방 송 통 신 위 원 회
심의·의결

안건번호 제2018 - 05 - 018호

안 건 명 개인정보보호 법규 위반에 대한 시정조치에 관한 건

피 심 인 (사업자등록번호 :)

대표이사

의 결 일 2018. 1. 24.

주 문

1. 피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, ②개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하여야 하며, ③이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ④개인정보처리시스템에서 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

2. 피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 제출하여야 한다.

3. 피심인에 대하여 다음과 같이 과태료를 부과한다.

가. 과 태 료 : 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 전기통신사업자의 전기통신역무를 이용하여 가상통화 거래 사이트( )를 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자이다.

피심인은 가상통화 거래 사이트( )를 운영하면서 기간 동안 명의 회원 개인정보(이메일(ID), 비밀번호, 이름, 생년월일, 성별, 휴대폰번호, 계좌번호 등)를 수집하고 DB(Table명 :)에 저장·관리하고 있으며, 피심인의 최근 3년간 매출액은 다음과 같다.

〈 피심인 일반 현황 〉

구 분	2014년	2015년	2016년	평 균
매출액(단위 : 만원)				

※ 자료 출처 : 피심인이 제출한 자료

Ⅱ. 사실조사 결과

1. 조사 대상

방송통신위원회는 가상통화 탈취를 위한 악성코드 유포·표적 공격 등이 성행함에 온라인 가상통화 거래 사이트를 운영하는 주요한 사업자를 대상으로 정보통신망법 위반 여부에 대한 개인정보 취급·운영 실태를 기획조사 하였고, 피심인에 대한 현장조사(2017. 11. 28. ~ 2017. 12. 21.) 결과, 다음과 같은 사실을 확인하였다.

2. 행위 사실

가. 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 적용하지 않은 행위

피심인은 가상통화 이용자의 개인정보(이름, 휴대폰번호, 이메일, 계좌번호)를 조회 및 다운로드 가능한 관리자페이지( )에 외부에서 접속 시 별도의 안전한 인증수단 없이 아이디와 비밀번호만으로 접속이 가능하도록 하였다.

< 안전한 인증수단 미적용 화면 >

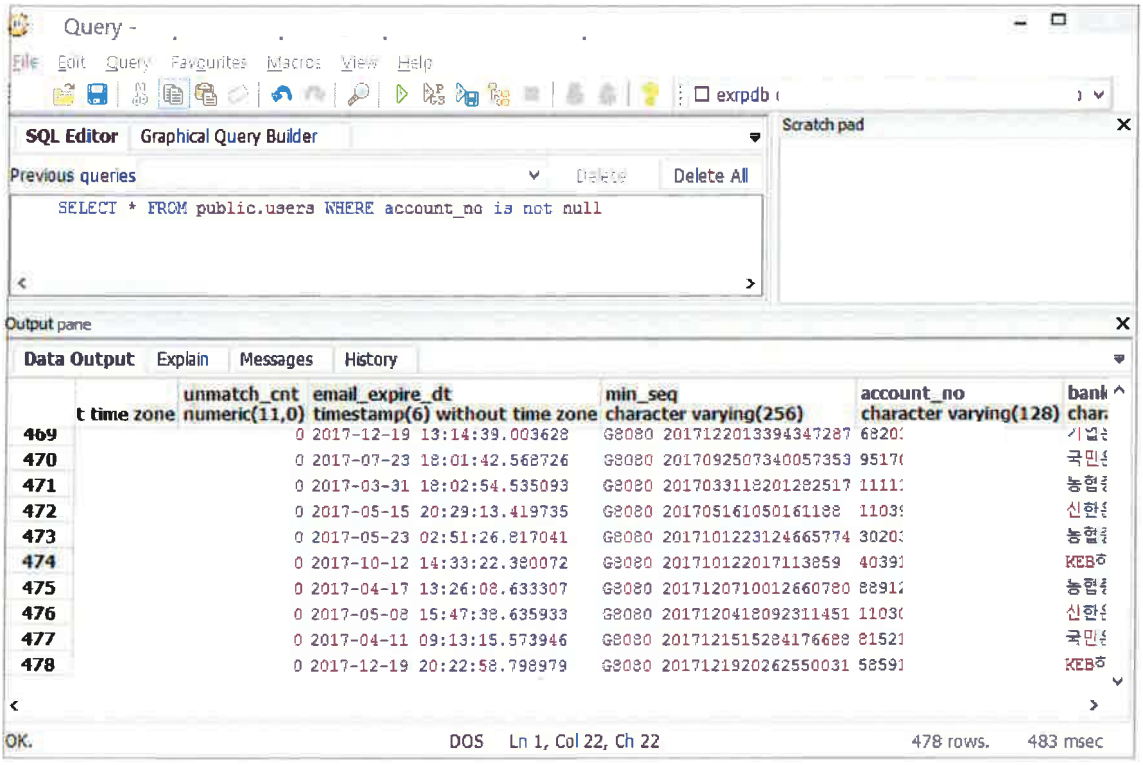
나. 개인정보처리시스템에 접속한 기록을 보관·점검하지 아니한 행위

피심인은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하지 않았으며 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하지 않았다.

다. 이용자의 계좌번호를 암호화하지 않은 행위

피심인은 2017. 12. 21. 이용자의 계좌번호를 암호화하는 등 개선조치 전까지, 이용자의 원화 환급 및 입금 등을 처리하기 위해 수집한 이용자의 계좌번호 건을 개인정보처리시스템(DB)에 안전한 암호알고리듬으로 암호화하여 저장하지 않고 평문으로 저장한 사실이 있다.

< 이용자 계좌번호 평문저장 화면 >

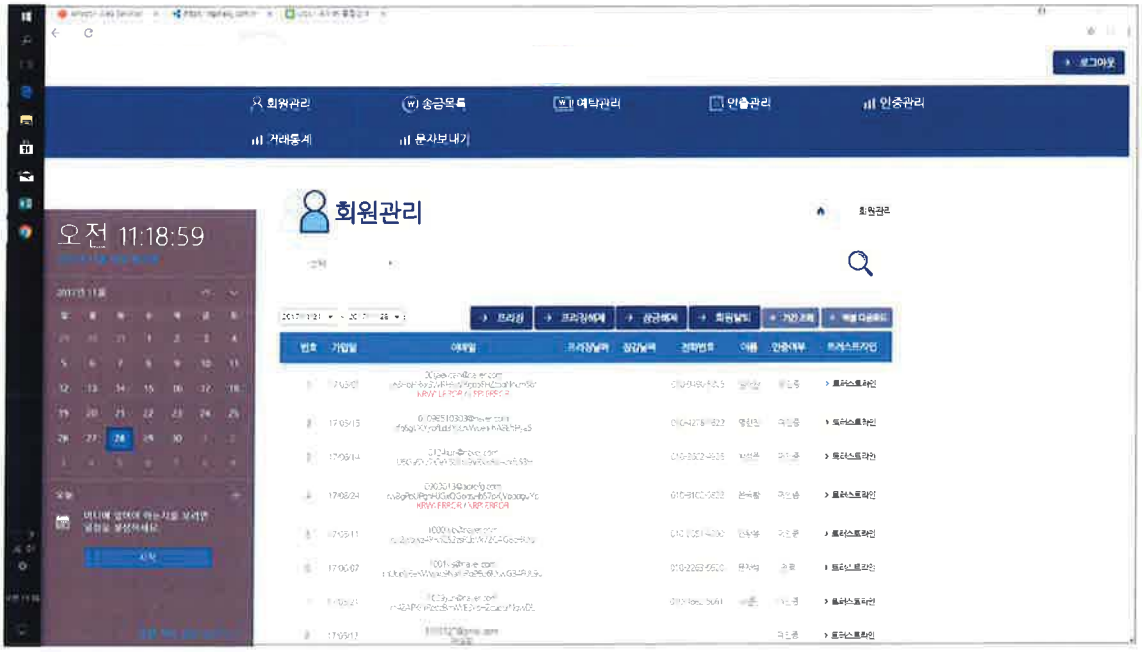


라. 개인정보의 출력·복사 시 보호조치를 하지 않은 행위

피심인은 2017. 12. 21. 이용자의 개인정보를 마스킹 처리하여 화면에 식별되지

않도록 개선조치하기 전까지, 개인정보처리시스템의 개인정보취급자 페이지 ( )에서 개인정보의 화면표시 용도를 특정하지 않고 이용자의 이름, 휴대폰번호, 계좌번호, 이메일 등 개인정보 항목을 용도에 따라 최소화하지 않고 화면에 출력한 사실이 있다.

< 이용자 개인정보 출력 화면 >



마. 처분의 사전통지 및 의견 수렴

방송통신위원회는 2018. 1. 4. '개인정보보호 법규 위반사업자 시정조치(안) 사전통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 의견을 제출하지 않았다.

Ⅲ. 위법성 판단

1. 관련법 규정

가. 정보통신망법 제28조제1항은 "정보통신서비스 제공자등이 개인정보를 처리

할 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)', '접속기록의 위조·변조 방지를 위한 조치(제3호)', '개인정보를 안전하게 저장·전송할 있는 암호화기술 등을 이용한 보안조치(제4호)', '그 밖에 개인정보의 안정성 확보를 위하여 필요한 보호조치(제6호)'를 하여야 한다."라고 규정하고 있다.

정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 등을 조치하여야 한다."고 규정하고 있고, 제3항은 "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)'을 하여야 한다."고 규정하고 있고, 제4항은 "개인정보를 안전하게 저장·전송될 수 있도록 보안조치를 하기 위하여 '그 밖에 암호화 기술을 이용한 보안조치(제4호)'를 하여야 한다."고 규정하고 있으며, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 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') 제4조제4항은 "정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통한 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증수단을 적용하여야 한다."라고 규정하고 있다.

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 안전한 인증수단을 적용하여야 한다."라고 설명하고 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

고시 제6조제2항은 "정보통신서비스 제공자등은 계좌번호에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다(제6호)."라고 규정하고 있으며,

고시 해설서는 ▲"주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리듬으로 암호화하여 저장하여야 한다."라고 설명하고 있다.

고시 제9조제1항은 "정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다."라고 규정하고 있으며,

고시 해설서는 "정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 출력(인쇄, 화면표시, 파일생성 등) 할 때에는 다음과 같은 사항 등을 고려하여 용도를 특정하고, 용도에 따라 출력 항목을 최소화 하여야 한다."라고 설명하고 있다.

나. 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. 외부에서 개인정보처리시스템에 접속 시 안전한 인증 수단을 적용하지 않은 행위

피심인이 운영하고 있는 '　　' 서비스의 관리자페이지는 이용자의 개인정보가 저장되어 있는 데이터베이스와 연결되어 가상통화 이용자의 개인정보를 조회, 다운로드 할 수 있도록 체계적으로 구성한 데이터베이스시스템으로 개인정보처리시스템이다.

개인정보처리스템인 관리자페이지에 개인정보취급자가 추가적인 인증수단 없이 아이디, 비밀번호만으로 접속이 가능하다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

따라서 피심인은 개인정보취급자가 외부에서 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.

나. 개인정보처리시스템에 접속한 기록을 보관·점검하지 아니한 행위

피심인은 관리자페이지의 웹 로그를 보관하고 있지 않아 개인정보취급자가 관리자페이지에서 개인정보를 조회, 다운로드 등 처리하는 경우 해당 개인정보취급자를 확인할 수 없었다.

특히 피심인은 개인정보취급자가 직접 '　　' 가상통화 거래 서비스 관련 데이터베이스(DB)에 접속하여 개인정보를 조회하는 등의 업무를 하는 경우에 대한 접속기록을 보관하지 않고 있었다. 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 ' ' 가상통화 거래 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. 이용자의 계좌번호를 암호화하지 않은 행위

피심인은 가상통화 거래 서비스 관련하여 이용자의 계좌번호를 개인정보처리시스템(DB)에 저장하면서 안전한 암호알고리즘으로 암호화하지 않고 있었다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

따라서 이용자의 계좌번호를 개인정보처리시스템(DB)에 저장하면서 안전한 암호알고리즘으로 암호화하지 않음으로써 정보통신망법 제28조제1항제4호(기술적·관리적 보호조치 중 암호화), 시행령 제15조제4항제2호, 고시 제6조제2항을 위반하였다.

라. 개인정보의 출력·복사 시 보호조치를 하지 않은 행위

피심인은 2017. 12. 21. 이용자의 개인정보를 마스킹 처리하여 화면에 식별되지 않도록 개선조치하기 전까지, 개인정보처리시스템의 개인정보취급자 페이지( )에서 개인정보의 화면표시 용도를 특정하지 않고 이용자의 이름, 휴대폰번호, 계좌번호, 이메일 등 개인정보 항목을 용도에 따라 최소화하지 않고 화면에 출력한 사실이 있다. 피심인은 이러한 위반사실에 대하여 별다른 소명은 없다.

피심인은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하고, 용도에 따라 출력항목을 최소화하지 않음으로써 정보통신망법 제28조제1항제6호, 시행령 제15조제6항, 고시 제9조제1항을 위반하였다.

〈참고〉 피심인의 위반사항

사업자 명	위반 내용	법령 근거		
		법률	시행령	세부내용(고시 등)
	접근 통제	§28①2호	§15②1호	외부에서 개인정보처리시스템에 접속시 단순히 아이디와 비밀번호이외 추가적으로 안전한 인증수단을 적용하지 않은 행위(고시 §4④)
	접속 기록	§28①3호	§15③1호	개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 확인·감독하지 않고 최소 6개월 이상 저장하지 않은 행위(고시 §5①)
	암호화	§28①4호	§15④2호	이용자의 계좌번호를 개인정보처리시스템에 저장하면서 안전한 암호알고리즘으로 암화화하지 않은 행위(고시 §6②)
	출력·복사물	§28①6호	§15⑥	개인정보처리시스템에서 개인정보의 출력시 용도를 특정하고, 용도에 따라 출력 항목을 최소화하지 않은 행위(고시 §9①)

Ⅳ. 시정조치 명령

1. 시정명령

피심인은 개인정보를 보관, 관리하는 자로서 개인정보를 처리할 때에는 개인정보의 분실·도난·유출을 방지하고 개인정보의 안전성을 확보하기 위하여 ①외부에서 개인정보처리시스템에 접속이 필요한 경우에는 아이디와 비밀번호를 통한 개인정보처리자 식별·인증과 별도로 공인인증서, 보안토큰, 휴대폰인증, 일회용 비밀번호(OTP : One Time Password), 바이오정보 등을 활용한 추가적인 인증수단을 적용하여야 하며, ②개인정보취급자의 개인정보처리시스템 접속일시·처리내역 등 접속기록을 작성하여 월1회 이상 이를 확인·감독하고 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 개인정보처리시스템의 접속기록(로그기록)을 보존·관리하여야 하며, ③이용자의 계좌번호에 대해 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, ④개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.

2. 시정명령 이행결과의 보고

피심인은 제1항의 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 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 [별표 9] 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '처리지침')에 따라 다음과 같이 부과한다.

가. 기준금액

정보통신망법 시행령 [별표 9]와 '처리지침' 제7조는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 이번 피심인의 위반행위가 첫 번째에 해당하여 1회 위반 과태료인 1,000만원을 적용한다.

〈 위반 횟수별 과태료 금액 〉

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 기술적·관리적 조치를 하지 아니한 자	법 제76조 제1항제3호	1,000	2,000	3,000

나. 과태료의 가중 및 감경

1) **(과태료의 가중)** '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, '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 정보통신망법 제28조제1항 위반행위가 2개 이상인 경우이므로 기준금액의 50%를 가중한다.

2) **(과태료의 감경)** '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 '처리지침' 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 특별히 감경할 사유가 없으므로 과태료를 감경하지 않는다.

< 과태료 산출내역 >

위반조문	기준금액	과태료 가중	과태료 감경	최종 과태료
§28①	1,000만원	500만원	없음	**1,500만원**
계				**1,500만원**

다. 최종 과태료

이에 따라, 피심인의 정보통신망법 제28조제1항제2·3·4·6호 위반에 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 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 과태료를 납부하여야 한다.

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)