드(2016. 8. 28.)하고, 2017. 10. 29. 20:45~20:59 생성된 웹쉘에 접근을 시도하여 추가적인 웹쉘을 생성하였다.

미상의 해커는 업로드한 웹쉘을 통해 2017. 11. 2. 20:44 피심인이 운영하는 홈페이지 메인화면( )을 변조, 이용자가 해당 페이지에 아이디와 패스워드를 입력하면 해커의 중계서버( )로 2017. 11. 2. ~ 12. 6. 기간 동안 전송되게 함으로써 약 6,000여건의 이용자 계정(아이디, 비밀번호)을 탈취하였다.

* 스마트에디터 : 네이버에서 제공하는 홈페이지 게시판 편집기능 등이 있는 프로그램으로 파일업로드 취약점이 확인되어 '16. 7.19. 보안 업데이트를 공지하였음

(3) 유출신고

피심인은 운영 중인 홈페이지( )게시판에 해킹신고 및 문의 게시물이 증가함에 따라 자체 서버분석을 통해 개인정보 유출 가능성을 2017. 12. 11. 인지하고 2017. 12. 12. 개인정보보호 포털(i-privacy.kr, KISA)에 개인정보 유출신고를 한 후 홈페이지 공지를 통해 이용자에게 이를 알린 사실이 있다.

3. 개인정보의 기술적·관리적 보호조치 등 사실관계

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

피심인은 미상의 해커가 스마트에디터(2.0) 프로그램에 악성 프로그램인 웹쉘

파일을 서버에 2016. 8. 28. 업로드 할 시점에 불법적인 접근 및 침해사고를 방지할 수 있는 침입차단 및 탐지 기능이 포함된 시스템을 설치·운영하지 않은 사실이 있다.

또한, 피심인은 2017. 2. 서버를 이전(AWS, 아마존클라우드 웹서비스)하고, 2017. 5.부터 아마존에서 제공하는 방화벽, IPS 기능이 있는 보안 솔루션(Deep Security)를 적용하고 있으나 이 솔루션 또한 웹쉘 업로드 등을 탐지할 수 없는 것이므로 2017. 10. 29. 20:45~20:59 미상의 해커가 기존에 업로드 한 웹쉘을 통해 접근을 시도하고 추가적인 웹쉘을 생성한 것에 대해서도 탐지하지 못한 사실이 있다.

※ IPS 및 WAF(방화벽서비스) 등의 솔루션으로는 실제 서버 상 업로드 성공 여부 등을 확인할 수 없어 웹쉘 전용 솔루션 도입을 피심인에게 권고(안랩, 2017. 12. 11.)

나. 보안 프로그램 설치·운영 등 악성프로그램 방지{정보통신망법 제28조(개인정보의 보호조치) 중 악성프로그램 방지}를 소홀히 한 행위

피심인이 사용 중인 스마트에디터(2.0)가 파일 업로드 취약점으로 인한 웹쉘 공격과 홈페이지 변조 등 개인정보 유출이 발생될 우려가 있어 2016. 7. 19. 제조사(네이버)에서 보안 업데이트를 시행하고 공지하였으나 피심인은 이를 즉시 업데이트 하지 않음으로써 해커가 파일 업로드 취약점을 이용하여 악성 프로그램을 업로드(2016. 8. 28.) 하는 것을 방지하지 못한 사실이 있다.

※ 피심인은 2016. 11월 스마트에디터의 취약점에 대해 보안 업데이트를 하였음

나. 처분의 사전통지 및 의견수렴

방송통신위원회는 2018. 4. 4. '개인정보보호 법규 위반사업자 시정조치(안) 사전통지 및 의견수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2018. 4. 19. 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 침해 방지조치(제5호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 조치를 하여야 한다."라고 규정하고 있고, 제5항은 "개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다."라고 규정하고 있고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적 기준을 정하여 고시하여야 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'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)', '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)' 기능을 포함한 시스템을 설치·운영하여야 한다."라고 규정하고 있다.

제7조는 "악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안

프로그램을 설치·운영하여야 하며 '보안프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지(1호)'하고 '악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시(2호)'를 준수하여야 한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 정보통신서비스 제공자등은 불법적인 접근(인가되지 않은 자가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말함) 및 침해사고(해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태) 방지를 위해 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있으며, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 하며 신규 위협 대응 등을 위하여 지속적인 업데이트 적용 및 운영·관리하여야 한다고 해설하고 있다.

고시 제7조제2호에 대해 보안 업데이트 공지 여부를 지속적으로 확인하여 보안 업데이트 적용 시점 및 방법 등을 검토하고 적용하여야 한다고 해설하고 있다.

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

2. 위법성 판단

가. 개인정보처리시스템에 대한 접근권한 부여 등 접근통제{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**를 소홀히 한 행위**

피심인은 미상의 해커가 2016. 8. 28. 악성프로그램인 웹쉘 파일을 업로드 할 당시 시점에 불법적인 접근 및 침해사고를 방지할 수 있는 침입차단 및 탐지 기능이 포함된 시스템을 설치·운영하지 않았다.

2017. 5. 이후 미상의 해커가 기존(2016. 8. 28.)에 업로드 한 웹쉘을 통해 접근을 시도하였고 업로드 된 웹쉘이 추가적인 웹쉘을 생성하였지만 이를 탐지하지 못하는 등 피심인이 개인정보처리시스템에 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 및 접속한 IP 등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는 기능을 포함한 침입탐지시스템 설치·운영을 소홀히 한 행위는 정보통신망법 제28조제1항제2호, 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

나. 보안 프로그램 설치·운영 등 악성프로그램 방지{정보통신망법 제28조(개인정보의 보호조치) 중 악성프로그램 방지}**를 소홀히 한 행위**

피심인이 사용 중인 스마트에디터(2.0)의 제조사(네이버)가 자사의 스마트에디터 파일 업로드 부분이 웹쉘 공격이나 홈페이지 변조 등에 취약하여 개인정보가 유출될 우려가 있기 때문에 보안 업데이트를 시행할 것을 공지하였지만 피심인이 이를 즉시 업데이트하지 아니한 행위는 정보통신망법 제28조제1항제5호, 같은 법 시행령 제15조제5항, 고시 제7조제2호를 위반한 것이다.

〈참고〉 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)
	악성프로그램 방지	§28①5호	§15⑤	응용프로그램 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하지 아니한 행위(고시§7)

Ⅳ. 시정조치 명령

1. 시정명령

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

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.

3. 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.

가. 기준금액

정보통신망법 시행령 [별표 9]와 과태료 부과 등 처리지침 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피

심인의 위반행위가 첫 번째에 해당하므로 1회 위반 과태료인 1,000만원을 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

나. 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.

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

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

< 과태료 산출내역 >

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

다. 최종 과태료

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

Ⅴ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령) 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)