개 인 정 보 보 호 위 원 회
심의·의결

안 건 번 호 제2024-009-183호
안 건 명 개인정보보호 법규 위반행위에 대한 시정조치에 관한 건
피 심 인 (사업자등록번호 :)

대표자
의결연월일 2024. 5. 22.

주 문

1. 피심인 에 대하여 다음과 같이 시정조치를 명한다.

가. 피심인은 이용자 대상 개인정보 유출 통지를 실시하여야 한다.

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분통지를 받은 날로부터 60일 이내에 이행 결과를 개인정보보호위원회에 제출하여야 한다.

2. 피심인 에 대하여 다음과 같이 과징금과 과태료를 부과한다.

가. 과 징 금 : 15,141,960,000원

나. 과 태 료 : 7,800,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

3. 피심인 에 대한 시정조치 명령과 과태료 부과의 내용 및 결과를 개인정보보호위원회 홈페이지에 1년간 공표한다.

이 유

Ⅰ. 기초 사실

1. 일반 현황

온라인 메신저 서비스(카카오톡) 등을 운영하는 피심인은 「舊 개인정보 보호법」[1](이하 '舊 보호법')에 따른 정보통신서비스 제공자이며 피심인의 일반현황은 다음과 같다.

< 피심인의 일반현황 >

피심인명	사업자등록번호 (법인등록번호)	대표자 성명	주소	종업원 수(명)

피심인은 온라인 메신저 서비스(카카오톡)를 운영하면서, 2023. 3. 15. 기준으로 이용자 명의 개인정보를 수집하여 보관하고 있다.

1) 법률 제16930호, 2020. 2. 4. 일부개정, 2020. 8. 5. 시행

< 개인정보 수집현황 >

구분	항목	수집일	건수
회 원			
합 계			

2. 조사 배경

개인정보보호위원회는 카카오톡 이용자의 개인정보가 유출되어 불법적으로 거래되고 있다는 언론보도에 따라 피심인의 개인정보 취급·운영 실태 및 舊 보호법 위반 여부를 조사(2023. 3. 14. ~ 2024. 2. 15.)하였으며, 다음과 같은 사실을 확인하였다.

Ⅱ. 사실조사 결과

1. 카카오톡 서비스 개요

피심인은 2010. 3. 앱 기반의 메신저 서비스 '카카오톡(이하, 일반채팅)'을 출시한 이후 제공 기능과 연계 서비스를 확대하여, '선물하기'(2010. 12.), '이모티콘'(2011. 11.), '오픈채팅'(2015. 8.) 등 15개 기능과 카카오T 등의 외부 제휴 서비스(별도 앱/외부 웹 링크 방식으로 연결)를 포함하여 총 40여 개 기능과 서비스를 연계·제공하는 '슈퍼앱'으로 발전하였다.

카카오톡 이용자는 ① 카카오톡 앱 다운로드, ② 카카오 계정 만들기, ③ 휴대전화번호 등록(인증), ④ 프로필[프로필명(이름[2]) 또는 닉네임), 사진(선택)] 등록 이후 메신저 서비스인 '일반채팅'을 이용할 수 있다. 카카오톡의 '일반채팅'은 휴대전화번호 등을 통해 등록한 '친구' 또는 '친구 그룹'간 메신저 기능으로, 사전에

2) 피심인은 2023. 9. 13.까지 이용자가 카카오톡 회원가입 시 프로필명을 입력하도록 구성하면서, 프로필명 입력란의 기본 설정은 빈칸이지만 이용자의 입력을 유도하는 UI(User Interface) 화면상으로는 '이름(필수)'로 표기하여 운영하였다.

‘내친구 목록’에 추가한 ‘친구’를 클릭하여 선택한 경우에만 대화가 가능(그룹채팅방에 초대받는 경우는 친구 추가 없이 대화는 가능함)하다.

‘오픈채팅’은 관심·취미가 비슷한 카카오톡 이용자 누구나 오픈채팅방을 개설하고 참여할 수 있으며 참여자 간 상호 소통할 수 있는 대화 기능으로, ‘일반채팅’과 달리 ‘내친구 목록’에 등록되지 않은 비지인 간에도 대화(‘오픈채팅’)가 가능하다.

< 오픈채팅방 및 닉네임 예시 >

< 연령대별 수다 오픈채팅방 >	**< 오픈채팅방용 프로필명(닉네임) 예시 >**

다만, 카카오톡 이용자는 ‘오픈채팅’ 서비스에 대한 별도의 회원가입이나 로그인 또는 개인정보 수집·이용 동의 절차 없이 ‘오픈채팅’ 기능을 곧바로 이용할 수 있으며, 2015. 8. 오픈채팅 개시 시점부터 2023. 5.까지 ‘일반채팅’ 채팅방 목록과 ‘오픈채팅’ 채팅방 목록은 카카오톡 내에서도 같은 화면(2탭)에 위치[3]하고 있었다.

3) 2023. 5.부터 피심인은 ‘일반채팅’과 ‘오픈채팅’ 채팅방 목록 화면을 분리하여 운영 중이다.

2. 개인정보 유출 관련 사실관계

가. 개인정보 유출 경위

해커가 피심인의 보안 취약점을 이용해 피심인이 서비스하는 일반채팅과 오픈채팅에서 대량의 정보[4]를 획득한 후, 양 정보에 공통된 회원일련번호(　　)를 매개로 오픈채팅방 참여자들의 개인정보 DB를 완성하고 판매하였다. 판매된 개인정보 DB는 휴대전화번호, 프로필명(이름 등), 오픈채팅방 닉넥임, 회원일련번호, 오픈채팅방명 등으로 구성되어 있었다. 특히, 오픈채팅방은 앞서 설명한 대로 특정 관심사(예; 주식, 부동산, 투자 등)를 공유하는 사람들이 모여있어 마케팅(예, 타겟 광고)적 관심에서 가치가 높았고 그 결과 일반 개인정보 DB보다도 높은 가격에 거래되었다는 언론 보도 등이 있었다.

1) 일반채팅 정보의 취득

먼저 해커는 카카오톡 API[5]를 활용하여 제작된 비인가 프로그램[6](피심인은 "유사 클라이언트[7]"라고 지칭)를 이용해, 휴대전화번호 형식의 11자리 숫자를 무작위로 입력하여 카카오톡 회원인 이용자(휴대전화번호 점유자)를 카카오톡 친구로 추가한 다음, 친구로 등록된 일반채팅 이용자의 '휴대전화번호, 프로필명(이름 등), 회원일련번호(　　)[8]' 정보(A)를 취득하였다(친구추가 기능에 대한 상세 내용은 아래 3. 가. 1)항 참조).

---

4) 일부 언론(전자신문, 2023. 3. 14.)에서는 기자가 텔레그램 등을 통해 해커와 직접 접촉, 오픈채팅방을 무작위로 제시한 후 단시간내 해당 오픈채팅방 구성원의 DB를 받을 수 있었다고 지적하며, 해커가 카카오톡 이용자 대다수의 DB를 이미 확보하고 있을 것으로 추정하였으며, 정확한 유출 규모는 경찰에서 수사 중

5) API(Application Programming Interface) : 운영체제와 응용프로그램 사이의 통신에 사용되는 언어나 메시지 형식을 말하며, 시스템 내부 구조를 알 필요 없이 해당 API에 정의된 값(함수)을 입력(호출)하면 결과(응답)값을 사용할 수 있음

6) 공개된 카카오톡 API를 활용하고 기능 분석을 통해 일반 카카오톡에서 불가능한 각종 악성행위와 회원일련번호(　　) 확인 등이 가능한 프로그램으로, 피심인은 '유사 클라이언트'라고 부름

7) 공개된 카카오톡 API를 활용하고 기능 분석을 통해 일반 카카오톡에서 불가능한 각종 악성행위와 회원일련번호(　　) 확인 등이 가능한 프로그램으로, 피심인은 '유사 클라이언트'라고 부름

8) 카카오톡 가입 시 피심인이 이용자 식별을 위해 이용자에게 부여하는 고유번호로, 가입 이후 변경되지 않고 탈퇴 후 재가입하는 경우 새로 부여됨

2023. 3. 이 사건 조사 과정에서, 개발자 사이트인 [9]에 암암리에 노출되어 있는 비인가 프로그램 중 하나인 를 이용해 휴대전화번호를 무작위 입력하여 친구 추가와 동시에 추가된 친구의 회원일련번호( ) 등 정보(A)를 알아내는 행위가 피심인의 안티 어뷰징 시스템[10]을 통해 탐지·차단되지 않고 가능하다는 것이 확인되었다.

2) 오픈채팅 정보의 취득

해커는 비인가 프로그램으로 오픈채팅방명, 오픈채팅방 닉네임, 오픈채팅방 참여자의 임시ID( )[11]를 추출하고, 추출한 임시ID( )를 통해 회원일련번호( )를 알아내는 방법으로 오픈채팅방 이용자의 '회원일련번호( ), 오픈채팅방명, 오픈채팅방 닉네임' 정보(B)를 취득하였는데, 공격 대상이 된 오픈채팅방이 생성된 시기별로 다음와 같은 방법을 사용하였다.

2020. 8. 5. 이전에 생성된 오픈채팅방에서는 카카오톡 서버와 앱 간의 통신을 위해 사용하는 임시ID( )를 암호화되지 않은 평문으로 송수신하여, 해커가 평문 임시ID( )를 취득한 후 쉽게 회원일련번호( )를 알아낼 수 있었다(상세내용은 아래 3. 가. 3)항 참조). 또, 2020. 8. 5. 이후 생성된 오픈채팅방은 암호화된 임시ID( )를 사용하였지만, 해커가 오픈채팅방 게시판의 파라미터 변조 취약점을 이용해 암호화가 해제된 평문 임시ID( )와 회원일련번호( )를 알아낼 수 있었다(상세내용은 아래 3. 나. 2)항의 마) 참조). 이 과정을 거쳐 해커는 임시ID( ) 암호화 여부와 오픈채팅방이 생성된 시기에 상관없이 알아내고자 하는 특정 오픈채팅방 참여자의 '회원일련번호( ), 오픈채팅방명, 오픈채팅방 닉네임' 정보(B)를 취득하였다.

9)
10) 이용자 이용환경, 행동패턴 등을 종합적으로 고려하여 이용자 보호조치를 할 수 있는 비정상 이용자 모니터링 정책 (상세내용은 아래 3. 다. 2)에서 후술)
11) 이용자가 참여 중인 오픈채팅방을 구분하기 위해서 서버와 앱 간의 통신에 사용하는 식별번호로, 회원일련번호와 오픈채팅방ID로 구성되어 있음. 이용자가 특정 오픈채팅방에 참여하는 동안 동일한 임시ID( )가 유지되며, 해당 오픈채팅방을 탈퇴하였다가 재참여해도 동일한 임시ID( )로 이용자를 구분함

2023. 3. 이 사건 조사 과정에서, 비인가 프로그램(　　)를 이용해 특정 오픈채팅방 이용자의 임시ID(　) 등을 알아내는 행위가 피심인의 안티 어뷰징 시스템을 통해 탐지·차단되지 않고 가능하다는 것이 확인되었다.

3) 카카오톡 오픈채팅 이용자 개인정보 판매

해커는 일반채팅에서 획득한 정보(A)와 오픈채팅에서 획득한 정보(B)를 회원일련번호(　　)를 기준으로 조합하여 '특정 오픈채팅방 참여자'의 개인정보 파일을 완성하고 판매하였다. 판매된 개인정보 파일은 휴대전화번호, 프로필명(이름 등), 오픈채팅방 닉네임, 회원일련번호, 오픈채팅방명으로 구성되어 있다.

개인정보보호위원회와 한국인터넷진흥원의 검증 과정에서, 공개된 비인가 프로그램을 이용하면 위 정보를 일괄 취득할 수 있다는 점이 확인되었다.

< 일반 카카오톡과 비인가 프로그램 이용 시 확인 가능한 정보 비교(개인정보위 확인) >

	일반 카카오톡(공개정보)	비인가 프로그램(카카오톡API 활용)
일반채팅 <친구추가 시>	휴대전화번호, 프로필명(이름 등), 상태메시지, 프로필사진	휴대전화번호, 프로필명(이름 등), 상태메시지, 프로필 사진, 회원일련번호(　　)
오픈채팅 <오픈채팅방 접속 시>	오픈채팅방명, 오픈채팅방 닉네임	오픈채팅방명, 오픈채팅방 닉네임, 임시아이디(　　)

나. 유출된 개인정보의 항목과 규모

개인정보보호위원회와 한국인터넷진흥원이 2023. 3.　　인(　　)에 업로드되어 있는 개인정보 파일 2개를 확보하여 분석한 결과, 카카오톡 오픈채팅방 이용자 696명의 개인정보(회원일련번호, 프로필명, 휴대전화번호, 오픈채팅방명, 오픈채팅방 닉네임)가 포함되어 있는 사실을 확인하였다. 같은 달인 2023. 3. 현장 조사 과정에서도 피심인의 카카오톡 일반채팅 DB와 오픈채팅 DB에 각각 저장된 이용자 정보와 개인정보보호위원회가　　에서 입수한 파일 내 개인정보가 일치하는 것이 확인되었다.

< ‘ ’에서 입수한 카카오톡 오픈채팅 이용자 개인정보 파일 현황 >

오픈채팅방명	유출 규모	오픈채팅방 생성시점
	679명	2022.12.23.
	17명	2018.01.13.

피심인이 제출한 자료에 따르면, 2023. 2. 10.부터 2023. 3. 10.까지의 한 달 동안에만 해커로 추정되는 자(개 계정)가 다른 오픈채팅방 참여자의 임시ID( )를 총 156,493건(중복 제거 시 65,719건) 조회한 것으로 확인되었다[12]. 피심인은 관련 로그를 만 보관하고 있어, 이전에 임시ID( )를 조회한 건수는 확인이 불가능하다고 소명[13]하였다.

< 해커의 게시판 API 호출을 통한 임시ID( ) 조회 현황 >

기준	진입 채팅방수		게시판 API 호출수	조회 임시ID ( )(중복)	조회 임시ID ( )(중복제거)
로그 보관기간 ( )	암호화X				
	암호화O				
사건 인지 당일 ('23.3.10.)	암호화X				
	암호화O				

다. 개인정보 유출 신고·통지 현황

2023. 3. 12. 카카오톡 오픈채팅 이용자의 개인정보 유출과 관련된 최초 언론 보도 이후, 2023. 3. 14. ‘카톡 오픈채팅 해킹...1명당 단가 7,000원·2시간 만에 ‘뚝딱’(전자신문)’ 등 다수의 뉴스 기사에서 카카오톡 오픈채팅방 이용자의 개인정보가 유출되고 있다고 보도하였다. 피심인은 2023. 3. 이루어진 개인정보보호위원회 조사과정에서 ‘ ’ 사이트에 공개된 특정 오픈채팅방 이용자의 개인정보가 피심인이 관리하는 카카오톡 일반채팅 DB 및 오픈채팅 DB 내 정보와 일치하는 사실도 확인하였다.

12) 게시판 API 호출 시 멘션에 포함된 임시ID( )가 실제 해당 오픈채팅방에 참여하지 않는 다른 오픈채팅방 참여자의 임시ID( )인 경우를 의미함

13) 실제로 확인된 696명의 개인정보[회원일련번호( ), 프로필명, 휴대전화번호, 오픈채팅방명, 오픈채팅방 닉네임]만이 아니라 최소 65,719명의 개인정보가 유출되었을 것으로 추정됨

그러나, 피심인은 개인정보보호위원회가 2024. 2. 16. 피심인에게 개인정보 유출 신고·통지 소홀로 인한 과태료 부과 등에 관한 사전통지서를 송부하고 이 사건 의결에 이르기까지 개인정보 유출 신고와 개인정보가 유출된 이용자를 대상으로 유출 통지를 하지 않은 사실이 있다.

3. 피심인의 개인정보 취급.운영 관련 사실관계

가. 피심인의 카카오톡 서비스 제공

1) 2010. 3. 카카오톡 '일반채팅' 서비스 개시

피심인은 2010. 3. 카카오톡 앱을 출시한 이후 현재까지, 휴대전화 등 단말기에 저장되어 있는 연락처 정보(휴대전화번호)를 이용해 카카오톡 '친구'로 등록하거나 휴대전화번호를 직접 입력하여 '친구'로 등록하는 기능을 제공하고 있다. 이용자가 휴대전화번호로 카카오톡 '친구'를 등록할 때, 해당 휴대전화번호를 점유한 카카오톡 이용자가 있다면, 이용자는 해당 휴대전화번호를 점유한 당사자의 동의나 인지 없이도 그 당사자의 카카오톡 프로필명(이름 또는 닉네임), 프로필 사진 등을 확인할 수 있다.[14)]

2) 2011. 로코 프로토콜의 개발 적용

피심인은 2011년경 카카오톡 이용자 증가에 대비하기 위해 경량화된 로코 프로토콜[15)]을 개발하고 카카오톡의 메시지 전송 방식으로 사용하기 시작하였다.

3) 2015. 8. 카카오톡 '일반채팅'과 연계한 '오픈채팅' 서비스의 개시

가) 피심인은 2015. 8. 카카오톡 일반채팅의 친구로 등록되지 않은 이용자끼리도

14) 피심인은 회원일련번호( )를 통해 이용자를 식별하고 관리하며, 이용자가 일반채팅으로 친구에게 메시지를 보낼 때에는 [회원일련번호( ), 메시지 내용] 형태로 메시지를 송수신하도록 서비스를 구성·운영

15) 패킷 사이즈 경량화 등 개선을 통해 최적화된 메시지를 지연 없이 전송할 수 있는 피심인 고유의 프로토콜

별도 프로필을 사용하여 소통할 수 있는 '오픈채팅' 서비스를 개시[16]하였다.

나) '오픈채팅'은 관심·취미가 비슷한 카카오톡 이용자 누구나 오픈채팅방을 개설하고 참여할 수 있으며 참여자 간 상호 소통할 수 있는 대화 기능으로, '일반채팅'과 달리 '내친구 목록'에 등록되지 않은 비지인 간에도 대화('오픈채팅')가 가능하다. 오픈채팅방은 '일반채팅'에서 사용하는 프로필[프로필명(이름 또는 닉네임), 사진]과 다르게 참여하는 특정 오픈채팅방 내에서만 사용하는 프로필(닉네임, 사진)을 별도로 설정할 수 있어, 익명성이 보장[17]된다고 설명한다.

다) 그러나, 피심인은 오픈채팅방에 참여하는 이용자를 식별하고 관리하기 위해서 서버에서는 일반채팅에서 이용하는 회원일련번호( )를 동일하게 활용하고 있으며, 이용자가 오픈채팅으로 메시지를 주고받을 때에는 회원일련번호( ) 대신 임시ID( )를 사용하도록 구성한 후, [임시ID( ), 메시지 내용] 형태로 메시지를 송수신하였다. 그러나, 임시ID( )는 회원일련번호( )와 이용자가 참여한 오픈채팅방 정보( )를 로 변환한 후 단순 연결한 다음 로 다시 변환한 것에 불과하다.

라) 결론적으로 오픈채팅방 참여자의 임시ID( )는 그 구조상 로 변환한 임시ID( )의 를 떼어내 로 변환하면 회원일련번호( )에 해당하여, 오픈채팅방 이용자의 임시ID( )를 알면 그 이용자의 회원일련번호( )도 쉽게 알 수 있다.

16) 피심인이 '15.8.31. 발표한 보도자료(https://kakaocorp.com/page/detail/7813)에 따르면, 오픈채팅 서비스를 통해 개인정보 공개에 대한 불편함 없이 더 많은 사람과 쉽고 편하게 채팅할 수 있는 수단을 제공하고, 이는 이용자의 프라이버시를 강화하는 데 의미가 있다고 본다고 밝힘

17) 피심인이 '15.8.31. 발표한 보도자료(https://kakaocorp.com/page/detail/7813)에 따르면, 오픈채팅 서비스를 통해 개인정보 공개에 대한 불편함 없이 더 많은 사람과 쉽고 편하게 채팅할 수 있는 수단을 제공하고, 이는 이용자의 프라이버시를 강화하는 데 의미가 있다고 본다고 밝힘

< 임시ID( )에서 회원일련번호를 추출하는 과정>

①임시ID( ) :

↓(로 변환)

②임시ID( ) :

구조
( ) = | ( ) | ( ) | ( ) |

↓(를 로 변환)

③회원일련번호( ) :

4) 2018. 9. 6. 오픈채팅 게시판 기능 도입, 2020. 2. 멘션 기능의 도입

2018. 9. 6. 피심인은 '오픈채팅'에 공지사항 등을 게시하는 '게시판 기능'을 추가하였고, 2020. 2. 해당 오픈채팅방에 참여한 이용자를 게시글, 메시지 등에서 언급하는 '멘션 기능'[18]을 추가하였다.

나. 카카오톡 비인가 프로그램(유사 클라이언트)의 공개 및 피심인의 대응

1) 2012. 2. 로코 프로토콜 분석 내용의 최초 공개

2012. 12. 5.부터 피심인이 개발한 로코 프로토콜을 역분석한 내용이 개발자 사이트에 공개적으로 게시[19]되기 시작하였다. 특히, 2012. 12. 8.에 게시된 로코 프로토콜의 보안 취약점 분석 글에는 휴대전화번호만으로 쉽게 해당 이용자의 카카오톡 회원일련번호( )와 프로필 정보를 추출하는 방법 등이 포함[20] 되어 있었다.

---

18) 채팅메시지 또는 채팅방 게시글 작성 입력창에 '@'+닉네임을 입력하여 해당 오픈채팅방에 존재하는 닉네임 소유자에게 알림을 보내는 기능

19)

20)

2) 2020. 5. ~ 2020. 10. 비인가 프로그램 공개와 피심인의 대응

가) 2020. 5. 2. 카카오톡 비인가 프로그램 ( )가 개발자 사이트인 에 최초 게시[21]된 이후 지속적으로 업데이트되어 ( )가 2021. 11. 21.에 공개되었다. 이 때, 비인가 프로그램을 이용해 일반 카카오톡 앱에서는 불가능한 여러 기능을 구현하는 방법과 그 소스코드도 함께 공개되어 불특정 다수의 사람에게 공유되었다(개발자 사이트 에는 뿐만 아니라, [22] 등 카카오톡 API를 활용한 오픈소스[23] 라이브러리가 다수 공개되어 있다.).

나) 2020. 7. 23. 피심인도 "카카오톡의 통신 프로토콜을 분석해 유사 클라이언트를 제작할 수 있는 라이브러리가 시중에 공개되어 있고, 오픈채팅방을 통해 1백여 명의 사람들이 비슷한 정보를 나누고 있는 것을 발견했습니다. 이러한 기술과 지식이 악용될 경우, 우리 서비스 시스템에 실질적 피해(서비스 불가 상태 발생)를 줄 수 있으며, 스팸 기계(프로그램)를 만드는 데 쓰이는 등으로 인해 서비스에 악영향 및 신뢰도 추락을 초래할 수 있는 상황입니다."라고 내부적으로 논의하는 등 관련 이슈를 인지하고 있었다. 피심인은 이에 대해 저작권법, 정보통신망법, 형법 등의 침해 여부에 대한 법률 검토를 추진하였으나 알 수 없는 이유로 더 이상의 대응을 보류하였다고 소명하면서 관련 자료를 제출하지 않았다.

다) 2020. 7. 24. 비인가 프로그램 를 통해 카카오톡에 존재하지 않는 기능들을 구현할 수 있고 온라인 커뮤니티를 통해 해당 프로그램이 암암리에 이용되고 있다는 내용의 글이 게시[24]되었다.

라) 2020. 8. 5. 피심인은 새로 생성되는 오픈채팅방에 한하여 참여자의 임시ID ( )를 암호화[25]하여 전송하도록 시스템을 변경하였다[26] 그러나, 2015. 8. 오픈

21) 작성자 는 2012. 12. 게시된 " "(각주13참조) 글을 로 하여, 을 에 공개함

22) 작성자 는 2020. 5. 카카오톡 API를 활용한 오픈소스 라이브러리를 제작하여 카카오톡 일반채팅 이용자 회원일련번호( ) 조회 등 행위를 할 수 있는 방법과 소스코드와 함께 에 공개함

23) 누구나 검사, 수정 및 개선할 수 있는 소스코드가 포함된 소프트웨어

24) ('20.7.24.)( )

채팅 서비스 개시 시점부터 2020. 8. 5. 이전까지 생성된 오픈채팅방은 여전히 참여자의 임시ID( )를 암호화하지 않은 평문으로 사용하는 방식을 유지함으로써, 이용자의 임시ID( )로부터 회원일련번호( )를 쉽게 알 수 있는 상황이 지속되었다. 그 결과, 2년 7개월이 지난 2023. 3. 20.에도 오픈채팅방 참여자 최대 명의 임시ID( )가 평문 상태로 사용되고 있었다.

마) 한편, 오픈채팅방 참여자의 임시ID( )가 암호화된 경우에도 오픈채팅방 게시판의 멘션 기능 관련 보안 취약점을 이용하면 암호화가 해제된 임시ID( )를 알아낼 수 있었는데 그 구체적인 방법은 다음과 같다.

① 2020. 8. 5. 이후 생성된 오픈채팅방(임시ID 암호화)에 입장하여 해당 오픈채팅방 참여자의 암호화된 임시ID( )를 취득한다.
② 2020. 8. 이전에 생성된 오픈채팅방(임시ID 평문)의 게시판에서 게시글을 작성하면서 암호화된 임시ID( )를 멘션한다.
③ 게시글 게시 요청에 대한 응답값으로부터 암호화가 해제된 평문 임시ID( )를 취득한다[27].

이 과정이 가능한 이유는 멘션(@ 입력 후 알림을 보낼 닉네임을 선택)할 때 해당 오픈채팅방에 존재(참여)하지 않은 타 오픈채팅방 참여자의 임시ID를 변조하여 입력하는 경우에도 차단되지 않고 정상 처리되는 파라미터 변조 취약점[28]과, 멘션한 이용자의 임시ID( )가 응답값으로 전송되는 구조 때문이었다. 그 결과, 2020. 8. 이후에 생성된 오픈채팅방 참여자의 임시ID( )가 암호화되었다 하더라도, 암호화가 해제된 평문 임시ID( )를 쉽게 확인할 수 있었고, 이 평문 임시ID( )를 통해 해당 이용자의 회원일련번호( )도 쉽게 알 수 있었다.

25) 피심인은 (알고리즘)을 사용하였다고 소명함
26) 피심인은 이용자들의 오픈채팅 서비스 이용 패턴이 '익명성'에 집중하는 쪽으로 변화함에 따라 서비스 안전성 등을 다각도로 검토하여 2020. 8월 이후에 생성되는 오픈채팅방에 대해서만 임시ID( ) 암호화를 적용하였다고 소명
27) 응답값에 포함된 임시ID( )는 오픈채팅방 생성 시기에 따라서 암호화 또는 평문 형태로 전송되었으며, 위 과정 ②는 오픈채팅방 생성시기가 2020. 8. 이전이므로 평문 임시ID( )가 전송됨
28) 파라미터 변조는 웹 브라우저에서 웹 서버로 전달하는 파라미터 값을 임의로 변경함으로써 정상적인 경우의 통신 결과와 달라지는 결과를 기도하는 것으로, 널리 알려진 해킹 수법임

바) 2020. 10. 피심인은 개발자 사이트인 에 비인가 프로그램 관련 게시글을 삭제 요청하였으나 게시글은 현재까지 삭제되지 않았다.

사) 개인정보보호위원회와 한국인터넷진흥원은 조사에 착수한 이후 내부 시연[29]을 통해, 비인가 프로그램을 이용한 카카오톡 시스템 접속과 일반적인 카카오톡에서는 가능하지 않은 기능(대규모 친구추가 자동화, 회원일련번호·임시ID 등 정보의 일괄 확인 등)을 사용할 수 있음을 확인하였다. 피심인은 조사 과정에서 와 같이, 공개된 카카오톡 API를 이용하여 제작된 비인가 프로그램을 사용하는 것은 회사 정책에 반한다고 소명하였다.

3) 2021. 8. ~ 2023. 1. 카카오톡 보안 위험성 제보 관련 피심인의 대응

가) 2021. 8. 12. 개발자 사이트의 관련 토론방 내 게시글[30]에서 카카오톡 이용자의 회원일련번호( )와 2020. 8. 이전에 생성된 오픈채팅방 참여자의 임시ID( ) 간 연결 로직이 확실히 존재하고, 2020. 8. 이후에 생성된 오픈채팅방 참여자의 임시ID( )가 그 이전에 생성된 오픈채팅방 참여자의 임시 ID( )와 다르다면서, 연결 로직에 해당 오픈채팅방 ID( )가 연관되어 있을 가능성도 있다는 점이 언급되었다.

나) 2021. 8. 15. '카카오톡 로코 프로토콜 악용사례 처리 요청'이라는 글이 피심인이 운영하는 공식 개발자 커뮤니티 사이트 '데브톡'에 게시[31]되었다. 제보자는 카카오톡의 통신 프로토콜인 로코 프로토콜이 역분석되어 악용되고 있고, 오픈채팅방의 질서를 어지럽히는 사례가 발생하고 있으며, 카카오톡 고객센터로 신고하여도 대처가 안되고 있다고 주장하면서 기술적인 차단방안을 요청하였다.

다) 2021. 8. 21. 온라인 커뮤니티인 ' '에 한 이용자가 '뉴스 20곳에 모두 제보했음(카카오톡 보안망 뚫림/로코)'이라는 제목으로 글을 게시[32]하고,

---

29) 에 공개된 비인가 프로그램 를 통해 일반채팅 참여자의 회원일련번호( ) 등과 오픈채팅 참여자의 임시ID( ) 등의 정보를 확인하는 시연임

30) ' '('21.8.12.)( )

31) (현재 삭제된 상태)

관련 영상을 링크하였다. 게시글에는 “카카오톡에서 송/수신되는 메시지를 모두 볼 수 있음”, “유저들의 IP 주소 딸 수 있음”, “카카오톡 보안이 뚫려 모든 내용을 알 수 있음”, “1년 이상 수많은 사용자들이 패킷을 이용한 악용”, “현재 소스코드는 뿌려졌으며, 판매되는건 1만원~30만원에 거래 되고 있음”이라는 내용이 언급되었다. 이외에도, 유튜브[33]에는 비인가 프로그램을 통해 정상적인 카카오톡 환경에서 보이지 않는 정보를 확인할 수 있는 기능 등 각종 악성행위를 시연하고 비인가 프로그램을 판매하는 영상도 다수 존재하였다.

라) 2023. 1. 10. ‘카카오톡 오픈채팅방의 보안 허점과 개인정보 누출’ 문제를 지적하는 게시글이 ‘데브톡’에 게시[34]되었다. 제보자는 비인가 프로그램으로 로그인하는 악성행위자가 늘어나고 있고, 악성행위자들이 오픈채팅방 참여자의 회원일련번호( )와 이메일 주소, 휴대전화번호까지 추출해 공개하고 있으며, 카카오톡 API를 사용해 카카오톡에서 불가능한 각종 악성행위가 가능하다는 내용과 함께 관련 캡처 화면을 첨부하였다. 그러나 카카오 측은 관련 업무 처리는 카카오톡 고객센터에 제보 부탁드린다는 답변[35] 외 별도의 조치를 취하지 않았다.

다. 언론 보도 이후 피심인의 대응

1) 2023. 3. 언론의 카카오톡 보안 문제 취재 및 피심인의 대응

가) 2023. 3. 10. 피심인은 카카오톡 오픈채팅 시스템의 보안상 취약점 관련 언론사의 취재 요청 이후에야 오픈채팅방 게시판에 게시글 작성시 참여자 검증 절차[36]를 추가하였다.

나) 2023. 3. 12. 은 ‘카톡 오픈채팅 보안 구멍 뚫렸다’라는 제목으로, 카카오톡 로코 프로토콜의 보안 결함으로 인해 오픈채팅 이용자의 실명·휴대전화

32)
33) ('21.11.27.), ('21.12.10.) 등
34) (현재 삭제된 상태)
35) (현재 삭제된 상태)
36) 오픈채팅방 게시판에서 해당 오픈채팅방이 아닌 다른 오픈채팅방의 참여자 임시ID를 멘션하는 경우, 참여자인지 여부를 확인하여 게시글 입력이 차단됨

번호를 비롯한 개인정보가 고가에 거래되고 있다고 보도하였다. 구체적으로는, 불법 솔루션 판매자와 접촉해 '테스트'를 요청하면 지목한 오픈채팅방에서 사용하는 닉네임, 실명, 휴대전화번호가 포함된 리스트를 샘플로 제공하며, 정식 거래 단가는 통상 유통되던 불법 DB의 수십 배에 달하고, 당시 유출된 실명과 전화번호는 실제 사용자와 일치하는 것으로 확인됐다는 내용이었다. 또, 비인가 프로그램으로 특정 오픈채팅방에 접속하면 회원일련번호( )를 추출하여 해당 회원일련번호( )와 연결된 카카오톡 이용자의 프로필 정보를 캐낼 수 있는 보안 취약점이 발견되었다는 내용도 있었다.

다) 2023. 3. 11.부터 2023. 3. 13.까지 피심인은 오픈채팅방 활동현황 관련 로그를 자체적으로 분석하여 카카오톡 오픈채팅방 게시판 API를 비정상적으로 호출(오픈채팅방 게시판에 다른 오픈채팅방에 참여하는 이용자의 임시ID( )를 멘션하여 API를 호출한 행위)한 계정 등 19개 계정을 영구 이용제한(카카오톡 모든 기능 이용불가, 계정정지) 조치하였다.

라) 2023. 3. 14. 은 '카톡 오픈채팅 해킹...1명당 단가 7,000원·2시간만에 뚝딱'이라는 제하의 후속 기사를 보도하였다. 기자는 제보자와 함께 카카오톡 오픈채팅 이용자의 개인정보를 불법 판매한다는 텔레그램 광고글 게시자와 접촉하여, 기자와 제보자가 입장해 있는 오픈채팅방의 링크주소와 해당 오픈채팅방에서 기자가 사용하는 닉네임을 포함해 10개 닉네임을 대상으로 지목하여 개인정보를 요청하였으며, 해커가 두 시간만에 휴대전화번호와 실명, 숫자, 유저 아이디(회원일련번호)가 포함된 엑셀표를 캡처하여 전달하였다는 내용이었다.

<참고 : 해커가 기자·제보자에게 제공한 개인정보파일 해당 오픈채팅방>

오픈채팅방명	유출 규모	오픈채팅방 생성시점
	10명	2022.10.6.

마) 2023. 3. 14. 개인정보보호위원회는 한국인터넷진흥원과 함께 이 사건에 대해 조사에 착수하고, 2023. 3. 15. 경찰청, 과학기술정보통신부, 한국인터넷진흥원 합동 1차 현장 조사를 포함한 서면 조사, 현장 조사 등을 진행하였다.

2) 2023. 4. 안티 어뷰징 시스템 정책 보완

이 사건 조사 과정에서, 피심인은 '안티 어뷰징 시스템'을 통해 카카오톡을 비정상적인 방법으로 이용하여 이득을 취하는 어뷰징 행위[37]를 탐지하여 제재하고 있으며, 언론보도 이후인 2023. 4.초에는 기존 안티 어뷰징 시스템의 정책을 보완하기 위하여 추가로 정책을 적용하였다고 소명하였다. 피심인이 소명한 안티 어뷰징 시스템 정책의 변경 이력을 종합하면 다음와 같다.

< 피심인의 안티 어뷰징 정책 변경 이력 >

일 시	정책 적용
'11. 상반기	
'14. 1분기	
'14. 12.	
'19.	
'21. 5.	
'21. 10.	
'22. 2.	
'23. 4월초	

37) 판단기준은 등을 종합적으로 고려한다고 소명함

일 시	정책 적용

※ ‘ ’의 구체적인 범위 등은 영업비밀이라는 이유로 제출하지 않음

3) 2023. 5. 임시ID( ) 암호화 및 휴대전화번호 친구추가 설정 개선

가) 2023. 5. 3.에서야 피심인은 모든 오픈채팅방 참여자의 임시ID( )에 대한 암호화 조치를 위하여 카카오톡 앱을 업데이트하도록 이용자에게 안내하고, 앱 업데이트를 하지 않는 경우 카카오톡 메시지 작성이 제한되도록 조치하였다. 이를 통해, 2015. 8. 오픈채팅 서비스 개시 시점부터 2020. 8. 5. 이전까지 생성된 오픈채팅방 참여자의 임시ID( )를 포함한 모든 오픈채팅방 참여자의 임시ID( )가 비로소 암호화되었다[38].

나) 피심인은 기존에는 카카오톡 회원가입 시 프로필 입력 단계에서 프로필명에 ‘이름(필수)’을 입력하도록 안내하였으나, 2023. 9. 13. ‘닉네임’으로 안내 문구를 변경하였다.

다) 2023. 9. 14. 피심인은 휴대전화번호를 입력하여 제3자가 친구로 추가하지

38) 2023. 3. 20. 기준, 임시ID( ) 암호화 미적용 오픈채팅방은 % 수준임

구분	오픈채팅방	참여자수(중복 포함)	비율
암호화			
암호화 미적용			
계			

2023. 3. 20. 기준으로 최근 1개월 내 메시지 수발신 내역이 존재하는 ‘활성화’된 오픈채팅방 총 개 중 암호화가 적용되지 않은 오픈채팅방은 개로 여기에 참여한 참여자는 명임

못하도록 이용자가 설정하는 기능을 추가하였으나, 기본 설정은 휴대전화번호 입력을 통한 친구추가를 '허용'하는 것이었다.

< 언론취재 이후 피심인의 대응 경과 >

일 시	피심인의 유출 인지 및 대응 내용
'23. 3. 10.	언론 취재요청으로 오픈채팅방 개인정보 관련 사고 인지
'23. 3. 10.	오픈채팅방 게시판의 게시글 내 참여자 검증* 절차 추가 * 오픈채팅방 게시판에서 해당 오픈채팅방에 존재하지 않는 다른 오픈채팅방 참여자 ID를 멘션하는 경우 게시글 입력을 차단
'23. 3. 11. ~ '23. 3. 13.	로그를 분석하여, 비정상 호출이 발생한 공격자 계정(개) 영구제재 조치
'23. 3. 13.	'오픈채팅방 불법 행위 관련 조치 및 대응' 이용자 공지 및 한국인터넷진흥원 사이버침해대응센터 사고 신고
'23. 4월 초	안티 어뷰징 시스템 내 안티어뷰징 탐지·차단 정책 추가 적용
'23. 5. 3.	오픈채팅방 임시ID( ) 암호화 및 이용자 앱 업데이트 안내 공지
'23. 9. 13.	카카오톡 회원가입 시 프로필 이용자 "이름" → "닉네임" 변경
'23. 9. 14.	휴대전화번호로 친구추가 설정 기능(기본값 : 허용*) 추가 * '23.9.14. 이전에는 휴대전화번호 무작위 대입을 통해 친구추가가 가능하나, '23.9.14. 이후에는 비허용 설정시 해당 휴대전화번호로 친구추가 불가

Ⅲ. 위법성 판단

1. 개인정보 해당성 및 유출 여부에 대한 판단

가. 개인정보 해당성

1) '이 사건 유출정보'의 특징

이 사건에서 해커가 취득한 정보 집합(회원일련번호, 프로필명, 휴대전화번호, 오픈채팅방명, 오픈채팅방 닉네임, 이하 '이 사건 유출정보')은 이용자의 관심 주제를 나타내는 오픈채팅방 명칭(예: ,)과 프로필명(이름 등), 휴대전화번호를 포함하고 있다.

특히, 피심인이 제공하는 오픈채팅 서비스는 익명성을 특징으로 내세우고 실제 오픈채팅방별 전용 프로필을 설정할 수 있어, 이용자들이 이러한 익명성을 전제로 내밀한 정보를 공유하는 경우(예:기혼/돌싱/연애, 건강/다이어트, 자취/고민 오픈채팅방 등)도 많다. 또, 오픈채팅방명으로 이용자의 관심 주제가 특정되므로, 특정 오픈채팅방 참여자의 휴대전화번호 등 개인정보를 알게 되면 영리나 홍보 목적의 개인정보 활용 가능성이 크다는 특성이 있다. 실제, '이 사건 유출정보'는 1건당 5천 원에서 2만 원까지의 적지 않은 가격에 판매된 것으로 알려졌고, 스팸 메시지를 수신한 오픈채팅방 운영자의 인터뷰가 방송을 통해 보도되는 등[39], 일반적인 식별정보나 연락처 정보와 달리 정보주체의 사생활 피해 우려가 큰 정보에 해당한다.

2) 관련 규정 및 개인정보 해당성에 대한 판단

舊 개인정보 보호법(법률 제16930호, 2020 2. 4. 일부개정, 2020. 8. 5. 시행, 이하 '舊 보호법') 제2조제1호는 개인정보란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다고 하면서, 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보와 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보를 개인정보로 정의하고 있다. 이 때, 쉽게 결합할 수 있는지 여부에 관하여는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다고 규정하고 있다.

39) [단독] 오픈채팅방 개인정보 유출 "6만 5천 건"(SBS 뉴스, 24. 5. 7.)

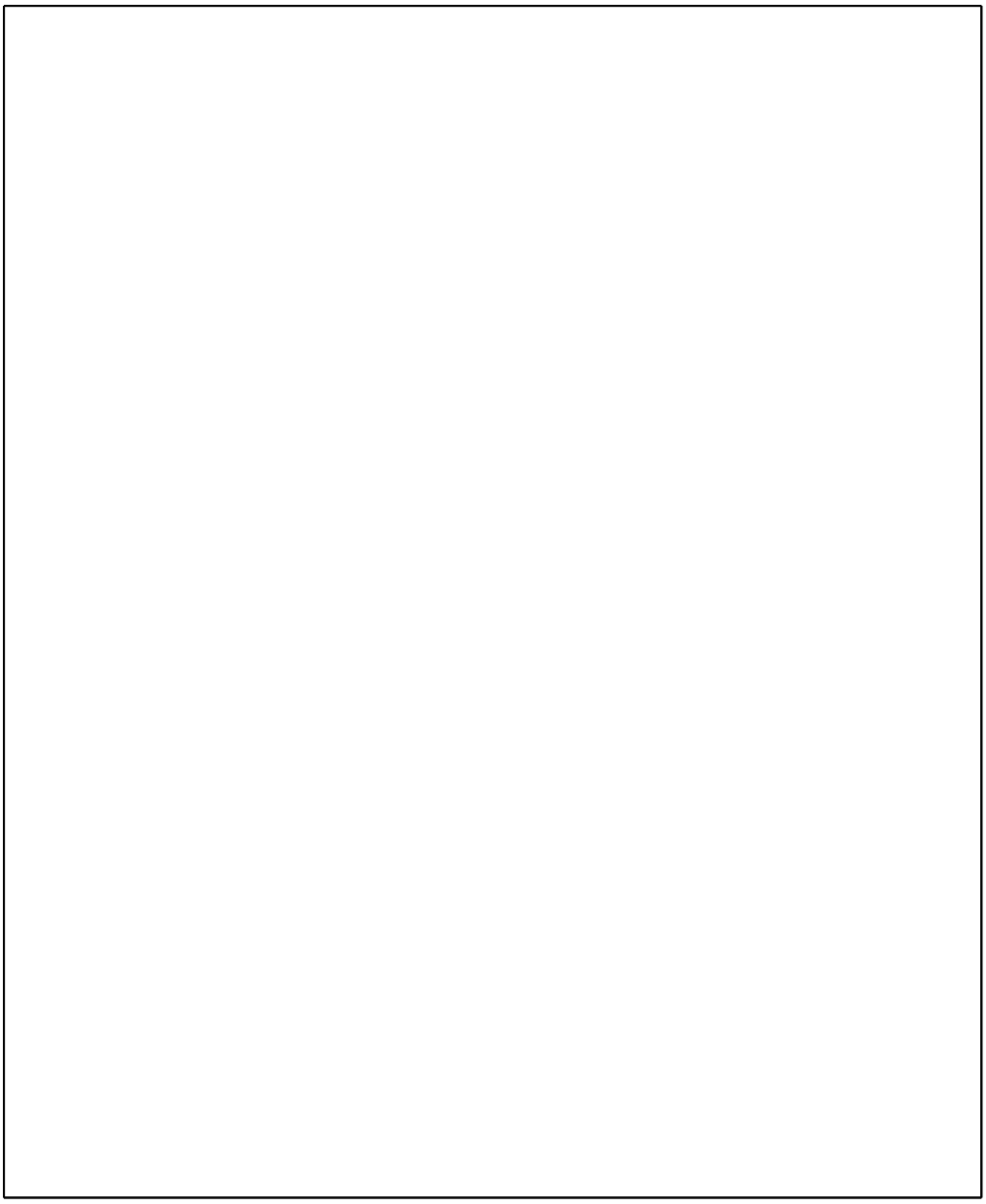
그런데, 앞서 본 바와 같이 '이 사건 유출정보'는 휴대전화번호, 프로필명(이름 등), 회원일련번호(　　), 오픈채팅방명, 오픈채팅방 닉네임 등 개인의 식별이 가능한 개인정보의 집합으로서 존재하고 있으므로, 개인을 알아볼 수 있는 정보로서 舊 보호법 제2조제1호의 개인정보에 해당함은 분명하다.

3) 회원일련번호(　　)(또는 임시ID(　　))가 개인정보가 아니라는 피심인의 주장에 대한 판단

피심인은 ① 회원일련번호(　)(또는 임시ID(　))가 개인정보에 해당하지 않고, ② 해커가 일반채팅 정보를 수집하는 과정(DB 사전제작)에 불법성이 개입되어 있으므로, 그 입수 가능성을 고려할 때 이는 쉽게 결합할 수 있는 정보가 아니라는 주장을 제출한 바 있다.

① 그러나, 이 사건에서 개인정보인지 여부를 판단하여야 하는 정보는 회원일련번호(　)(또는 임시ID(　))가 아닌 '이 사건 유출정보'이다. '이 사건 유출정보'에는 이용자가 참여한 오픈채팅방의 명칭과 휴대전화번호, 이름(프로필명) 등이 포함되어 있어, 이용자의 관심사 등을 추론할 수 있고, 이름(프로필명)을 언급하며 전화와 문자메시지 등 연락을 취함으로써 이용자에게 영향을 미칠 수 있으므로, 특정 오픈채팅방에 참여한 개인을 알아볼 수 있는 정보로서 개인정보에 해당한다. 또한, 이미 '이 사건 유출정보'의 집합이 유출된 상황에서(상세내용은 아래 나. 2) 참조) 회원일련번호(　　) 또는 임시ID(　)만 분리하여 개인정보가 아니라고 주장하는 것은 사실과 다르며 현실을 왜곡하는 것으로서 부적절하다.

< ‘이 사건 유출정보’ 일부 발췌 >



한편, 개인정보 보호 법령 및 지침·고시 해설(이하 ‘개인정보 보호법 해설서’)에서는 “해당 정보를 ‘처리하는 자’의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당한다.”고 설명하고 있다. 이에 따르면, 회원일련번호(　　)는 그 자체로도 개인정보에 해당할 뿐만 아니라, 회원일련번호(　　)를 기준으로 추가적인 정보(‘이 사건 유출정보', 프로필 사진, 이메일 주소 등)를 보유·관리하고 있는 피심인은 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있으므로, 회원일련번호(　　)도 개인정보에 해당한다.

② 다음으로, ‘이 사건 유출정보'는 그 자체만으로도 피심인뿐만 아니라 해커, 구매자, 또는 객관적 제3자 입장에서 충분히 개인의 식별이 가능한 정보, 즉 개인정보로서 舊 보호법 제2조제1호 가목의 정보에 해당한다. 따라서 해킹 과정의 일부인 일반채팅 정보 취득(DB 사전제작)의 어려움을 검토하며 개인정보의 입수 가능성을 논할 실익이 없다. 나아가 ‘이 사건 유출정보'에 포함된 회원일련번호( ), 휴대전화번호, 임시ID( ), 참여 오픈채팅방 명칭 등을 결합하는데 필요한 정보의 입수 가능성을 보더라도, 이는 극히 고도의 해킹으로써만 취득될 수 있는 것은 아니고, 개발자 사이트 등에 이미 확산되어 있던 비인가 프로그램 및 로코 프로토콜 역분석 정보 정도만 가지고도 취득할 수 있는 성질의 것이다. 실제 이 사건을 조사한 개인정보보호위원회와 한국인터넷진흥원 또한 개발자 사이트 등에 게시된 취약점 제보글을 참고하여 임의의 오픈채팅방에서 ‘이 사건 유출정보'를 쉽게 추출·결합할 수 있었던 점 등을 고려할 때, 개인정보 해당요건인 입수 가능성 또한 충분히 인정될 수 있다[40].

한편, 입수 가능성을 판단함에 있어 해킹 등 불법적인 방법으로 취득한 정보까지 포함한다고 볼 수 없다는 피심인의 주장은 입수 가능성의 규범적 판단과 관련하여 관념적·가정적으로 그 가능성의 범위를 설정해야 할 때 불법적인 방법으로 취득한 경우까지 상정하는 것은 곤란하다는 것으로 이해된다. 그러나 이 사건과 같이 이미 해킹이 발생하여 그 결과 해커나 다른 제3자가 실제로 특정 정보를 보유하고 있는 경우에 대해서까지 그 정보를 개인정보성 판단 과정에서 고려할 수 없다는 피심인의 주장은 ‘(가정적) 입수 가능성’과 ‘실제 입수된 상태’를 구별하지 못한 부당한 것이다. 나아가, 해커는 본질상 불법적인 행위를 통해 개인정보를 습득하기 마련인데, 이 때 수집 과정에 정당성이 결여되거나 불법성이 개입되어 있다는 이유로 입수 가능성이 부정된다면 해킹으로 개인정보가 유출되는 경우 언제나 개인정보 해당성이 부정된다는 주장과 다를 바 없어 이는 매우 잘못된 것이다.

---

40) 언론에서도 특정 오픈채팅방 링크주소와 닉네임 전달 후 2시간이 경과하자 실명, 휴대전화번호, 유저아이디가 포함된 엑셀표를 확인하는 것이 가능했다는 점이 보도되었음([단독]카톡) 오픈채팅 해킹…1명당 단가 7000원, 2시간 만에 ‘뚝딱’(2023. 3. 15.)

나. 개인정보 유출 여부

1) 관련 규정 및 '유출' 여부에 대한 판단

요건대 해커가 취득한 '이 사건 유출정보'는 해커가 임의로 생성한 정보가 아니라 피심인이 관리·통제하던 일반채팅 정보와 오픈채팅 정보를 해커가 획득한 후 회원일련번호( )를 기준으로 나열한 것이다. 실제로, 피심인은 해커가 취득한 '이 사건 유출정보' 중 '회원일련번호( ), 프로필명, 휴대전화번호'는 카카오톡 일반채팅 DB에서, '회원일련번호( )(가 포함된 임시ID), 오픈채팅방명, 오픈채팅방 닉네임'은 카카오톡 오픈채팅 DB에서 처리하고 있다.

이처럼 해커는 피심인이 관리·통제하고 있던 '이 사건 유출정보'를 열람한 것은 물론, 일부는 웹사이트에도 공개하여 판매하였으므로, '이 사건 유출정보'는 피심인의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것으로서 개인정보가 유출된 것에 해당한다.

대법원 역시 개인정보 유출이란 '개인정보가 해당 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 의미한다'고 하고(대법원 2014. 5. 16. 선고 2011다24555, 2011다24562 판결 등 다수), 표준 개인정보 보호지침 제25조(개인정보의 유출등)에서도 "개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것"이라고 규정하고 있다.

2) 임시ID( )만 유출된 것이라는 피심인의 주장에 대한 판단

피심인은 '이 사건 유출정보' 중 임시ID( )[또는 임시ID( )와 회원일련번호( )가 연계되어 있다는 정보]만이 실제 유출된 것일 뿐, ① 해커가 무작위 대입한

휴대전화번호와 ② 카카오톡 이용자들이 서비스 이용 과정에서 열람할 수 있는 정보(프로필명, 오픈채팅방명, 오픈채팅방 닉네임), 그리고 통신 과정에서 접근이 제한될 수 없는 정보(회원일련번호, 임시ID)는 유출된 것이 아니라는 의견을 제출하였다.

그러나, 이 사건은 이용자의 추단되는 의사(해커의 불법적인 접근을 통한 채팅 정보의 취득 및 사용을 허락할 의사가 있다고 보기 어려움), 피심인의 서비스 제공 의도(일반채팅과 오픈채팅을 분리·운영함으로써 익명성을 보장), 이용자가 허용한 정보 공개 허용 범위(일반채팅과 오픈채팅 내에서 각각 공개 허용)와 이용자의 오픈채팅 익명성 보장기대에 반하여, 오픈채팅방의 익명성이 훼손됨과 동시에 피심인이 관리·통제권을 상실하여 해커가 '이 사건 유출정보'를 취득하고, 일부는 공개된 웹사이트( )에도 게시되어 제3자의 접근이 가능했던 사안으로, 휴대전화번호를 포함한 '이 사건 유출정보' 전체가 유출된 것에 해당한다.

① 먼저, 해커가 휴대전화번호를 무작위로 입력한 목적은 특정 오픈채팅 참여자들의 개인정보(회원일련번호, 프로필명, 휴대전화번호, 오픈채팅방명, 오픈채팅방 닉네임)를 취득하여 판매하기 위한 것이었다. 이때, 카카오톡 회원인 이용자가 입력된 휴대전화번호를 등록한 경우에 한하여 친구로 추가되었기 때문에, 해커는 무작위 휴대전화번호 입력을 통해서 피심인이 이용자의 개인정보로 처리 중인 '카카오톡 가입자 A'의 휴대전화번호라는 점을 비로소 확인할 수 있었으며, 더 나아가 '카카오톡 가입자 A'의 일반채팅 정보(회원일련번호와 프로필명), 그리고 오픈채팅 정보까지도 함께 취득함으로써, 오로지 피심인의 시스템을 통해서만 확보할 수 있는 오픈채팅방 참여자의 개인정보를 확보하게 되었다.

② 또한, 피심인이 주장하는 '서비스 이용 과정에서 열람할 수 있는 정보' 또는 '통신 과정에서 접근이 제한될 수 없는 정보'는 일반채팅과 오픈채팅 서비스 각각의 목적과 범위 내에서만 개별적으로 정보의 열람이 가능한 정보이다(회원일련번호와 임시ID는 정상적인 이용 환경에서는 열람할 수 없음). 특히, 카카오톡 이용자는 오픈채팅방의 익명성이 훼손되지 않고 일반채팅 정보(특히, 이용자의 실명, 휴대전화

번호 등)와 연계되지 않을 것이라고 기대하면서 서비스를 이용하였으며, 피심인도 일반채팅 정보와 오픈채팅 정보가 저장된 서버와 DB를 분리하여 운영하고, 메시지 송수신 시에도 일반채팅의 경우 회원일련번호( )를, 오픈채팅의 경우 임시ID( )를 사용하면서 오픈채팅의 익명성을 보장하기 위한 노력을 기울였다.

이처럼, 일반채팅과 오픈채팅 서비스를 이용하는 과정에서 열람할 수 있는 정보라고 하더라도, 이는 각 서비스의 목적과 범위 내에서만 개별적이고 제한적으로 이용되는 것을 의미하는 것이지, 일반채팅과 오픈채팅 서비스 양자가 연계된 정보집합을 통해 오픈채팅방 참여자의 개인정보가 열람되는 것을 허용하는 것이 아님은 분명하다. 그러나 이 사건 해커는 일반채팅과 오픈채팅 서비스 각각의 목적과 범위 내에서만 처리되어야 할 정보를 이용자와 피심인이 기대하는 처리 범위를 벗어나 연계함으로써 오픈채팅방 참여자의 개인정보를 취득하였다.

2. 개인정보 안전성 확보에 필요한 조치를 소홀히 한 행위

[舊 보호법 제29조(안전조치의무)]

가. 관련 법령

舊 보호법 제29조는 “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 규정하고 있다.

같은 법 시행령[41](이하 ‘舊 시행령’) 제48조의2제1항제2호는 개인정보에 대한 불법적인 접근을 차단하기 위해 ’그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치(마목)’ 등의 조치를 하여야 한다고 규정하고 있다.

舊 시행령 제48조의2제3항은 “제1항에 따른 안전성 확보 조치에 관한 세부 기준은

41) 대통령령 제32813호, 2022. 7. 19. 일부개정, 2022. 10. 20. 시행

보호위원회가 정하여 고시한다.”라고 규정하고 있다.

舊 시행령 제48조의2제3항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 舊 개인정보의 기술적·관리적 보호조치 기준[42](이하 ‘舊 기술적 보호조치 기준’) 제4조제5항은 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 ‘개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한(제1호)’, ‘개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지(제2호)’ 기능을 포함한 시스템을 설치·운영하여야 한다고 규정하고 있으며, 舊 기술적 보호조치 기준 해설서는 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 정책 설정 운영(신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리하는 것) 및 이상 행위 대응(모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응하는 것), 로그 분석(로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단하는 것) 등을 활용하여 체계적으로 운영·관리하여야 한다고 해설하고 있다.

또한, “IP 주소 등에는 IP 주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)를 포함한다”고 안내하고 있다.

한편, 舊 기술적 보호조치 기준 제4조제9항은 “정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.”라고 규정하고 있으며, 舊 기술적 보호조치 기준 해설서는 정보통신서비스 제공자 등이 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 및 보안기술을 마련

42) 개인정보보호위원회고시 제2021-3호, 2021. 9. 15. 시행

하고 운영 및 관리 측면에서의 개인정보 유·노출 방지조치를 하여야 하며, 인터넷 홈페이지 설계 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하여야 하고, 인터넷 홈페이지 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다고 해설하고 있다.

나. 접근 제한 및 유출 탐지 기능의 운영 소홀

1) 관련 판례

서울고등법원 2020. 11. 4. 선고 2019누43964 판결은 “침입차단·침입탐지시스템의 운영이란 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 통상적인 기능과 용법에 맞게 적정하게 활용하는 것을 말한다. 침입차단·침입탐지시스템은 사전에 정해진 정책 설정에 따라 차단·탐지 기능을 수행하므로, 이를 적정하게 활용하려면 상시적인 모니터링, 로그 분석 등을 통한 새로운 위험요소를 인지하고, 시스템에 침입차단 및 침입탐지 정책 재설정 등을 반영하여 개인정보에 대한 불법적 접근을 탐지·차단하여야 한다. 침입차단·탐지시스템의 적정한 운영에는 상시적인 모니터링, 웹 서버 접속 로그기록 등에 대한 로그 분석, 침입차단 및 침입탐지정책 설정 등 조치가 포함된다고 할 것이다.”고 전제하고, “이 사건 보호조치 기준 제4조 제5항이 정한 접속권한 제한 및 재분석 대상인 IP 주소 등에는 IP 주소, 포트에 한정되지 않고 웹 서버 접속 로그기록도 포함되고, 웹 서버 접속 로그기록을 실시간으로 분석하거나 사후적으로 분석하는 행위도 침입탐지차단시스템의 운영에 포함된다고 봄이 상당하다”고 판시한 바 있다(대법원 2021. 9. 30. 선고 2020두55220 판결로 상고 기각되어 확정).

2) 피심인의 접근 제한 및 유출 탐지 기능의 운영 소홀

피심인은 2010. 3. 18. 카카오톡 서비스를 개시한 시점부터, 이용자 일방이 휴대전화번호를 입력하여 계정당 최대 명의 친구를 등록한 다음, 이를 통해 친구의 프로필명(이름 등)과 프로필 사진, 휴대전화번호를 확인할 수 있는 시스템을 운영해

왔다. 한편, 2015. 8. 출시한 오픈채팅 서비스의 경우, 메시지 송·수신을 위한 식별 부호로 임시ID( )를 사용하면서 임시ID( ) 안에 일반채팅에서 사용되는 회원일련번호( )를 포함시켜 사실상 평문으로 운영하는 구조를 2023. 5. 3. 이전까지 유지하였다.

이 같은 상황에서는 공격자가 휴대전화번호 무작위 대입을 통해 친구추가 후 일반채팅 정보를 취득하고, 카카오톡 일반채팅과 오픈채팅을 연결하는 핵심 요소인 임시ID( )에서 회원일련번호( )를 추출하여 '이 사건 유출정보'를 취득함으로써 이용자와 피심인이 기대하는 오픈채팅의 익명성이 훼손될 위험성이 크다.

게다가, 피심인은 비인가 프로그램을 이용한 카카오톡 정보획득 방법, 악성행위 방법 등과 관련된 공개 게시글과 제보가 잇따르자 2020. 7.말 내부적으로 스팸 프로그램 제작이 우려된다는 내용의 내부 검토를 진행하고, 2020. 8. 5. 일부 임시ID( )를 암호화하는 조치를 실행하였으므로, 적어도 이 무렵에는 비인가 프로그램을 통한 이상행위와 이로 인한 회원일련번호( )의 유출, 더 나아가 오픈채팅 이용자의 개인정보가 유출될 위험성을 인지한 것으로 보인다.

그렇다면, 피심인은 2020. 8.에는, 비인가 프로그램을 이용한 이상행위에 대응할 수 있도록 상시적인 모니터링, 로그 분석 등을 통해 새로운 위험 요소를 인지하고, 불법적인 접근과 개인정보 유출 시도를 탐지·차단하는 정책에 반영하여 접근제한 및 유출탐지 기능이 충족되도록 시스템을 체계적으로 관리·운영하였어야 한다. 구체적인 방법으로는, 1) 안티 어뷰징 시스템 등에 신규 정책(비인가 프로그램으로 대규모의 친구를 단시간에 추가하거나 정보를 추출하는 행위 등)을 추가로 적용하는 것과, 2) 비인가 프로그램을 통해 단시간 내 과도한 API 호출, 비정상적인 형식의 요청 메시지 전송 등이 발생하는 경우 이용자 로그 분석을 통해 이상행위 또는 정보 유출 시도에 대한 탐지·차단을 실시하는 것, 3) 특히, 오픈채팅방 익명성 보장의 핵심 요소인 임시ID( ) 조회 관련 로그를 분석함으로써 소수의 계정에서 과도한 횟수의 입력을 시도하는 행위 등의 이상징후를 탐지하고 차단하는 것을 상정할 수 있다.

그러나 피심인은 2020. 8. 무렵부터 언론사의 취재요청을 받은 2023. 3. 10. 이전까지, 세 차례(2021. 5./2021. 10./2022. 2.)에 걸쳐 안티 어뷰징 시스템 내에 친구추가 횟수를 제한하는 정책을 보완[43]한 것 외에, 2020. 8. 무렵의 정책 변경 이력이나 그 밖의 구체적인 이상행위 탐지·차단 기준 및 정책 등을 제출하지 않았다.

피심인이 이상행위 탐지·차단 기준 및 정책 대신 2022년 이후의 이상행위에 대한 차단 이력을 제출하기는 하였으나, 이 사건과 직접적으로 관련되어 있다고 판단한 상세 이유를 기재한 이력은 총 14건(2022. 1. 26. 이후 7건, 2022. 2. 24. 이후 [44] 3건과 [45] 4건)에 불과하였다[46]. 또, 이 사건 조사 과정에서, 공개되어 있는 비인가 프로그램 로 일반 채팅 이용자 회원일련번호( )와 오픈채팅 이용자 임시ID( ) 등 정보를 추출하는 행위가 피심인의 안티 어뷰징 시스템을 통해 탐지·차단되지 않고 가능하다는 것도 확인되었다.

한편, 피심인이 2023. 3. 17. 제출한 자료에 따르면, 비인가 프로그램을 이용하여 카카오톡 일반채팅 또는 오픈채팅 메시지 내 특정 필드의 데이터 사이즈를 비정상적으로 큰 값으로 조작( )하여 메시지 전송 요청을 시도한 것이 비정상 요청 행위로 분석되었으나, 피심인이 2023. 2. 14.까지 해당 행위를 비인가 프로그램의 비정상 요청으로 간주하여 차단한 이력을 확인할 수 없었다.

---

43) (‘21. 5.) , (‘21.10.) , (’22.2.)

44) 등

45) 등

46) 이외에도, 피심인은 2021. 10. 비정상 클라이언트 대량 제재(건) 건수를 제출하면서, 해당 제제건수에는 , 봇 관련 비정상 클라이언트 등 다수의 제재 건수가 포함되어 있다고 주장하나 실제 이 사건과 직접적으로 연관되어 있다는 객관적인 증빙자료나 제재기준 등 객관적으로 입증할 수 있는 자료는 제출하지 않음

무엇보다도, 피심인이 2020. 8. 이후에 생성된 오픈채팅방에 한하여 임시ID( ) 암호화 정책을 적용하면서도, 오픈채팅 시`스템에 대한 비정상적인 접근 시도(임시ID에 대한 과도한 조회 등)를 분석하여 유사한 유출 시도를 탐지하거나 차단할 수 있는 정책은 반영하지 않았다. 그 결과, 유출 사실이 알려진 2023. 3. 10. 이전의 한달 동안에만 개의 계정에서 15만 6천여건의 임시ID( )가 조회되었음에도 이 같은 행위가 탐지·차단되지 않았다. 나아가 피심인은 그러한 이상행위를 탐지하기 위해 별도 로그 분석을 했다거나, 해당 룰의 적정성을 주기적으로 모니터링 및 재검토했다는 등의 자료도 제출하지 않았다.

한편, 피심인이 2023. 3. 11. 언론사의 취재 요청를 받은지 불과 하루만에 해커로 추정되는 19개 계정을 차단하는 제재조치를 시작한 점과, 한 달여가 지난 2023. 4월초, 안티 어뷰징 시스템에 비인가 프로그램 등을 이용하는 환경을 탐지·차단하는 정책을 적용한 점을 고려하여 보면, 피심인이 메시지 전송 요청 데이터와 임시ID( ) 등의 이용자 로그를 실시간 또는 사후적으로 분석하여 탐지·차단하거나 정책을 재설정하는 것이 곤란했다고 보기도 어렵다.

결국, 피심인은 비인가 프로그램을 이용한 이상행위에 대하여, 정책 설정 운영, 이상 행위 대응, 로그 분석 등을 활용하여 접근 제한 및 유출 탐지 기능이 포함된 시스템을 체계적으로 운영·관리하지 않고 소홀히 함으로써 舊 보호법 제29조, 같은 법 시행령 제48조의2제1항제2호, 舊 기술적 보호조치 기준 제4조제5항을 위반하였다.

다. 개인정보 유·노출 방지조치 소홀

피심인은 비인가 프로그램을 악용한 해커의 불법적인 접근에 적기 대응하기 위한 접근제한 및 이상행위에 대한 탐지·차단을 소홀히 하였으며, 개발자·이용자 등이 지속적으로 제기한 보안 취약점에 대한 조치도 즉각적으로 취하지 않은 위법성이 있다.

1) 관련 판례

舊 기술적 보호조치 기준 제4조제9항은 정보통신서비스 제공자등의 내·외부적인 요인 등으로 인하여 개인정보가 외부로 유출되는 사고를 방지하기 위한 목적에서 마련된 것으로, 舊 기술적 보호조치 기준 제4조제9항의 문언과 입법 목적, 규정 체계 등을 고려하면, 본 조항이 정보통신서비스 제공자등의 의무로 규정하고 있는 조치는 정보통신서비스 제공자등이 취급 중인 개인정보가 내·외부적 요인에 의하여 유출되지 않도록 개인정보처리시스템에 합리적으로 기대 가능한 정도의 기술적 보호조치라고 해석된다.

대법원도 舊 기술적 보호조치 기준 "제4조제9항에서 정보통신서비스 제공자 등의 의무로 규정하고 있는 조치는 정보통신서비스 제공자 등이 취급 중인 개인정보가 인터넷 홈페이지 등에 대한 해킹 등 침해사고에 의해 유출되지 않도록 개인정보처리시스템과 개인정보취급자의 컴퓨터에 취하여야 할 사회통념상 합리적으로 기대 가능한 정도의 기술적 보호조치'라고 해석할 수 있"다고 하면서 나아가 정보통신서비스 제공자등이 舊 기술적 보호조치 기준 제4조제9항에서 정한 보호조치를 다하였는지 여부는 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, 정보통신서비스 제공자의 업종·영업규모, 정보통신서비스 제공자등이 인터넷 홈페이지 등의 설계에 반영하여 개발에 적용한 보안대책·보안기술의 내용과 실제 개발된 인터넷 홈페이지 등을 운영·관리하면서 실시한 보안기술의 적정성 검증 및 그에 따른 개선 조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹에 의한 개인정보 유출의 경우 이에 실제 사용된 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, 정보통신서비스 제공자등이 수집한 개인정보의 내용과 개인정보의 유출로 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 판단하여야 한다고 판시한바 있다. (대법원 2021. 8. 19. 선고 2018두56404 판결 참조)

2) 피심인의 개인정보 유·노출 방지조치 소홀

개인정보처리자가 개인정보 보호법상 안전조치의무를 위반하여 해당 개인정보가 유출되는 경우, 정보주체의 개인정보 자기결정권에 심각한 위협을 줄 수 있으므로, 개인정보 보호법은 개인정보처리자에게 이용자의 개인정보가 유출되지 아니하도록 안전조치 등을 할 의무를 부여하고 있다. 이러한 전제에서, 이 사건에서의 안전조치 중 하나는 개인정보처리자인 피심인이 서비스를 설계·운영하는 과정에서 피심인의 의도대로, 그리고 이용자가 믿고 기대하는 대로[47] 서비스가 운영되는 것을 의미한다. 즉, 오픈채팅의 익명성 보장을 위하여 일반채팅 정보와 오픈채팅 정보를 안전하게 '구별하여' 처리하는 조치가 필요하며, 이는 '마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치'에 해당한다.

구체적으로 카카오가 취할 수 있었던 사회통념상 합리적으로 기대 가능한 보호조치로는, 오픈채팅의 익명성을 보장할 수 있도록 회원일련번호( )와 임시ID( )의 연계 로직을 개선하여 별도의 고유번호를 사용하는 등 근본적으로 연계성을 제거하거나, 이를 유지하고자 하는 경우에는 임시ID( )를 통해 회원일련번호( )를 알아낼 수 없도록 하는 보완조치[API를 통해 회원일련번호( )나 임시ID( )가 노출되지 않도록 조치하거나, 모든 임시ID( )를 암호화하는 등의 조치]를 상정할 수 있다.

그러나 피심인의 경우, 2015. 8. 오픈채팅 서비스 개시 당시부터 회원일련번호( )와 임시ID( ), 그리고 일반채팅과 오픈채팅 정보가 연계되는 시스템을 설계함으로써 오픈채팅방의 익명성이 훼손될 가능성이 있는 상황에서, 2020. 7.경에는 공개된 비인가 프로그램 등을 이용한 스팸 기계 제작 등 악영향이 우려된다는 점을 명확히 인지하였음에도, 2020. 8. 이후 신규 생성되는 오픈채팅방의 임시ID( )만 암호화하였을 뿐 문제점을 깊이 검토하고 보완조치를 통해 이를 개선하지 않았다[48].

47) 피심인이 '15.8.31. 발표한 보도자료(https://kakaocorp.com/page/detail/7813)에 따르면, 오픈채팅 서비스를 통해 개인정보 공개에 대한 불편함 없이 더 많은 사람과 쉽고 편하게 채팅할 수 있는 수단을 제공하고, 이는 이용자의 프라이버시를 강화하는 데 의미가 있다고 본다고 밝힘. 카카오는 최근까지도 오픈채팅 서비스가 "'내 프로필 정보를 제한적으로 노출할 수 있었으면 좋겠다' 등 이용자들의 니즈"를 바탕으로 하고 있다고 밝힘으로써 익명성이 보장되는 것처럼 홍보함(2024. 1. 9. 카카오 보도자료 https://www.kakaocorp.com/page/detail/10811)

또한, 피심인은 익명성 강화를 위해 2020. 8월부터 생성되는 오픈채팅방은 임시ID( )를 암호화하여 일반채팅 정보와 연계될 수 없도록 조치하였으나 2020. 8월 이전에 생성된 오픈채팅방은 2023. 5. 3. 이전까지 이 같은 조치를 하지 않고 방치하고 있었다. 뿐만 아니라, 암호화된 임시ID( )조차 오픈채팅방 게시판 내 파라미터 변조 취약점으로 인하여 여전히 회원일련번호( ) 추출, 일반채팅 정보와 오픈채팅 정보 연계가 가능한 상태로 유지되었다.

해커는 이러한 피심인 시스템의 취약점을 이용하여 임시ID( ) 암호화 여부와 상관없이 알아내고자 하는 특정 오픈채팅방 참여자의 '회원일련번호( ), 오픈채팅방명, 오픈채팅방 닉네임' 정보를 취득하고 이를 통해 '특정 오픈채팅방 참여자'의 개인정보 파일을 완성하고 판매할 수 있었다.

대법원 판례에 따른 사회통념상 합리적으로 기대 가능한 정도의 보호조치에 관한 판시내용을 적용해 보아도, 위와 같은 피심인의 대응은 ① '이 사건 유출정보'가 유출되었을 당시 보편적으로 알려져 있는 정보보안 기술의 수준에 미달하였고(임시ID를 통해 회원일련번호를 알아낼 수 있도록 서비스를 설계·구현한 상황에서, 비인가 프로그램으로 인한 보안 취약점이 제보된 2020. 8. 이후에도 오픈채팅방의 익명성을 보장하는 보완조치[49]를 하지 아니하고 파라미터 변조 등의 보안 취약점을 방치), ② 피심인은 정보통신서비스 제공자로 그 주요 상품이 6천만 명 이상의 국민이 이용하는 카카오톡 서비스이고 영업규모가 에 달하며, ③ 피심인이 보유한 인재풀과 사업규모를 고려할 때 회원일련번호( )와 임시ID( )의 연계성을 제거하거나, 임시ID( )를 통해 회원일련번호( )를 알아낼 수 없도록 하는 암호화 조치, 파라미터 변조 방지를 위한 입력값 검증이나 오픈채팅방 참여자 검증 절차 추가 등의 조치는 구현을 위한 경제적 비용이 적은 반면 효용은 높으며, ④ 피심인이 비인가 프로그램에 대한 이용자들의 제보를 충실히 검토하고 피심인이 보유하고 있는 시스템 설계·구현 기술을 적절히 이용하는 것만으로도 피해 발생을

48) 2021. 8.경에는 관련 토론방 내 게시글에서 회원일련번호( )와 임시ID( ) 연결 로직이 존재하고, 연결 로직에 오픈채팅방 ID( ) 연관 가능성이 직접 언급되었을 정도로 문제점이 구체적으로 공개된 상황이었음

49) API를 통해 회원일련번호( ), 임시ID( )가 노출되지 않도록 조치하거나 모든 임시ID( )를 암호화하는 등의 조치

막을 수 있었고, ⑤ 카카오톡 서비스 이용자 규모와 유출에 따른 사회적 파장을 종합적으로 고려했을 때, 사고 당시 사회통념상 합리적으로 기대가능한 대응조치가 충분히 이루어졌다고 볼 수 없다고 할 것이다.

게다가, 피심인이 2020. 8. 이미 일부 임시ID( )에 대해 암호화를 적용한 점과, 2023. 3. 10. 언론 취재요청을 받은 당일에 파라미터 변조 취약점을 즉시 개선한 점, 2023. 5. 3. 앱 업데이트로 모든 임시ID( )를 암호화한 점에 비추어 보면, 피심인이 이 같은 조치를 하는 것이 특별히 곤란하였다고 보기도 어렵다.

이처럼 피심인이 임시ID( )를 통해 회원일련번호( )를 추출할 수 있도록 서비스를 설계·구현한 상황에서, 비인가 프로그램으로 인한 보안 취약점이 제보된 2020. 8. 이후에도 오픈채팅방의 익명성을 보장하는 보완조치를 하지 아니하고 파라미터 변조 등의 보안 취약점을 방치하는 등 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 소홀히 하였는바, 이는 舊 보호법 제29조, 같은 법 시행령 제48조의2제1항, 舊 기술적 보호조치 기준 제4조제9항을 위반[50]한 것이다.

3. 개인정보 유출 통지를 소홀히 한 행위

[舊 보호법 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항)]

가. 관련 법령

舊 보호법 제39조의4제1항은 정보통신서비스 제공자등이 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 유출등이 된 개인정보 항목(제1호), 유출등이 발생한 시점(제2호), 이용자가 취할 수 있는 조치(제3호), 정보통신서비스 제공자등의 대응 조치(제4호), 이용자가 상담 등을 접수할 수 있는 부서 및 연락처(제5호)를 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24

50) 피심인은 여타 SNS도 비교적 쉽게 이름, 전화번호 등이 확인될 수 있다고 주장하나, 피심인처럼 일반적인 커뮤니케이션과 익명 기반의 커뮤니케이션을 함께 제공하는 사례는 찾아보기 힘들었다. 특히, 피심인은 익명성을 오픈채팅 서비스의 특징으로 홍보하면서도 각각의 이용자 정보가 연계될 수 있도록 서비스를 설계·운영하며 보안 취약점에 대한 주의를 충분히 기울이지 않은 사실이 있다.

시간을 경과하여 통지·신고해서는 아니 된다고 규정하면서, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다고 규정하고 있다.

舊 시행령 제48조의4제2항은 “정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면 등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.”라고 규정하고 있으며, 제3항은 “정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.”라고 규정하고 있다.

나. 위법성 판단

피심인이 2023. 3. 10. 언론보도 및 개인정보위 조사 과정에서 카카오톡 오픈채팅방 이용자의 개인정보가 유출되고 있다는 사실을 인지했음에도 개인정보 유출 신고 및 이용자 대상 유출 통지를 하지 않은 행위는 舊 보호법 제39조의4제1항을 위반한 것이다.

< 피심인의 위반사항 >

위반행위	법률	舊 시행령	세부내용(고시 등)
안전조치의무	舊 보호법 §29	§48의2① 제2호	• 불법적인 접근 및 침해사고 방지를 위한 개인정보 처리 시스템에 대한 침입 탐지·차단 시스템 운영 소홀 (舊 기술적 보호조치 기준 §4⑤) • 열람 권한이 없는 자에게 공개되거나 유출되지 않도록 필요한 조치를 취하지 않은 행위 (舊 기술적 보호조치 기준§4⑨)
개인정보 유출등의 통지·신고에 대한 특례	舊 보호법 §39의4①	§48조의4	• 정당한 사유 없이 유출 사실을 안 때부터 24시간 이내에 개인정보 유출 신고·통지를 하지 않은 행위

Ⅳ. 처분 및 결정

1. 과징금 부과

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11제1항과 제4항, [별표 1의5] '과징금의 산정기준과 산정절차' 및 舊 개인정보보호 법규 위반에 대한 과징금 부과기준[51] (이하 '舊 과징금 부과기준')에 따라 다음과 같이 부과한다.

가. 과징금 상한액

피심인의 舊 보호법 제29조 위반에 대한 과징금 상한액은 같은 법 제39조의15, 舊 시행령 제48조의11에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의 · 중과실 여부

舊 과징금 부과기준 제5조제1항은, 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 舊 시행령 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 따라, 舊 보호법 제29조(안전조치의무), 舊 시행령 제48조의2(개인정보의 안전성 확보 조치에 관한 특례)를 소홀히 한 피심인에게 이용자 개인정보 유출에 대한 중과실이 있다고 판단한다.

51) 개인정보보호위원회고시 제2022-3호, 2022. 10. 20. 시행

2) 중대성의 판단

舊 과징금 부과기준 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있다. 다만, 舊 과징금 부과기준 제5조제3항 단서에서 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 해당하는 경우 '보통 위반행위'로, 1개 이상 2개 이하에 해당하는 경우 '중대한 위반행위'로 감경하도록 규정하고 있다.

피심인의 경우, 해킹으로 인해 개인정보가 유출되었으므로 위반행위로 인해 직접적 이득을 취하지 않았다고 볼 수도 있으나, 유출된 이용자의 개인정보 파일이 웹사이트(　　)에 공개되어 다운로드가 가능하였으므로 '이용자의 개인정보가 공중에 노출(제3호)'되었고 실제로 불법적으로 판매되는 등 2차 피해도 발생하여 '중대한 위반행위'로 판단한다.

3) 기준금액 산출

舊 과징금 부과기준 제4조제1항은 "관련 매출액은 위반 정보통신서비스 제공자등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다."라고 규정하고 있다.

피심인의 위반행위로 인하여 영향을 받는 서비스에는 카카오톡 일반채팅·오픈채팅 서비스와 함께 회원일련번호(　　)로 연동되어 있는 서비스가 포함되고, 그 중 매출액이 존재하는 선물하기, 쇼핑하기, 라이브쇼핑, 프렌즈, 주문하기, 이모티콘, 톡서랍 등 7개에서 발생한 수수료/상품 매출, 광고 등 매출액을 위반행위 관련

매출액으로 하며, 직전 3개 사업년도의 연평균 매출액 천 원에 舊 시행령 [별표 1의5] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 천 원으로 한다.

< 피심인의 위반행위 관련 매출액 >

(단위 : 천원)

구 분	2020년	2021년	2022년	평 균
관련 매출액*				

* 사업자가 제출한 재무제표 등 회계자료를 토대로 작성

<舊 시행령 [별표 1의5] 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

舊 과징금 부과기준 제6조와 제7조에 따라 피심인 위반행위의 기간이 2년을 초과하므로(2020. 8. ~ 2023. 5.) '장기 위반행위'에 해당하여 기준금액의 100분의 50에 해당하는 금액인 천 원을 가중하고,

최근 3년 이내 舊 보호법 제39조의15제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액의 100분의 50에 해당하는 금액인 천 원을 감경한다.

라. 추가적 가중 및 감경

舊 과징금 부과기준 제8조는 사업자의 위반행위의 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 가중·감경할 수 있다고 규정하고 있다.

이에 따를 때, 피심인이 ▲위반 정보통신서비스 제공자등이 개인정보 보호를 위해 개인정보보호위원회가 인정하는 인증을 받은 경우, ▲조사에 적극 협력한 점, ▲기타 제1호 내지 제3호의 사항에 준하는 사유가 있는 경우 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 40에 해당하는 천 원을 감경한다.

마. 과징금의 결정

피심인의 舊 보호법 제29조(안전조치의무) 위반행위에 대한 과징금은 같은 법 제39조의15제1항제5호, 舊 시행령 제48조의11, [별표 1의5] 2. 가. 2)(과징금의 산정기준과 산정절차) 및 舊 과징금 부과기준에 따라 위와 같이 단계별로 산출한 금액인 천 원을 최종 과징금으로 결정한다.

<과징금 산출 내역>

①기준금액	②필수적 가중·감경	③추가적 가중·감경	④최종과징금
• 직전 3개 사업연도 연평균 매출액 (천 원) • 연평균 매출액에 2.1% 적용(중대한 위반*)	• 장기 위반으로 50% 가중 (천 원) • 최초위반으로 50% 감경 (천 원)	• 개인정보 보호 인증, 조사협력 등으로 40% 감경 (천 원)	**천 원**
⇒ 천 원	⇒ 천 원	⇒ 천 원	

* 중대한 위반 : 고의·중과실이 있는 경우, 매우 중대한 위반행위로 판단하나, ▲위반행위로 직접적으로 이득을 취득하지 않은 경우에 해당하여 '중대한 위반행위'로 판단함

2. 과태료 부과

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보의 유출등의 통지·신고에 대한 특례)제1항 위반행위에 대한 과태료는 같은 법 제75조제2항제6호·제12호의3, 舊 시행령 제63조, 舊 시행령 [별표2] '과태료의 부과기준' 및 舊 개인정보 보호법 위반에 대한 과태료 부과기준[52](이하 '舊 과태료 부과기준')에 따라 다음과 같이 과태료를 부과한다.

가. 기준금액

舊 시행령 제63조의 [별표2]는 최근 3년간 같은 위반행위를 한 경우 위반 횟수에 따라 기준금액을 규정하고 있고, 피심인은 최근 3년간 같은 위반행위로 과태료 처분을 받은 사실이 없으므로 각 위반행위별 기준금액을 600만원으로 산정한다.

< 舊 시행령 [별표2] 2. 개별기준 >

위 반 사 항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 **제29조**를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
도. 법 **제39조의4제1항**(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항제12호의3	600	1,200	2,400

나. 과태료의 가중 및 감경

1) (과태료의 가중) 舊 과태료 부과기준 제8조는 사전통지 및 의견제출 결과와 당사자의 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표2]의

52) 개인정보보호위원회지침, 2023. 3. 8. 시행

가중기준(▲조사방해, ▲위반의 정도, ▲위반기간, ▲기타 위반행위의 정도와 동기, 사업규모, 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 가중할 수 있다고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제8조 및 [별표2] 과태료의 가중기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우'에 해당하여 기준금액의 10%를 가중하고, 같은 법 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례)제1항 위반행위는 '법 위반상태의 기간이 3개월 이상인 경우', '제3호 위반행위별 각 목의 세부기준에서 정한 행위가 2개에 해당하는 경우'에 해당하여 기준금액의 20%를 가중한다.

2) (과태료의 감경) 舊 과태료 부과기준 제7조는 사전통지 및 의견제출 결과와 당사자의 위반행위 정도, 위반행위의 동기와 그 결과 등을 고려하여 [별표1]의 감경기준(▲당사자 환경, ▲위반정도, ▲조사협조 및 자진시정 등, ▲개인정보보호 노력정도, ▲사업규모, ▲기타 위반행위의 정도와 동기, 사업 규모, 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우)에 따라 기준금액의 100분의 50의 범위 이내에서 감경할 수 있다고 규정하고 있다.

피심인의 경우, 舊 과태료 부과기준 제7조 및 [별표1] 과태료의 감경기준에 따라 舊 보호법 제29조(안전조치의무) 위반행위는 '과태료의 사전통지 및 의견제출 기간이 종료되기 이전에 위반행위를 중지하는 등 시정을 완료한 경우', '조사에 적극 협력한 경우', '위반행위자가 보호법 제32조의2에 따른 개인정보보호 인증(ISMS-P)을 받은 경우'에 해당하여 기준금액의 50%를 감경하고, 같은 법 제39조의4(개인정보 유출 등의 통지·신고에 대한 특례)제1항 위반행위는 '조사에 적극 협력한 경우', '위반행위자가 보호법 제32조의2에 따른 개인정보보호 인증(ISMS-P)을 받은 경우'에 해당하여 기준금액의 50%를 감경한다.

다. 최종 과태료

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대해 기준금액에서 가중·감경을 거쳐 총 780만 원의 과태료를 부과한다.

< 과태료 산출내역 >

위반행위(세부내용)	기준금액	가중액	감경액	최종 과태료
안전조치의무 (접근통제)	600만원	60만원	300만원	**360만원**
개인정보 유출등의 통지·신고에 대한 특례	600만원	120만원	300만원	**420만원**
계				**780만원**

3. 시정조치 명령

피심인에 대하여 舊 보호법 제64조제1항에 따라 다음과 같이 시정조치를 명한다.

가. 이용자 대상 개인정보 유출 통지를 실시할 것

나. 피심인은 가.의 시정명령에 따른 시정조치를 이행하고, 시정조치 명령 처분 통지를 받은 날로부터 90일 이내에 이행 결과를 개인정보보호위원회에 제출할 것

4. 결과 공표

舊 보호법 제66조제1항 및 「舊 개인정보보호위원회 처분 결과 공표기준」(2020. 11. 18. 개인정보보호위원회 의결) 제2조(공표요건)에 따라, '법 제75조제2항 각 호에 해당하는 위반행위를 2개 이상 한 경우(제4호)', '피심인의 위반행위는 위반상태가 6개월 이상 지속된 경우(제5호)'에 해당하므로, 피심인이 시정조치 명령을 받은 사실과 과태료 부과에 대해 개인정보보호위원회 홈페이지에 공표한다. 다만, 개정된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침」(2023. 10. 11. 시행)에 따라 공표 기간은 1년으로 한다.

※ 질서위반행위규제법에 근거하여 피심인에게 유리하게 변경된 「개인정보 보호법 위반에 대한 공표 및 공표명령 지침(2023.10.11. 시행)」에 따라 공표기간 1년을 소급 적용

개인정보 보호법 위반 행정처분 결과 공표

개인정보 보호법 위반에 따라 행정처분한 내용 및 결과를 아래와 같이 공표합니다.

순번	위반행위를 한 자	위반행위의 내용		행정처분의 내용 및 결과	
	명칭	위반조항	위반내용	처분일자	처분내용
1		舊 보호법* 제29조	안전조치의무	2024. 5. 22.	과태료 부과 360만원
		舊 보호법* 제39조의4 제1항	개인정보 유출등의 통지·신고에 대한 특례	2024. 5. 22.	시정조치 명령 과태료 부과 420만원

* 舊 보호법 : 2020. 8. 5. 시행, 법률 제16930호

2024년 5월 22일

개 인 정 보 보 호 위 원 회

Ⅴ. 결론

피심인의 舊 보호법 제29조(안전조치의무), 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)제1항을 위반한 행위에 대하여 같은 법 제64조(시정조치 등)제1항, 제39조의15(과징금의 부과 등에 대한 특례)제1항제5호, 제75조(과태료)제2항제6호·제12호의3, 제66조(결과의 공표)제1항에 따라 시정조치 명령, 과징금·과태료 부과 및 결과 공표를 주문과 같이 의결한다.

이의제기 방법 및 기간

피심인은 이 과징금 부과처분, 시정조치 명령, 공표에 불복이 있는 경우, 「행정심판법」 제27조 및 「행정소송법」 제20조의 규정에 따라 처분을 받은 날부터 90일 이내에 행정심판을 청구하거나 행정소송을 제기할 수 있다.

피심인은 이 과태료 부과처분에 불복이 있는 경우, 「질서위반행위규제법」 제20조의 규정에 따라 처분을 받은 날로부터 60일 이내에 개인정보보호위원회에 서면으로 이의를 제기할 수 있다.

과태료 부과처분에 대한 피심인의 이의제기가 있는 경우, 개인정보보호위원회의 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.

이상과 같은 이유로 주문과 같이 의결한다.

2024년 5월 22일

위 원 장　　고 학 수　(서 명)

부위원장　　최 장 혁　(서 명)

위　　원　　김 진 욱　(서 명)

위　　원　　김 진 환　(서 명)

위　　원　　박 상 희　(서 명)

위　　원　　윤 영 미　(서 명)

위　　원　　이 문 한　(서 명)

위　　원　　조 소 영　(서 명)