방 송 통 신 위 원 회
심의·의결

안건번호 제2019 - 57 - 298호

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. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

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 : 5,000,000원

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)은 영리를 목적으로 온라인 가상통화 거래 사이트　　를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황 및 3년간 매출액은 다음과 같다.

< 피심인 일반 현황 >

대표이사	설립일자	자본금	주요서비스	종업원 수('18.7.26. 기준)

< 피심인의 최근 3년간 매출액 현황 >

(단위 : 백만원)

구 분	2015년	2016년	2017년	평 균
매출액				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 피심인이 보관, 관리하는 이용자의 개인정보가 미상의 해커(이하 '이 사건 해커'라 한다)에게 65명의 회원정보가 유출되었다는 피심인의 신고(2018. 7. 25.)를 접수하였다.

※ 유출인지 : 피심인은 2018. 7. 24. 18시경 해커로부터 관리자 페이지 접속이 불가능할거라는 카카오톡 메시지를 받고 개인정보 유출 징후를 인지

이에, 방송통신위원회는 한국인터넷진흥원과 함께 피심인으로부터 넘겨받은 사고 관련 자료와 개인정보처리시스템 등에 남아있는 접속기록 등을 토대로 해킹 경로 파악과 정보통신망법 위반 여부 확인을 위한 개인정보 취급·운영 사실을 조사(2018. 7. 25. ~ 2018. 7. 26.)하였고 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 개인정보 수집현황

피심인은 가상통화 거래 사이트 를 운영하면서 2018. 7. 26. 현재 아래와 같이 이용자의 개인정보를 수집·보관하고 있다.

< 피심인의 개인정보 수집·보관 현황 >

구분	항목	수집일	건수
유효회원	이름, 아이디(이메일주소), 비밀번호, 휴대전화번호		13,429명

나. 개인정보 유출규모 및 경로

1) 개인정보 유출규모

피심인이 가상통화 거래 사이트 를 운영하면서 수집한 2018. 7. 26. 기준의 회원정보 총 13,429명 중 65명의 개인정보(아이디, 이름, 연락처, 이메일 등)가 외부에 유출된 것으로 확인되었다.

< 개인정보 유출현황 >

구 분	유 출 항 목	건 수
회원정보	이메일, 패스워드, 핸드폰번호, SMS인증값 등	65건

2) 유출 경로

이 사건 해커는 2018. 7. 16. 17:07:40 ~ 2018. 7. 22. 05:46:06 기간 동안 357차례에 걸쳐 SQL Injection[1] 공격을 시도하여 DB내 회원정보 테이블 의 회원고유번호 , 이메일 , SMS 인증값 , 암호화된 패스워드 , 핸드폰 번호 등 65명의 회원정보를 유출하였다.

1) SQL(Structured Query Language) Injection : 데이터베이스에 대한 질의값(SQL구문)을 조작하여 정상적인 자료 이외에 해커가 원하는 자료까지 데이터베이스로부터 유출 가능한 공격기법

< SQL-Injection 공격(접속 IP주소, 국가, 시간) >

IP	국가	공격 시각(비고)
118.219.54.	KR(SKB)	'18.7.21. 19:28:09 ~ 7.22. 05:46:06
113.124.34.	CN	'18.7.21. 05:27:18 ~ 05:53:36
144.0.57.	AU	'18.7.21. 06:13:59 ~ 07:50:50
203.229.230.	KR(KT)	'18.7.21. 13:30:04 ~ 19:01:35
39.89.243.	CN	'18.7.21. 18:33:28 ~ 18:44:58

3. 개인정보의 기술적 · 관리적 보호조치 등 사실 관계

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

피심인은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근 제한 기능 및 유출 탐지 기능이 포함된 시스템을 설치·운영하지 않았다.

나. 웹페이지 취약점 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**등 개인정보의 유 · 노출 방지에 필요한 조치를 하지 않은 행위**

피심인은 가상통화 거래사이트 에 대하여 SQL-Injection 등을 방지하기 위한 웹페이지 취약점 점검 등의 조치를 취하지 않았다.

다. 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. 2. 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)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)', '그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(제5호)'하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제6항에 따라 제2항 등의 구체적인 기준을 정한 고시인 「개인정보의 기술적·관리적 보호조치 기준」(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)'하는 기능, '개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)'하는 기능을 포함한 시스템을 설치·운영하여야 한다."라고, 제4조제9항은 "정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다."라고 규정하고 있다.

'고시 해설서'는 고시 제4조제5항에 대해 "정보통신서비스 제공자등은 불법적인 접근 및 침해사고 방지를 위해 다음과 같은 시스템 등을 스스로의 환경을 고

려하여 접근 제한 기능 및 유출 탐지 기능이 적합하게 수행되도록 설치·운영하여야 한다."라고

제4조제9항에 대해 "정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안 기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 한다."라고 해설하고 있다.

나. 정보통신망법 제64조제3항은 "과학기술정보통신부장관 또는 방송통신위원회는 정보통신서비스 제공자등이 이 법을 위반 한 사실이 있다고 인정되면 소속 공무원에게 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}**설치·운영을 소홀히 한 행위**

피심인이 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·운영하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제2호, 고시 제4조제5항을 위반한 것이다.

나. 웹페이지 취약점 점검{정보통신망법 제28조(개인정보의 보호조치) 중 접근통제}**등 개인정보의 유·노출 방지에 필요한 조치를 하지 않은 행위**

피심인이 가상통화 거래사이트 에 대하여 SQL-Injection 등을 방지하기 위한 웹페이지 취약점 점검 등의 조치를 취하지 않은 행위는 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 같은 법 시행령 제15조제2항제5호, 고시 제4조제9항을 위반한 것이다.

< 피심인의 위반사항 >

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②2호	개인정보처리시스템에 침입차단 및 침입탐지시스템을 설치하지 아니한 행위(고시§4⑤)
	접근 통제	§28①2호	§15②5호	웹페이지 취약점 점검 등의 조치를 취하지 않은 행위(고시§4⑨)

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. 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) 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 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

피심인은 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 유출규모(65건)가 적고, 위반행위 관련한 매출액( )이 많지 않아 과징금 부과의 실효성이 미미한 점을 고려하여 과징금 부과를 시정명령으로 갈음한다.

Ⅵ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항에 대한 과태료는 같은 법 제76조제1항제3호, 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 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 부과지침 제8조는 ▲증거인멸, 조작, 허위의 정보제공 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.

그러나 피심인의 정보통신망법 제28조제1항 위반 행위에 대해서 특별히 해당 사항이 없으므로 과태료를 가중하지 않는다.

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 위반행위에 대해 시정조치(안) 사전통지 및 의견제출 기간 내에 시정이 완료된 점을 고려하여 기준금액의 100분의 50인 500만원을 감경한다.

< 과태료 산출내역 >

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

다. 최종 과태료

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

Ⅶ. 고 발

피심인의 위반행위는 정보통신망법 제28조제1항제2호부터 제5호까지의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 유출한 경우이므로 같은 법 제64조의3제1항제6호에 해당하는 행위가 있다고 인정된다. 이에 피심인을 같은 법 제73조(벌칙) 및 제69조의2(고발) 규정에 따라 수사기관에 고발한다.

Ⅷ. 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.

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)