과징금부과처분취소

[서울고등법원 2018. 8. 24. 2016누64533]

【전문】

【원고 피항소인】 주식회사 케이티(소송대리인 변호사 최재혁 외 3인)

【피고 항소인】 방송통신위원회(소송대리인 법무법인 민후 담당변호사 김경환 외 2인)

【제1심판결】 서울행정법원 2016. 8. 18. 선고 2014구합15108 판결

【변론종결】2018. 6. 8.

【주문】

】

1. 피고의 항소를 기각한다.

2. 항소비용은 피고가 부담한다.

【청구취지 및 항소취지】1. 청구취지 피고가 2014. 6. 26. 원고에 대하여 한 '과징금 7,000만 원 부과'처분을 취소한다.2. 항소취지 제1심판결을 취소한다. 원고의 청구를 기각한다.

【청구취지 및 항소취지】1. 청구취지 피고가 2014. 6. 26. 원고에 대하여 한 '과징금 7,000만 원 부과'처분을 취소한다.2. 항소취지 제1심판결을 취소한다. 원고의 청구를 기각한다.

【청구취지 및 항소취지】1. 청구취지 피고가 2014. 6. 26. 원고에 대하여 한 '과징금 7,000만 원 부과'처분을 취소한다.2. 항소취지 제1심판결을 취소한다. 원고의 청구를 기각한다.

【청구취지 및 항소취지】1. 청구취지 피고가 2014. 6. 26. 원고에 대하여 한 '과징금 7,000만 원 부과'처분을 취소한다.2. 항소취지 제1심판결을 취소한다. 원고의 청구를 기각한다.

【이유】

】1. 처분의 경위

가. 원고의 지위 등

원고는 전기통신사업법상의 전기통신사업자이자 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률(2014. 5. 28. 법률 제12681호로 개정되기 전의 것, 이하 '구 정보통신망법'이라 한다)이 정한 정보통신서비스 제공자이다.

원고가 개설한 ○○○○ 홈페이지(홈페이지 생략)는 일반 가입자(고객)가 요금명세서를 조회할 수 있는 홈페이지이고, ○○클럽 홈페이지는 원고의 상담사 또는 일반 가입자가 고객 포인트 조회 등을 할 수 있는 홈페이지이다.

나. 해킹사고의 발생

소외인(해커)은 2013. 8. 8.부터 2014. 2. 25.까지 ○○○○ 홈페이지를 통하여 불법적으로 접근하여 타인의 요금명세서를 조회하는 방식으로 합계 11,708,875건(이용자 수 기준 9,818,074명)의 개인정보를 유출하였다.

또 다른 해커는 ○○클럽 홈페이지의 DB 서버에 합계 약 2,753회 접속하여 합계 83,246건의 개인정보를 유출하였다(이하 모두 합하여 '이 사건 해킹사고'라고 한다).

다.

이 사건 해킹사고의 발생 경위

1) ○○○○ 홈페이지 부분

이 사건 해킹사고에 대한 민관합동조사단 등의 조사결과에 의하면 해커는 다음과 같은 방법과 경로로 개인정보를 유출해간 것으로 추정되었다.

가) 해커는 자신의 PC에 파로스 프로그램을 설치・실행한 후 ○○○○ 홈페이지에 접속하여 로그인 버튼을 누르고 자신의 인증 정보(ID, 비밀번호)를 입력하였다.

나) ○○○○ 홈페이지의 웹 서버는 사용자 인증 정보를 통합인증 서버로 전송하고, 통합인증 서버는 해커가 웹 사이트 가입 회원이고 비밀번호가 일치하는지를 판별한다.

일치할 경우 웹 서버는 해커가 회원 자격으로 로그온 되었다는 정보를 사용자 PC에 전달한다.

이때 해커의 서비스계약번호가 쿠키 내에 저장된다.

다) 해커가 웹 브라우저에 표시된 메뉴 중 '요금명세서 보기'를 선택하면 웹 브라우저는 해커의 요금명세서 표시 화면을 웹 서버에 요청한다.

누구의 정보를 요청하는지는 '서비스계약번호'에 의해 결정되는데, 이 단계에서는 서비스계약번호 항목이 해커의 서비스계약번호로 채워져 있다.

해커는 웹 브라우저의 요청 메시지가 웹 서버에 전송되기 전에 자신의 PC에 있는 파로스 프로그램을 이용해서 전송을 멈춘다.

해커는 파로스 프로그램을 통해 웹 브라우저의 요청 메시지 중 해커의 서비스계약번호로 되어 있는 '서비스계약번호 항목'을 임의의 9자리 숫자로 변경한 후 '전송' 버튼을 누르면 '바뀐 서비스계약번호'에 대한 요금 조회 메시지가 웹 서버로 전송된다.

웹 서버는 해당 작업 요청을 웹 애플리케이션 서버에 넘긴다.

라) ○○○○ 홈페이지의 웹 애플리케이션 서버는 '바뀐 서비스계약번호'의 요금정보 데이터를 ESB 서버에 요청하고 ESB 서버는 DB 서버에 API 형태로 요금정보 데이터를 요청한다.

DB 서버는 데이터베이스 조회 명령을 통해 '바뀐 서비스계약번호'의 요금정보 데이터를 추출하여 이를 ESB 서버로 전달하고, ESB 서버는 웹 애플리케이션 서버로, 웹 애플리케이션 서버는 이를 사용자 PC로 송신한다.

사용자 PC는 수신한 정보를 이용해 웹 브라우저 화면에 '바뀐 서비스계약번호'에 해당하는 요금명세서 페이지를 표시한다.

마) 해커는 '바뀐 서비스계약번호'에 해당하는 사용자의 요금정보와 웹 서버가 웹 브라우저에 송신해 준 '고객의 이름, 주민등록번호, 주소, 서비스가입정보' 등(이는 웹 브라우저 화면에는 표시되지 않는다)을 파로스 프로그램을 통해 수집한다.

해커는 서비스계약번호 항목에 해당하는 임의의 9자리 숫자를 계속 변경하는 자동화된 컴퓨터 프로그램을 이용하여 위 과정을 반복하였다.

2) ○○클럽 홈페이지 부분

가) DB 서버에 정상적으로 접속하는 경로는 다음과 같다.

(1) ○○클럽은 원고의 휴대전화 대리점 내에 위치한 PC에서 상담사가 고객과 가입 상담을 하며 고객의 ○○클럽 포인트를 조회하거나, 원고의 휴대전화 서비스 가입자가 자신의 ○○클럽 포인트를 조회하는 데 사용할 수 있다.

원고의 상담사가 ○○클럽 포인트를 조회하기 위해서는 N-STEP 시스템을 통하여야 한다.

N-STEP 시스템은 원고의 상담사 또는 대리점이 PC에서 실행하는 N-STEP UI '클라이언트 구성'과 원고의 데이터센터에서 실행하는 '서버 구성'으로 나눌 수 있다.

대리점에는 VPN 장치가 설치되어 있고 이것은 원고의 데이터센터 내 VPN 서버와 연결하여 터널을 구성하도록 미리 설정되어 있다.

(2) 원고의 상담사는 N-STEP 시스템에 유효한 ID와 그에 대응하는 비밀번호를 입력하여야 하고, MAC 주소도 N-STEP 포털 서버로 전송된다.

N-STEP 포털 서버는 이를 AUT 서버로 전달하고, AUT 서버는 접속을 시도하려는 사용자 계정이 정상적으로 접속이 허용된 사용자인지 여부를 확인하여 접속이 허용된 사용자일 경우 인증토큰을 N-STEP 포털 애플리케이션 서버로 전달한다.

(3) N-STEP 포털 애플리케이션 서버가 대리점 PC에 설치된 웹 브라우저에 인증토큰을 보내면 웹 브라우저는 N-STEP UI 프로그램을 실행하고, 인증토큰을 N-STEP UI로 전달받는다.

N-STEP UI는 자신이 가진 인증토큰을 AUT 서버에 전송하고, AUT 서버가 정상적으로 발급된 인증토큰이라고 확인해 주면 N-STEP 프로그램을 사용할 수 있다.

(4) 상담사가 N-STEP UI 프로그램 중 '○○클럽 포인트 조회' 메뉴를 선택하면 N-STEP UI 프로그램은 그 상담사의 ID, 요청 작업이 내려진 애플리케이션 이름 등의 정보를 암호화하고 이들 정보를 조합하여 인터넷 접속 주소인 URL을 즉석에서 생성한다.

해당 URL 접속 요청을 데이터센터 쪽으로 전송하나 이 요청을 처리할 ○○클럽 웹 서버는 공중망인 인터넷에 접하여 있으므로 라우터를 통해 외부로 보내진다.

(5) ○○클럽 웹 서버는 URL을 해석(parsing)하여 가입자 정보를 조회할 수 있는 화면을 보내준다.

상담사는 N-STEP UI 프로그램 내 팝업으로 표시된 창에서 '전화번호, 고객명 등'을 기준으로 가입자를 검색하여 해당 가입자의 ○○클럽 포인트와 더불어 휴대전화 모델명, 요금제, 가입일 등을 조회할 수 있는 화면을 보게 된다.

(6) 상담사는 전화번호 등 원하는 기준을 선택하고 검색어를 입력한 뒤 '검색' 버튼을 누르면 N-STEP UI 프로그램은 검색 명령을 ○○클럽 웹 서버에 전달하고 이는 ○○클럽 웹 애플리케이션 서버로 전달된다.

○○클럽 웹 애플리케이션 서버는 ○○클럽 DB 서버로 검색 요청을 보내고, ○○클럽 DB 서버는 검색을 하여 그 결과를 웹 애플리케이션 서버로 응답한다.

최종적으로 대리점 내 상담사 PC는 ○○클럽 웹 애플리케이션 서버로부터 검색 결과를 전달받아 원하는 가입자에 대한 ○○클럽 포인트를 알 수 있다.

나) 이 사건 해킹사고에 대한 조사결과 등에 의하면 해커는 다음과 같은 방법과 경로로 개인정보를 유출해간 것으로 추측되었다.

(1) 해커는 상담사가 사용하는 PC에 불상의 방법으로 접근하여 네트워크 모니터링 도구를 설치하였다.

해커가 설치한 네트워크 모니터링 도구가 실행된 상태에서 상담사는 N-STEP 포털에 접속한다.

(2) 상담사는 정상적인 N-STEP 사용자 계정으로 로그온한 후 N-STEP UI 프로그램의 메뉴를 이용하여 일상적인 휴대전화 고객 처리 업무를 진행한다.

해커는 네트워크 모니터링 도구에 기록된 내용을 통해 N-STEP 프로그램 내에서 '고객의 별 포인트 조회' 기능을 선택하는 경우 사용되는 인터넷 주소(URL)를 획득한다.

(3) 해커는 대리점 내 상담사의 PC가 아닌 일반 공중망 인터넷에 위치한 PC에서 위 URL로 접속한다.

해커는 '고객의 별 포인트 조회' 화면에서 정상적인 상담사와 마찬가지로 '전화번호로 검색하기'를 선택하고 검색어란에 임의의 전화번호를 입력한 뒤 '검색' 버튼을 누른다.

○○클럽 웹 서버 및 웹 애플리케이션 서버는 상기 조회를 처리하기 위해 ○○클럽 DB 서버에 질의하고, ○○클럽 DB 서버는 검색된 결과를 웹 애플리케이션 서버로 응답하며 웹 애플리케이션 서버는 해커의 PC로 검색 결과를 회신한다.

라. 피고의 과징금 부과처분

피고는 2014. 6. 26. 이 사건 해킹사고와 관련하여 원고가 구 정보통신망법 제28조 제1항 제2호, 같은 법 시행령(2014. 11. 28. 대통령령 제25789호로 개정되기 전의 것, 이하 '구 정보통신망법 시행령'이라 한다) 제15조, 구 개인정보의 기술적·관리적 보호조치 기준(2015. 5. 19. 방송통신위원회고시 제2015-3호로 개정되기 전의 것, 이하 '이 사건 고시'라고 한다) 제4조 제2항, 제5항, 제9항을 위반하였다고 보아, 구 정보통신망법 제64조의3 제1항 제6호에 따라 과징금 7,000만 원을 부과하는 처분을 하였다(이하 '이 사건 처분'이라 한다). 그 구체적인 처분 사유는 다음과 같다.

홈페이지위반 사항비고○○○○이용자가 홈페이지 접속 후 요금명세서 조회시 접속한 이용자와 고객서비스계약번호(9자리)의 본인 일치 여부 인증 없이 홈페이지를 운영하였으며, 해커는 이용자 본인 일치 여부 인증이 없는 취약점을 이용하여 타인의 개인정보(이름 등)까지 조회함(이 사건 고시 제4조 제5항, 제9항 위반)제1 처분사유특정 IP에서 1일 최대 34만 1,279건의 개인정보를 조회하였음에도 비정상적인 접근을 탐지 및 차단하지 못함(이 사건 고시 제4조 제5항 위반)제2 처분사유○○클럽인가받은 개인정보취급자만이 사내망에서 접근할 수 있는 고객포인트 조회 웹페이지에 해커가 외부 인터넷망 IP로 접속하였음에도 비정상적인 접근을 탐지 및 차단하지 못함(이 사건 고시 제4조 제5항 위반)제3 처분사유사용 중지된 퇴직자 ID로 8만 건의 개인정보를 조회하였음에도 인가받지 않은 이용자

의 접근을 제한하지 못함(이 사건 고시 제4조 제2항, 제9항 위반)제4 처분사유

[인정근거] 다툼 없는 사실, 갑 제1, 14, 15, 45 내지 47, 55호증, 을 제1호증의 각 기재 또는 영상, 변론 전체의 취지

2. 이 사건 처분의 적법 여부

가. 관련 법령 및 이 사건 고시의 해설서(을 제7호증)

별지 기재와 같다.

나. 관련 법리

1) 침익적 행정처분의 근거가 되는 행정법규는 엄격하게 해석·적용하여야 하고 행정처분의 상대방에게 불리한 방향으로 지나치게 확장해석하거나 유추해석하여서는 안 되며, 그 입법 취지와 목적 등을 고려한 목적론적 해석이 전적으로 배제되는 것은 아니라 하더라도 그 해석이 문언의 통상적인 의미를 벗어나서는 안 될 것이다(대법원 2008. 2. 28. 선고 2007두13791 판결 등 참조).

2) 정보통신서비스가 '개방성'을 특징으로 하는 인터넷을 통하여 이루어지고 정보통신서비스 제공자가 구축한 네트워크나 시스템 및 운영체제 등은 불가피하게 내재적인 취약점을 내포하고 있어서 이른바 '해커' 등의 불법적인 침입행위에 노출될 수밖에 없고, 완벽한 보안을 갖춘다는 것도 기술의 발전 속도나 사회 전체적인 거래비용 등을 고려할 때 기대하기 쉽지 아니한 점, 해커 등은 여러 공격 기법을 통해 정보통신서비스 제공자가 취하고 있는 보안조치를 우회하거나 무력화하는 방법으로 정보통신서비스제공자의 정보통신망 및 이와 관련된 정보시스템에 침입하고, 해커의 침입 행위를 방지하기 위한 보안기술은 해커의 새로운 공격 방법에 대하여 사후적으로 대응하여 이를 보완하는 방식으로 이루어지는 것이 일반적인 점 등의 특수한 사정이 있다.

그러므로 정보통신서비스제공자가 구 정보통신망법 제28조 제1항이나 정보통신서비스이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단함에 있어서는, ① 해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준, ② 정보통신서비스 제공자의 업종·영업규모와 정보통신서비스 제공자가 취하고 있던 전체적인 보안조치의 내용, ③ 정보보안에 필요한 경제적 비용 및 효용의 정도, ④ 해킹 기술의 수준과 정보보안기술의 발전 정도에 따른 피해 발생의 회피 가능성, ⑤ 정보통신서비스 제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여, 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다(대법원 2015. 2. 12. 선고 2013다43994 판결 등 참조).

다.

판단

1) 개인정보처리시스템의 범위

이 사건 처분의 적법 여부를 살펴보기 위해서는 개인정보처리시스템의 개념을 어떻게 해석할 것인지에 대한 판단이 선행되어야 한다.

개인정보처리시스템의 범위를 어디까지 볼 것인지에 따라 이 사건 처분의 근거 규정인 이 사건 고시 제4조 제2항, 제5항, 제9항의 적용 여부 및 규율대상, 원고에게 요구되는 기술적·관리적 보호조치의 내용 및 이행 여부에 대한 판단이 달라지기 때문이다.

가) 당사자의 주장 요지

(1) 원고

개인정보처리시스템은 데이터베이스관리시스템(DBMS)으로 한정해서 보아야 하고, 웹 서버는 포함되지 않는다.

(2) 피고

개인정보처리시스템에는 개인정보 데이터베이스(DB)와 연동되어 개인정보를 처리하도록 구성되어 있는 웹 서버도 포함된다.

나) 웹 서버 포함 여부

을 제7 내지 9호증의 각 기재 및 변론 전체의 취지를 통하여 알 수 있는 다음의 사정을 종합하면, 개인정보처리시스템은 기본적으로 소위 '내부 영역'에 있는 데이터베이스관리시스템을 의미하고, 웹 서버나 웹 페이지는 이에 포함되지 않는다고 보는 것이 타당하다.

(1) 개인정보처리시스템이라는 용어는 구 정보통신망법 시행령에 처음 등장하는데, 그 시행령 제15조 제2항 제1호는 개인정보처리시스템을 '개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템'이라고 정의하고 있다.

이 사건 고시 제2조 제4호 또한 동일한 내용으로 정의하고 있다.

여기에 개인정보처리시스템이라는 용어가 사용된 다른 규정, 즉 그 시행령 제15조 제3항, 제5항, 이 사건 고시 제4조 제1항의 내용까지 고려하면 개인정보처리시스템은 기본적으로 DB 서버를 의미한다고 보아야 통일적인 해석이 가능하다.

(2) 피고가 2012. 9. 발간한 이 사건 고시 해설서(을 제7호증)는 "개인정보처리시스템은 법 시행령 제15조 제2항 제1호에 따라 개인정보를 보관·처리하기 위한 시스템이다.

일반적으로 체계적인 데이터 처리를 위해 DBMS를 사용하고 있으나, 이용자의 개인정보 보관·처리를 위해 파일처리시스템 등을 구성한 경우 개인정보처리시스템에 포함시키는 것이 타당하다.

"라고 설명하고 있을 뿐, DB 서버와 연동된 시스템이나 웹 서버 등을 포함하고 있지 않다.

(3) 한편 행정자치부에서 발간한 '개인정보의 안정성 확보조치 기준 해설서'(을 제8호증, 이하 '행정자치부 고시 해설서'라 한다)에서 개인정보처리시스템에 대해 "DB(데이터베이스) 자체뿐 아니라, DB에 연결되어 DB를 관리하거나 DB의 개인정보를 처리할 수 있는 응용프로그램(예: 웹 서버)까지 포함된다.

"라고 설명하고 있기는 하다.

그러나 이는 '개인정보 보호법'의 위임을 받아 제정된 행정자치부 고시에 대한 해설서일 뿐이고, 이 사건 해킹사고 후인 2015. 2.경에 각종 해킹사고의 원인을 분석하고 대응방안을 마련하는 차원에서 위와 같은 내용을 포함시킨 것으로 보인다.

또한 정보통신망법 시행령과 이 사건 고시와 달리 개인정보 보호법의 경우 법률은 물론 같은 법 시행령 및 시행규칙에서도 개인정보처리시스템에 대한 정의 규정을 두고 있지 않다.

이 사건 처분의 근거 법령인 정보통신망법 시행령과 이 사건 고시, 그 해설서에 명문의 정의 규정이 있음에도 직접적 연관이 없는 다른 고시에 대한 해설서를 참조하여 개인정보처리시스템의 범위를 문언의 통상적 의미를 넘어서까지 넓게 해석할 수는 없다.

(4) 또한 피고가 2013. 2. 발간한 '정보통신서비스 제공자 등을 위한 외부 인터넷망 차단조치 안내서(을 제9호증)'에 "'개인정보처리시스템'이란 개인정보를 이용한 데이터 처리를 위해 체계적으로 구성한 데이터베이스관리시스템(DBMS)을 말하고 개인정보 DB에 접근하기 위한 중계 서버, 애플리케이션 등도 포함시키는 것이 타당하다."라고 되어 있기는 하다.

그러나 '중계 서버, 애플리케이션 등'에 당연히 웹 서버가 포함된다고 단정할 수 없을 뿐만 아니라, 정보통신망법 시행령과 이 사건 고시 규정의 문언을 넘어 그와 같이 확장해석할 수는 없다.

(5) 웹 서버는 개인정보를 저장하거나 직접 처리하는 역할을 하는 것이 아니라 DB 서버와 이용자 사이의 중간 전달 매체에 불과하다.

그러므로 웹 서버는 '내부 영역'에 존재하는 DB 서버나 다른 시스템들에 비해 DB 자체와의 연계성에 근본적인 차이가 있고, 수많은 일반 이용자들의 접속이 상시적으로 이루어지는 특성상 기술적·관리적 보호조치 관점에서도 달리 평가할 필요성이 있다.

(6) 설령 개인정보 안정성 확보라는 목적 달성을 위해 개인정보 처리 과정에서 데이터베이스와 연계되는 일정한 범위의 웹 서버에 대해서는 보호조치를 취해야 할 필요성이 있다고 하더라도 그에 대해 규율하고 있는 법령이 미비한 상태라면 이는 입법을 통해 해결해야 할 문제라고 보는 것이 타당하다.

2) 제1 처분사유에 관하여

가) 당사자의 주장 요지

(1) 원고

(가) 원고는 침입차단 및 침입탐지 기능을 갖춘 시스템을 설치하고 제대로 운영함으로써 이 사건 고시 제4조 제5항을 준수하였다.

파라미터 변조는 잘 알려진 해킹 방법이긴 하나 방지하기가 쉽지 않으므로, 파라미터 변조를 방지하지 못했다고 하여 이 사건 고시 제4조 제5항을 위반하였다고 볼 수 없다.

(나) 개인정보처리시스템에 웹 서버는 포함되지 않고, 이 사건 고시 제4조 제9항은 일반 이용자의 보편적 접근을 통하여 개인정보가 유출되지 않도록 조치를 취하라는 규정이므로 제1 처분사유와 관련하여 이 사건 고시 제4조 제9항은 적용될 수 없다.

적용된다고 하더라도 이 사건 고시 제4조 제9항의 '조치를 취하여야 한다'의 의미는 필요하고 합리적인 조치를 취하여 취약점을 최소화하라는 것이고, 원고는 그런 조치를 취함으로써 이 사건 고시 제4조 제9항을 준수하였다.

(2) 피고

(가) 이 사건 고시 제4조 제5항의 '시스템 운영'에는 '웹 서버 접속 로그 기록' 등을 재분석하여 불법적인 정보 유출시도를 탐지하는 것이 포함된다.

파라미터 변조는 잘 알려진 취약점으로 웹 서버 접속 로그 분석을 통하여 '불법적인 개인정보 유출시도'를 탐지할 수 있었음에도 원고는 그러하지 아니하였다.

(나) 개인정보처리시스템에는 웹 서버도 포함되고, 이 사건 고시 제4조 제9항은 인터넷 홈페이지를 통한 개인정보 유출을 방지하기 위한 규정으로 해커가 접근하는 경우도 전제하고 있으므로 제1 처분사유와 관련하여 이 사건 고시 제4조 제9항이 적용된다.

원고는 인터넷 홈페이지에서 발생할 수 있는 웹 취약점인 '파라미터 변조'를 최소화하기 위한 충분한 조치를 취하지 않았으므로 이 사건 고시 제4조 제9항을 위반하였다.

나) 이 사건 고시 제4조 제5항 위반 여부

(1) 이 사건 고시 제4조 제5항 '시스템 설치'의 의미

앞서 본 관련 법리와 갑 제30호증, 을 제7호증의 각 기재 및 변론 전체의 취지를 통하여 알 수 있는 다음의 사정을 종합하면, 이 사건 고시 제4조 제5항의 '시스템 설치'는 침입차단 및 침입탐지 기능을 갖춘 상용화되고 인증된 설비를 설치하는 것으로 족하다고 보는 것이 타당하다.

(가) 구 정보통신망법 시행령 제15조 제2항 제2호는 "정보통신망법 제28조 제1항 제2호에 따라 정보통신서비스 제공자 등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 개인정보처리시스템에 대한 '침입차단시스템' 및 '침입탐지시스템'을 설치·운영하여야 한다.

"라는 취지로 규정하고 있다.

그에 따라 이 사건 고시 제4조 제5항은 그 '침입차단시스템 및 침입탐지시스템'의 내용을 구체화하고 있다.

(나) 이 사건 고시 해설서(을 제7호증)는 그 시스템에 관하여 다음과 같이 설명하고 있다.

▶ 침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법 - 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치·운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS: Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.

※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(service.nis.go.kr)에서 확인할 수 있다.

(다) 이 사건 고시 제4조 제5항에서 규정한 '시스템'이란 통상 보안업계에서 칭하는 침입차단시스템과 침입탐지시스템을 말하는 것으로 볼 수 있다.

(2) 이 사건 고시 제4조 제5항 '시스템 운영'의 의미

앞서 본 관련 법리와 앞서 든 증거들 및 제1심 증인 소외 3의 일부 증언에 변론 전체의 취지를 더하여 알 수 있는 다음의 사정을 종합하면, 이 사건 고시 제4조 제5항의 '시스템 운영'이란 위에서 본 '침입차단 및 침입탐지 기능을 갖춘 설비'를 그 통상적인 기능과 용법에 맞게 제대로 운영하는 것을 말하고, 여기에 웹 서버 접속 로그 기록을 실시간으로 분석하거나 사후에 상시적으로 분석하는 것이 포함된다고 볼 수 없다.

(가) 이 사건 고시 해설서는 이 사건 고시 제4조 제5항의 '시스템 운영'의 예로 '침입차단 정책 설정 및 침입탐지 로그 분석, 로그 훼손 방지'를 들고 있다.

여기에서 '침입탐지 로그 분석'은 기본적인 보안 장비인 침입탐지시스템(IDS)과 침입방지시스템(IPS)을 상정한 로그 분석의 의미라고 볼 수 있다.

(나) 이 사건 고시 제4조 제5항의 '개인정보처리시스템'에 웹 서버 등이 포함된다고 볼 수 없고, 'IP 등'은 침입차단시스템 및 침입탐지시스템에서 차단 및 탐지하는 IP(Internet Protocol) 주소, 포트(port)를 의미하므로 여기에 '웹 서버 접속 로그 기록 등'이 포함된다고 볼 수 없다.

그러므로 이 사건 고시 제4조 제5항의 '시스템 운영'에 웹 서버 접속 로그 기록 분석까지 포함된다고 보기는 어렵다.

(다) 을 제8호증의 기재에 의하면, 행정자치부 고시 해설서에서는 이 사건 고시 제4조 제5항과 문언이 거의 동일한 행정자치부 고시 개인정보의 안전성 확보조치 기준 제5조 제1항에 대하여 "불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비 설치와 더불어 적절한 침입차단 및 침입탐지 정책 설정, 로그 분석 및 이상행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요하다.

"라고 설명하고 있기는 하다.

그러나 앞서 본 바와 같이 위 해설서는 이 사건 처분의 근거 법령이 아닌 행정자치부 고시에 관한 것이고 이 사건 해킹사고 후인 2015. 2.경에 각종 해킹사고의 원인을 분석하고 대응방안을 마련하는 차원에서 위와 같은 내용을 포함시킨 것으로 보이므로, 이 사건 해킹사고 시점을 기준으로 이 사건 고시를 해석하는 데 직접 영향을 미친다고 볼 수 없다.

(라) 이 사건 고시 제4조 제5항은 해킹 등 침해사고를 방지·차단하기 위한 조치를 취할 의무를 부과하는 규정임은 분명하지만, 소위 '이상행위'라는 개념은 모호하고 추상적이어서 해킹으로 인한 정보 유출의 '모든 경우'가 이상행위에 해당하고 이 사건 고시 제4조 제5항의 규율 범위에 들어간다고 볼 수는 없다.

(3) 이 사건 고시 제4조 제5항 위반 여부

앞서 인정하였거나 갑 제2, 4, 12 내지 14, 16 내지 20, 26, 30, 31, 40, 44, 60, 84, 85호증(가지번호 있는 것은 각 가지번호 포함, 이하 같다)의 각 기재나 영상, 제1심 증인 소외 2, 소외 3의 각 일부 증언, 변론 전체의 취지를 통하여 알 수 있는 다음의 사정을 종합하면, 피고가 주장하는 사정이나 제출한 증거들만으로는 원고가 제1 처분사유와 관련하여 이 사건 고시 제4조 제5항을 위반하였다고 보기 어렵다.

(가) 이 사건 고시 제4조 제5항이 사전 혹은 사후에 상시적으로 웹 서버 접속 로그 기록을 분석할 의무를 부과하는 것이라고 볼 수 없음은 앞서 본 바와 같다.

특히 ○○○○ 홈페이지와 같이 방대한 규모의 시스템에서 모든 로그를 실시간 또는 상시적으로 분석하도록 하는 것은 상당한 시간이 소요되고 기술적으로도 한계가 있어 합리적으로 기대 가능한 보호조치의 범위 내에 있다고 보기는 어렵다.

(나) 원고는 침입차단과 침입탐지 기능이 동시에 구현된 침입방지시스템(IPS)인 Sniper IPS V7.0.e를, 침입탐지 기능을 수행하는 방화벽을, 웹쉘 공격을 방어하기 위한 웹쉘 탐지시스템 등을 설치・운영하였고, IPS의 침입차단 정책을 설정하였으며 침입탐지 로그를 분석하고 로그 훼손을 방지하였다.

또한 자동화된 점검 도구를 도입하였고 상시적으로 모의 해킹을 수행하였다.

따라서 원고는 이 사건 고시 제4조 제5항에서 요구하는 침입차단 또는 침입탐지 기능을 갖춘 시스템을 설치하여 그 용법에 따라 적절히 운영하였던 것으로 보인다.

(다) 파라미터 변조는 웹 브라우저 단계에서 웹 서버 간에 전달하는 파라미터 값을 임의로 변경함으로써 정상적인 경우의 통신 결과와 달라지는 결과를 기도하는 방식이다.

파라미터 변조는 취약점이 널리 알려진 해킹 수법이기는 하나, 수많은 웹 서버마다 각기 다른 파라미터가 존재하고 파라미터에 할당할 수 있는 값도 달라질 수 있기 때문에 점검 대상이 무수히 많고, 파라미터 변조가 동일한 방식으로 이루어지거나 항상 일정한 형태로 고정되어 있는 것이 아니어서 이를 사전에 탐지하여 차단하기가 쉽지 않다.

또한 파라미터 변조 수법은 정상적으로 로그인해서 자신의 요금정보를 조회할 때와 비교하면 시스템 입장에서는 서비스계약번호라는 숫자만 다른 숫자 값으로 달라졌기 때문에 이미 장착해놓은 '침입행위 패턴들'과는 달라 정상적인 이용자의 행동과 구별하기 어렵다.

(라) 또한 원고는 IPS에 파로스 프로그램을 사용한 홈페이지 접근이 있는 경우 이를 탐지하는 정책을 포함하여 운영하였으나 해커가 이를 우회하는 수단을 사용하여 개인정보를 유출한 것으로 보이는바, 이 사건 고시 제4조 제5항이 모든 침입을 탐지할 것을 강제하는 규정이 아닌 이상 파라미터 변조를 탐지하지 못하였다는 결과만으로 원고에게 합리적으로 기대 가능한 보호조치를 취하지 않았다고 그 책임을 묻기는 어렵다.

(마) 원고가 ○○○○ 홈페이지에 접속한 이용자와 서비스계약번호 대상자가 일치하는지 여부를 확인하는 2차 '인증' 통제를 하지는 아니하였다.

그러나 서비스계약번호는 원고 시스템 내부에서 검색을 하기 위한 기준값일 뿐 인증 수단이 아니었으므로, ○○○○ 홈페이지에 접속한 이용자와 서비스계약번호 대상자가 일치하는지를 확인하는 단계가 없었다고 하여 곧바로 이 사건 고시 제4조 제5항을 위반하였다고 볼 수 없다.

다) 이 사건 고시 제4조 제9항 위반 여부

(1) 이 사건 고시 제4조 제9항의 규율 범위

(가) 을 제7호증의 기재에 따르면 이 사건 고시 해설서는 이 사건 제4조 제9항에 관하여 다음과 같이 설명하고 있다.

▶ 개인정보취급자의 부주의로 고객 개인정보가 인터넷 홈페이지 또는 P2P를 통해 게시되거나 공유 설정된 PC 폴더에 고객명단 파일을 둠으로써 열람 권한이 없는 자에게 공개되는 사례가 많이 발견되고 있다.

▶ 과실로 인한 인터넷 홈페이지에서 노출 방지 - 인터넷 홈페이지 운영자 또는 자료게시 담당 직원의 실수로 게시판 등에 고객 주민등록번호 등이 포함된 파일을 게시하는 사례가 있다.

▶ 인터넷 홈페이지 취약점으로 인한 노출 방지 - 인터넷 홈페이지 개발시 보안기준을 따르지 않아 발생하는 취약점으로 인해 구글 등의 검색엔진을 통해 개인정보 DB가 노출되는 사례도 발생하므로 수시로 인터넷 홈페이지 취약

점을 점검하여 조치하도록 한다.

(나) 이 사건 고시 제4조 제5항에서 별도로 불법적인 접근 및 침해사고 방지를 위한 목적의 접근통제 조치에 대해 규정하고 있는 점과 제4조 제9항의 문언 및 그에 관한 해설서의 내용 등을 종합하면, 위 규정은 기본적으로 정보통신서비스 제공자측의 내부적 요인'(즉 개인정보취급자의 부주의, 인터넷 홈페이지 운영자나 자료 게시 담당 직원의 과실, 인터넷 홈페이지 개발 시 간과하여 발생한 취약점 등)으로 개인정보가 유출되지 않도록 조치를 취하라는 것이고, 나아가 '파라미터 변조'와 같은 해킹을 통한 개인정보 누출 방지를 직접적으로 규율하는 것으로 보기는 어렵다.

(2) 이 사건 고시 제4조 제9항 위반 여부

위에서 본 이 사건 고시 제4조 제9항의 규율 범위에다 앞서 인정하였거나 갑 제2, 12, 13, 20, 26, 30, 31, 33 내지 42, 48, 56호증의 각 기재, 제1심 증인 소외 2, 소외 3의 각 일부 증언, 제1심법원의 롯데정보통신 주식회사에 대한 사실조회 회신결과, 변론 전체의 취지를 통하여 알 수 있는 다음의 사정 등을 종합하면, 피고가 주장하는 사정이나 제출한 증거들만으로는 원고가 제1 처분사유와 관련하여 이 사건 고시 제4조 제9항을 위반하였다고 보기 어렵다.

(가) '개인정보처리시스템'에 웹 서버나 웹 페이지가 포함된다고 볼 수 없음은 앞서 본 바와 같다.

원고가 운영하는 ○○○○ 홈페이지는 개인정보처리시스템이라고 볼 수 없으므로, 원고가 ○○○○ 홈페이지에 이용자와 서비스계약번호 대상자가 일치하는지 여부에 관한 인증 통제를 하지 않았다 하더라도 이 사건 고시 제4조 제9항을 위반하였다고 볼 수 없다.

(나) 아래에서 보는 바와 같이 원고는 웹 취약점을 점검하고 이를 최소화하는 조치를 취하였다.

① 수많은 웹 서버마다 각기 다른 다수의 파라미터가 존재하고 파라미터에 할당할 수 있는 값도 달라질 수 있기 때문에 파라미터 변조를 사전에 방지하기는 어렵다.

파라미터 변조라는 취약점을 사전에 발견하기 위한 방법으로는 수동 검사와 자동화된 스캐닝툴이 있다.

수동 검사는 보안 전문가가 자신의 경험과 지식을 이용하여 소스코드를 한 줄 한 줄 점검하는 형태로서, 가장 효과적인 방법이나 큰 비용과 시간을 소모하며 오류를 발견하지 못하고 넘어갈 위험이 있다.

또한 자동화된 스캐닝툴은 인터넷 홈페이지에 상당히 많은 파라미터가 존재하는 데다 웹 서비스 환경에서 웹 애플리케이션 소스코드 변경이 발생할 때마다 대규모 웹 서비스에 대해서 취약점을 전체적으로 매번 진단해야 하는 점 등으로 인하여 파라미터 변조 취약점을 모두 탐지하는 데 한계가 있다.

또한 대규모 웹 서비스를 운영 중인 상황에서는 자동화된 스캐닝툴로 파라미터 전체를 분석할 경우 DB 훼손, 서비스 장애 등 치명적인 문제가 발생할 가능성이 존재한다.

② 원고는 2006. 10. 25. IBM Security AppScan을, 2006. 10. 1. HP Fortify Static Code Analyzer라는 자동화된 점검 도구를 도입하였다.

IBM Security AppScan과 HP Fortify Static Code Analyzer는 OWASP 10대 취약점을 검출할 수 있는 기능을 갖추고 있다.

그리고 원고는 IBM Security AppScan과 HP Fortify Static Code Analyzer를 원고의 보안점검관리 포털(Security Management Portal, SMP)에 연동시킴으로써, ○○○○ 홈페이지 등 원고 운영 웹사이트 개발자들이 소프트웨어 소스코드를 작성 및 수정(유지・보수)하는 단계에서부터 위와 같은 자동화된 점검 도구를 활용하여 취약점의 존재를 최소화하도록 하였다.

또한 원고는 2012. 5.경부터 보안점검관리 포털(SMP)을 이용하여 자신이 작성한 소스코드에 취약점이 있는지 여부를 자가 진단할 수 있는 환경을 구축하고 이에 대한 전사적인 교육 및 점검을 수행하였다.

③ 원고는 2012. 11.경 계열 기업인 'KT DS'로 하여금, 2013. 7.경 롯데정보통신 소속 보안 전문가로 하여금 ○○○○ 홈페이지의 시스템을 대상으로 모의해킹을 수행하도록 하였다.

롯데정보통신은 웹 취약점에 관해서도 모의해킹을 수행하였다.

또한 국가정보원 IT보안인증사무국이 인증한 침입방지시스템(IPS)을 설치・운영하였다.

3) 제2 처분사유에 관하여

가) 당사자의 주장 요지

(1) 원고

원고는 침입차단 및 침입탐지 기능을 갖춘 시스템을 설치하고 제대로 운영함으로써 이 사건 고시 제4조 제5항을 준수하였다.

해커의 요금명세서 대량 조회행위는 원고의 입장에서는 이상행위로 보기 어려웠고, 과다 조회에 대한 탐지 의무가 있다고 볼 수 없으므로 이 사건 고시 제4조 제5항을 위반하였다고 볼 수 없다.

(2) 피고

동일 IP 주소에서 요금명세서를 대량으로 조회하는 행위는 이상행위에 해당하고, '로그 기록 분석'을 통해 이러한 불법적인 개인정보 유출시도를 탐지할 수 있음에도 원고는 이를 탐지하지 못하였다.

비정상적인 대량 조회에 대해 원고가 아무런 탐지정책도 설정하지 않고 방치한 것은 침입차단 및 침입탐지 기능을 갖춘 시스템을 적절히 운영한 것이라고 볼 수 없다.

나) 이 사건 고시 제4조 제5항 위반 여부

(1) 이 사건 고시 제4조 제5항의 '시스템 설치'는 침입차단 및 침입탐지 기능을 갖춘 상용화되고 인증된 설비를 설치하는 것으로 족하고, '시스템 운영'이란 침입차단 및 침입탐지 기능을 갖춘 설비를 그 통상적인 기능과 용법에 맞게 제대로 운영하는 것을 의미한다는 것은 앞에서 본 것과 같다.

(2) 앞서 인정하였거나 갑 제2, 4, 5, 13, 14, 16 내지 20, 30, 31, 84, 85, 87, 90호증, 을 제5호증의 각 기재나 영상, 제1심 증인 소외 2, 소외 3의 각 일부 증언, 변론 전체의 취지를 통하여 알 수 있는 다음의 사정을 종합하면, 피고가 주장하는 사정이나 제출한 증거들만으로는 원고가 제2 처분사유와 관련하여 이 사건 고시 제4조 제5항을 위반하였다고 보기 어렵다.

(가) 이 사건 고시 제4조 제5항이 사전 혹은 사후에 상시적으로 웹 서버 접속 로그 기록을 분석할 의무를 부과하는 것이라고 볼 수 없음을 앞서 본 바와 같다[이와 달리 설령 이 사건 고시 제4조 제5항이 '대량 조회를 탐지할 의무'를 부과하는 것이라고 본다고 하더라도, ○○○○ 홈페이지 시스템과 같이 방대한 규모의 모든 로그(특히 웹 서버 접속

로그 기록)를 실시간으로 분석하거나 상시적으로 사후 분석하는 것은 합리적으로 기대 가능한 보호조치의 범위 내에 있다고 보기 어려운 점이 참작되어야 한다].

(나) 원고는 침입차단과 침입탐지 기능이 동시에 구현된 침입방지시스템(IPS)인 Sniper IPS V7.0.e를, 침입탐지 기능을 수행하는 방화벽을, 웹쉘 공격을 방어하기 위한 웹쉘탐지시스템 등을 설치・운영하였고, IPS의 침입차단 정책을 설정하였으며 침입탐지 로그를 분석하고 로그 훼손을 방지하였다.

또한 자동화된 점검 도구를 도입하였고 상시적으로 모의 해킹을 수행하였다.

따라서 원고는 이 사건 고시 제4조 제5항에서 요구하는 침입차단 또는 침입탐지 기능을 갖춘 시스템을 설치하여 그 용법에 따라 적절히 운영한 것으로 보인다.

(다) 을 제6호증의 기재에 의하면 해커가 ○○○○ 홈페이지에 1일 최대 34만 번 접속한 사실을 인정할 수 있기는 하다. 그러나 ○○○○ 홈페이지에 대한 1일 접속 건수가 약 3,300만 건에 이르는 점에 비추어 보면 해커의 접속은 정상 접속의 1% 미만에 불과하고, 2012. 11. 30.부터 2014. 2. 25.까지를 기준으로 ○○○○ 홈페이지에 1일 10만 건 이상 접속한 IP의 개수도 중복 IP를 제외하고도 43개에 이른다.

(라) 또한 원고가 설치한 침입방지시스템(IPS, Sniper IPS V7.0.e)은 하나의 IP 주소에서 접속 요청이 대량으로 발생하거나 다수의 IP 주소에서 동일한 형태의 접속 요청이 대량으로 발생하는 경우 이를 이른바 '서비스 거부 공격(Dos)'이나 '분산형 서비스 거부 공격(DDos)'으로 판단하도록 하고 있었는데, 이는 원고의 침입차단 정책상 초당 4,000회 이상 접속할 경우여서 초당 기준으로 환산하면 초당 약 3.94회였던 이 사건의 경우는 탐지할 수 없었다.

그러나 불특정 다수가 접속하는 인터넷 홈페이지에 대해 IP 단위로 대량 조회를 탐지하여 차단하는 방식은 오류 발생 비율이 높고, 일반적으로 활용도가 떨어지는 것으로 보이는 점, 원고도 IPS를 통해 과다 로그인에 대해서는 침입차단 정책을 설정하고 있었던 점 등을 고려하면 정상적인 로그인 이후 대량 조회행위를 탐지하지 못하였다고 하여 이 사건 고시 제4조 제5항을 준수하지 않았다고 볼 수는 없다.

4) 제3 처분사유에 관하여

가) 당사자의 주장 요지

(1) 원고

○○클럽 사이트는 애초에 외부에서의 접속도 허용된 사이트였고, 따라서 사내망에서의 접근만 허용됨을 전제로 외부 IP 주소를 차단할 이유가 없었다.

피고가 이 사건 소송 중에 주장한 (웹페이지 주소 생략) 웹페이지에 대한 접속권한을 IP 주소 등으로 제한하는 기능을 운영하지 않아 해커가 외부 IP로 접속하였음에도 비정상적인 접근을 탐지 및 차단하지 못하였다는 처분사유는 기본적 사실관계가 상이한 처분사유의 추가・변경에 해당한다.

원고는 침입차단 및 침입탐지 기능을 갖춘 시스템을 설치하고 제대로 운영하여 이 사건 고시 제4조 제5항을 준수하였다.

(2) 피고

원고는 인가받은 개인정보취급자만 사내망에서 접근할 수 있는 웹페이지에 해커가 외부 인터넷망 IP로 접속하였음에도 이에 대한 비정상적인 접근을 탐지 및 차단하지 못하였다.

피고가 기존의 웹페이지 주소를 (웹페이지 주소 2 생략)에서 그 하위페이지인 (웹페이지 주소 생략)으로 특정한 것은 처분사유를 구체화한 것에 불과하여 처분사유의 변경에 해당하지 않는다.

원고가 포트별 IP 차단 기능을 운용하지 아니하여 비인가자의 외부 IP를 통한 접근을 허용한 것은 침입차단시스템을 적절히 운영한 것으로 볼 수 없어 이 사건 고시 제4조 제5항을 위반한 것이다.

나) 처분사유 변경 여부

(1) 행정처분의 취소를 구하는 항고소송에 있어서는 처분청은 당초 처분의 근거로 삼은 사유와 기본적 사실관계가 동일성이 있다고 인정되는 한도 내에서는 다른 사유를 추가하거나 변경할 수도 있으나 기본적 사실관계가 동일하다는 것은 처분사유를 법률적으로 평가하기 이전의 구체적인 사실에 착안하여 그 기초인 사회적 사실관계가 기본적인 점에서 동일한 것을 말하며, 처분청이 처분 당시에 적시한 구체적 사실을 변경하지 아니하는 범위 내에서 단지 그 처분의 근거법령만을 추가·변경하거나 당초의 처분사유를 구체적으로 표시하는 것에 불과한 경우에는 새로운 처분사유를 추가하거나 변경하는 것이라고 볼 수 없다(대법원 2007. 2. 8. 선고 2006두4899 판결, 대법원 2011. 7. 28. 선고 2011두3166 판결 등 참조).

(2) 피고가 당초 이 사건 처분을 하면서 인가받은 개인정보취급자만이 사내망에서 접근할 수 있는 웹페이지에 해커가 외부 인터넷망 IP로 접속하였음에도 비정상적인 접근을 탐지 및 차단하지 못한 사실을 처분사유로 하였음은 앞서 본 바와 같다.

한편 갑 제53호증의 기재에 의하면 이 사건 해킹사고 당시 (웹페이지 주소 3 생략) 주소를 사용하는 서버의 웹페이지로 최상단 페이지인 (웹페이지 주소 2 생략), 그 하위페이지인 상담사용 페이지 (웹페이지 주소 생략)과 일반 가입자용 페이지(웹페이지 주소 2 생략)/(웹페이지 주소 4 생략)이 있었고, 각 웹페이지는 모두 100번 포트를 통해 웹 연결이 제공되었던 사실이 인정된다.

(3) 위 관련 법리와 인정사실에 비추어 살피건대, 피고가 당초 이 사건 처분의 근거로 삼은 사유와 이 사건 소송 계속 중에 주장한 사유 즉, 개인정보취급자 전용 고객포인트 조회 웹페이지 (웹페이지 주소 생략)에 해커가 외부 인터넷망으로 접속하는 것을 차단하지 못했다는 사유를 비교하여 보면 인가받은 개인정보취급자만이 사내망을 통해 접근할 수 있는 웹페이지에 외부 인터넷망으로 접속하였음에도 비정상적인 접근을 탐지 및 차단하지 못하였다는 내용을 공통으로 하고 있을 뿐만 아니라 기존의 웹페이지 주소를 보다 자세히 특정하여 당초의 처분사유를 구체적으로 표시한 것에 불과하여 이를 처분사유의 변경에 해당한다고 할 수 없다.

설령 처분사유를 변경한 것이라고 보더라도 이는 당초의 처분사유와 기본적 사실관계의 동일성이 인정되는 경우라고 봄이 타당하다.

다) 이 사건 고시 제4조 제5항 위반 여부

(1) 이 사건 고시 제4조 제5항의 '시스템 설치'는 침입차단 및 침입탐지 기능을 갖춘 상용화되고 인증된 설비를 설치하는 것으로 족하고, '시스템 운영'이란 침입차단 및 침입탐지 기능을 갖춘 설비를 그 통상적인 기능과 용법에 맞게 제대로 운영하는 것을 의미한다는 것은 앞에서 본 것과 같다.

(2) 앞서 인정하였거나 갑 제61, 62호증의 각 기재 및 변론 전체의 취지를 통하여 알 수 있는 다음의 사정, 즉 ① 원고는 상담사가 고객포인트 조회 웹페이지에 접속하는 경우 N-STEP 시스템을 통해 상담사의 ID와 비밀번호를 입력하고 해당 PC의 MAC 주소를 비교하여 인증토큰이 발행되는 등의 다중 인증 과정을 거치도록 하여 비정상적인 접근을

통제하기 위한 충분한 조치를 마련하고 있었던 점, ② 원고는 침입차단과 침입탐지 기능이 동시에 구현된 침입방지시스템(IPS)인 Sniper IPS V7.0.e와 침입탐지 기능을 수행하는 방화벽, 웹쉘 공격을 방어하기 위한 웹쉘탐지시스템 등을 설치하고 운영하였던 점, ③ 또한 이 사건 고시 제4조 제5항의 해석상 하나의 서버에서 2개의 도메인을 운영하는 경우 당연히 포트를 달리 설정해야 할 의무가 도출된다고 보기 어렵고, 원고가 설정하여 운영한 IPS의 침입차단 정책이 이 사건 고시 제4조 제5항이 요구하는 수준을 하회하는 것으로 보이지는 않는 점 등을 종합하면 원고가 침입차단 및 침입탐지 기능을 갖춘 시스템을 부적절하게 운영하였다고 볼 수 없다.

따라서 피고가 주장하는 사정이나 제출한 증거들만으로는 원고가 제3 처분사유와 관련하여 이 사건 고시 제4조 제5항을 위반하였다고 보기 어렵다.

5) 제4 처분사유에 관하여

가) 당사자의 주장 요지

(1) 원고

(가) ○○클럽 웹 서버는 개인정보처리시스템에 해당하지 않으므로 제4 처분사유와 관련하여 이 사건 고시 제4조 제2항과 제4조 제9항은 적용될 수 없다.

(나) 이 사건 고시 제4조 제2항이 적용된다고 하더라도 개인정보에의 접근은 식별・인증・인가의 순서로 행해지는데, 식별과 인증이 불가능하도록 사용자 계정을 말소하면 접근권한도 말소되는 것이다.

원고는 계정관리시스템 및 N-STEP 인증 서버의 데이터베이스상 퇴직자(소외 6)의 사용자 계정(ID)을 말소함으로써 이 사건 고시 제4조 제2항에서 규정하고 있는 퇴직자의 접근권한 말소의무를 다하였다.

해커가 불상의 방법으로 취득한 URL 주소 중 퇴직자 ID의 변환 값은 greeting message로 사용되었을 뿐 본인과 일치하는지 여부를 확인하기 위한 인증 수단으로 사용된 것이 아니므로 접근권한 말소 여부와 이 사건 해킹사고 발생 사이에는 인과관계가 없다.

(다) 이 사건 고시 제4조 제9항은 일반 이용자의 보편적 접근을 통하여 개인정보가 유출되지 않도록 조치를 취하라는 것이므로 이 사건 해킹사고에 직접적으로 적용될 수 없고, 적용된다고 하더라도 원고는 개인정보 유출을 방지할 수 있는 필요하고 적절한 조치를 취함으로써 이 사건 고시 제4조 제9항을 준수하였다.

(2) 피고

(가) ○○클럽 웹 서버는 개인정보처리시스템에 해당하므로 제4 처분사유와 관련하여 이 사건 고시 제4조 제2항과 제4조 제9항이 적용된다.

(나) 퇴직자 계정을 사용 중지한 것만 가지고는 퇴직자의 접근권한을 완전히 말소하였다고 보기 어렵다.

퇴직자 ID 및 그 ID가 포함된 전용 URL이 개인정보처리시스템에 대한 접근권한을 부여받는 수단으로 활용되었으므로 원고는 이 사건 고시 제4조 제2항에서 요구되는 접근권한 말소의무를 이행하지 않은 것이다.

(다) 이 사건 고시 제4조 제9항은 해커의 공격으로 인한 개인정보 유출의 경우에도 적용된다.

해커는 열람 권한이 없는 퇴직자 ID를 이용하여 아무런 인증 없이 ○○클럽에 접속하여 개인정보를 외부로 유출하였다.

원고는 인터넷 홈페이지를 통해 개인정보가 유출되지 않도록 ○○클럽 웹 서버에 아무런 조치를 취하지 아니하였으므로 이 사건 고시 제4조 제9항을 위반하였다.

나) 이 사건 고시 제4조 제2항 위반 여부

개인정보처리시스템에 웹 서버가 포함되지 않더라도 제4 처분사유와 관련하여 이 사건 고시 제4조 제2항이 적용될 수 있다.

위 조항은 퇴직자의 개인정보처리시스템에 대한 접근권한을 말소할 것을 요구하고 있고, 그 목적 달성을 위한 매개체를 개인정보처리시스템에 제한하는 취지는 아니라고 보이기 때문이다(개인정보취급자가 웹 서버를 통해 DB 서버에 접근하는 경로를 취하고 있는 경우에는 웹 서버에 조치를 하여 개인정보처리시스템에 대한 접근권한을 말소하는 것도 상정해 볼 수 있을 것이다).

앞서 인정하였거나 갑 제7호증, 을 제7, 16 내지 18호증의 각 기재, 제1심 증인 소외 4, 소외 5의 각 일부 증언 및 변론 전체의 취지를 통하여 알 수 있는 다음 사정을 종합하면, 원고는 제4 처분사유와 관련하여 이 사건 고시 제4조 제2항을 위반하였다고 판단된다.

(1) 이 사건 고시 제4조 제2항은 '접근권한을 말소하여야 한다.

'라고 규정하고 있고, 이 사건 고시의 해설서에는 임직원이 퇴직한 경우 '해당 사용자의 계정을 삭제(또는 폐쇄)'하라고 설명하고 있다.

(2) 개인정보처리시스템으로의 '접근'은 단순히 인증 절차를 통한 접속에 국한되는 것이 아니라, 서버와 서버 사이의 이동, 데이터의 송수신 등을 통하여 개인정보처리시스템에 가까이 다가가는 것을 광범위하게 포함한다.

이 사건 고시에서 접근통제 관련 조치 중 퇴직자에 대한 접근권한의 말소를 별개의 조항으로 규정하여 그 중요성을 강조한 취지에 비추어 보면, '접근권한 말소'는, 퇴직자의 계정으로는 개인정보처리시스템에 어떠한 접근도 가능하지 않도록 계정을 전면적으로 폐기하는 방법, 계정에 표식을 부여하는 방법, 계정을 변형하는 방법 등으로 개인정보처리시스템의 전 과정에서 식별되어 접근하지 못하도록 하는 조치를 취하였어야 한다는 의미로 보아야 한다.

(3) 소외 6이 2013. 1. 14. 원고에서 퇴사하였고 원고가 계정관리시스템 및 N-STEP 인증 서버의 데이터베이스상 그의 사용자 계정(ID)을 말소한 것은 맞다.

그러나 이는 사실상 '계정 사용 중지'에 불과하고, 그것만으로는 이 사건 고시 제4조 제2항에서 정한 퇴직자의 개인정보처리시스템에 대한 (일체의) '접근권한 말소'에 해당한다고 보기 어렵다.

(4) 해커가 불상의 방법으로 취득한 아래의 URL 주소에는 '퇴직자 ID 변환 값'(굵은 글자)이 포함되어 있고, 해커는 그 URL 주소를 통하여 '고객의 별 포인트 조회'를 할 수 있었다.

해킹에 사용된 URL 중 '퇴직자 ID 변환 값'에 해당하는 EMP_ID가 공란인 경우에는 에러가 발생하였다.

따라서 원고가 퇴직자의 접근권한을 완전히 말소하지 않음으로 인하여 해커가 개인정보처리시스템에 접근하여 개인정보를 누출하였다고 볼 수밖에 없다.

(URL 주소 생략)

다) 이 사건 고시 제4조 제9항 위반 여부

앞서 든 증거들 및 변론 전체의 취지를 통해 알 수 있는 다음의 사정을 종합하면, 피고가 주장하는 사정이나 제출한 증거들만으로는 원고가 제4 처분사유와 관련하여 이 사건 고시 제4조 제9항을 위반하였다고 보기 어렵다.

(1) 이 사건 고시 제4조 제9항은 앞서 본 바와 같이 기본적으로 일반적 이용자의 보편적 접근을 통하여 개인정보가 유출되지 않도록 조치를 취하라는 규정이지, ○○클럽 관련 URL을 불상의 방법으로 획득하는 것과 같은 해킹의 경우를 직접적으로 규율하기 위한 규정이 아니고, ○○클럽 웹 서버는 개인정보처리시스템으로 볼 수 없다.

(2) 해커는 불상의 방법을 통해 원고의 N-STEP 시스템의 사용자 인증 과정을 거치지 않고 ○○클럽 고객 포인트 조회 화면으로 바로 연결되는 URL 주소를 획득하여 이를 이용해 포인트 조회 화면을 열람함으로써 고객의 개인정보를 유출하였다.

N-STEP 시스템은 상담사의 ID와 비밀번호로 인증하고 해당 PC의 MAC 주소까지 비교하고 인증토큰이 발행되는 등 다중 인증 과정을 거쳐야 사용할 수 있고, 원고는 계정관리시스템 및 N-STEP 인증 서버의 데이터베이스상에서 퇴직자 계정(ID)을 말소했음을 고려하면 원고가 이 사건 고시 제4조 제9항에서 요구하는 조치를 다하지 못하였다고 단정하기 어렵다.

(3) 원고는 ○○클럽 시스템에도 웹 취약점을 점검하기 위하여 IBM Security AppScan, HP Fortify Static Code Analyzer 등 자동화된 점검 도구를 도입・활용하였고 외부 보안 전문가를 통하여 모의해킹을 수시로 수행하는 등 취약점을 최소화하기 위하여 현실적으로 취할 수 있는 조치들을 취하였다.

6) 재량권의 일탈・남용 여부

가) 구 정보통신망법 제64조의3 제1항 제6호는 '방송통신위원회는 이용자의 개인정보를 유출한 경우로서 제28조 제1항 제2호부터 제5호까지의 조치를 하지 아니한 경우에는 해당 정보통신서비스 제공자 등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다'고 규정하고 있다.

한편, 피고는 법 위반행위에 대하여 과징금을 부과할 것인지 여부와 과징금을 부과한다면 일정한 범위 안에서 과징금의 액수를 구체적으로 얼마로 정할 것인지에 관하여 재량을 가지고 있으나, 구 정보통신망법 시행령 제69조의2 제4항 [별표 8]은 과징금의 산정기준과 산정절차를 구체적으로 규정하면서 세부기준 및 부과방법 등에 관한 사항을 고시에 위임하고 있고, 피고는 이에 근거하여 별지 관련 법령의 '구 개인정보보호 법규 위반에 대한 과징금 부과기준(이하 '이 사건 과징금 기준'이라 한다)'을 제정하여 시행하고 있는데, 이 사건 과징금 기준이 비록 피고의 재량준칙에 불과한 것이라고 하더라도 이는 법에서 정한 금액의 범위 내에서 적정한 과징금의 산정기준을 마련하기 위하여 제정된 것이므로, 피고로서는 과징금액을 산출할 때 이 사건 과징금 기준상의 고려요소 및 법에서 정한 참작사유를 고려한 적절한 액수로 정하여야 할 것이다.

이러한 재량의 행사와 관련하여 과징금 부과의 기초가 되는 사실을 오인하였거나 비례・평등의 원칙에 위반되는 등의 사유가 있다면 이는 재량권의 일탈・남용으로서 위법하다고 볼 수 있다(대법원 2002. 9. 24. 선고 2000두1713 판결, 대법원 2008. 2. 15. 선고 2006두4226 판결 등 참조). 처분을 할 것인지 여부와 처분의 정도에 관하여 재량이 인정되는 과징금 납부명령에 대하여 그 명령이 재량권을 일탈하였을 경우 법원으로서는 재량권의 일탈 여부만 판단할 수 있을 뿐이지 재량권의 범위 내에서 어느 정도가 적정한 것인지에 관하여는 판단할 수 없어 그 전부를 취소할 수밖

에 없다(대법원 2009. 6. 23. 선고 2007두18062 판결 등 참조).

나) 위 법리와 관련 규정에 비추어 살피건대, 이 사건 처분사유 중 제4 처분사유를 제외하고 제1 내지 제3 처분사유는 인정되지 않는다면 원고의 위반행위의 내용, 위반행위로 인한 개인정보의 피해규모, 구 정보통신망법 제28조 제1항에 따른 기술적·관리적 보호조치의 이행 정도 등에 차이가 나타나므로 피고가 원고의 위반행위를 '중대한 위반행위'로 평가하여 과징금을 산정한 것은 재량권을 일탈·남용한 것으로 볼 수 있다.

라. 소결

따라서 이 사건 처분은 위법하다.

3. 결론

그렇다면 원고의 이 사건 청구는 이유 있으므로 인용하여야 할 것인데 제1심판결은 이와 결론을 같이하여 정당하므로, 피고의 항소는 이유 없어 이를 기각하기로 하여 주문과 같이 판결한다.

(별지 생략)

판사 한창훈(재판장) 김상우 원익선