방 송 통 신 위 원 회
심의·의결

안건번호 제2017 - 45 - 276호

안 건 명 ㈜ 의 개인정보 유출사고에 대한 시정조치에 관한 건

피 심 인 ㈜

대표이사
(사업자등록번호 : , 법인등록번호 :)

의 결 일 2017. 12. 12.

주 문

1. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고, 개인정보의 안전성을 확보하기 위하여 ①개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 및 탐지시스템 운영을 철저히 하여야 하며, ②개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하여야 하며, ③악성프로그램 방지를 위해 백신소프트웨어 등의 보안 프로그램을 설치·운영하여야 하고, ④개인정보가 복사된 외부 저장매체 등 개인정보 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 하여야 한다.

2. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지에 1주일 이상 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

3. 피심인은 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호 책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 분실·도난·유출 등을 방지하기 위한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

4. 피심인에 대하여 다음과 같이 과징금과 과태료를 각 부과한다.

가. 과 징 금 : 원

나. 과 태 료 : 15,000,000원

다. 납부기한 : 고지서에 명시된 납부기한 이내

라. 납부장소 : 한국은행 국고수납 대리점

마. 과태료를 내지 않으면 질서위반행위규제법 제24조, 제52조, 제53조제1항 및 제54조에 따라 불이익이 부과될 수 있음

5. 피심인에 대하여 정보통신망법 제69조의2제2항에 따라 개인정보 유출 및 정보통신망법 위반과 관련하여 피심인의 대표자 및 책임 있는 임원을 포함한 책임자에 대해 징계할 것을 권고한다. 피심인은 이를 존중하여야 하며 그 결과를 처분통지를 받은 날로부터 90일 이내에 방송통신위원회에 통보하여야 한다.

이 유

Ⅰ. 기초 사실

㈜ (이하 '피심인'이라 한다)은 '14. 1. 5.부터 영리를 목적으로 가상통화 취급관련 웹사이트 ' '( )을 운영하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)」 제2조 제1항 제3호에 따른 정보통신서비스 제공자이고, 피심인의 일반현황과 최근 3년간 매출액은 다음과 같다.

<참고 1> 피심인의 일반현황

('16년말 기준)

사업자명	대표자	업 종	종업원 수	매출액(단위:천원)
㈜		전자상거래 (가상통화 거래)		

<참고 2> 피심인의 최근 3년간 매출액

(단위 : 천원)

구 분	2014년	2015년	2016년	합 계	3년 평균*
전체 매출					
관련 매출					
관련없는 매출**					

* 정보통신망법 시행령 제69조의2제1항 단서에 따라 사업개시( ) 후 '16년말까지의 매출액을 연평균 매출액으로 환산

** 사이트 운영 외 기타 사업내역 없음

Ⅱ. 사실조사 결과

1. 조사대상

방송통신위원회는 피심인이 보관, 관리하는 이용자의 개인정보가 인적사항을 알 수 없는 해커(이하 '이 사건 해커'라 한다)에 의해 유출되었다는 신고('17. 6. 30.)를 접수하고,

한국인터넷진흥원과 함께 피심인을 대상으로 피심인으로부터 넘겨받은 사고 관련자료와 개인정보취급자가 피심인의 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 '개인정보처리시스템'이라 한다) 등에 남아있는 접속기록 등을 토대로 해킹경로 파악과 개인정보의 기술적·관리적 보호조치 등 정보통신망법 위반 여부 확인을 위한 개인정보 처리·운영 실태를 조사(2017. 7. 1. ~ 7. 28.)하였고, 다음과 같은 사실을 확인하였다.

2. 행위사실

가. 유출 규모

피심인이 ' ' 서비스를 운영하면서 수집한 명의 개인정보는 파일(2017년 .xlsx) 형태로, 최소 명의 회원접속에 필요한 이용자 정보(ID, PW)는 사전대입공격[1]에 따라 최소 명의 개인정보가 외부에 유출 또는 탈취되었다.

1) 사전대입공격(Dictionary Attack)이란 공격자가 사전에 확보한 ID/PW 정보 또는 일반적으로 사용되는 정보 파일을 가지고 프로그램을 통해 하나씩 모두 대입시켜 보는 방법

<참고 3> ㈜ 의 유출·정보 현황

구 분	유 출 항 목	건 수	중복제거
회원관리정책 파일	이름, 이메일, 핸드폰번호, 거래건수, 거래량, 거래금액	건	명
사전대입공격	홈페이지 ID(이메일), 패스워드*	최소 건	최소 명
합 계	-	최소 건	최소

※ 이메일은 그 자체로는 특정 개인을 알아 볼 수 없을지라도 다른 정보와 용이하게 결합할 경우 개인을 알아 볼 수 있는 정보(서울중앙지방법원 2007.2.8. 2006가합 33062)에 해당할 뿐만 아니라, 사이트에 해당 ID와 패스워드로 로그인 시 이름·연락처 등을 확인할 수 있음

나. 유출 경로

(1) 개인정보 수집현황

피심인은 ' ' 서비스를 운영하면서 시 기준으로 건의 회원정보, 건의 휴면 회원정보를 보유하고 있다.

<참고 4> ㈜ 의 개인정보 수집 현황

구 분	항 목	수집일	건수
이용자 정보 ( )	이름, 이메일(암호화), 핸드폰번호(암호화), 비밀번호(암호화), 생년월일, 성별	~	건

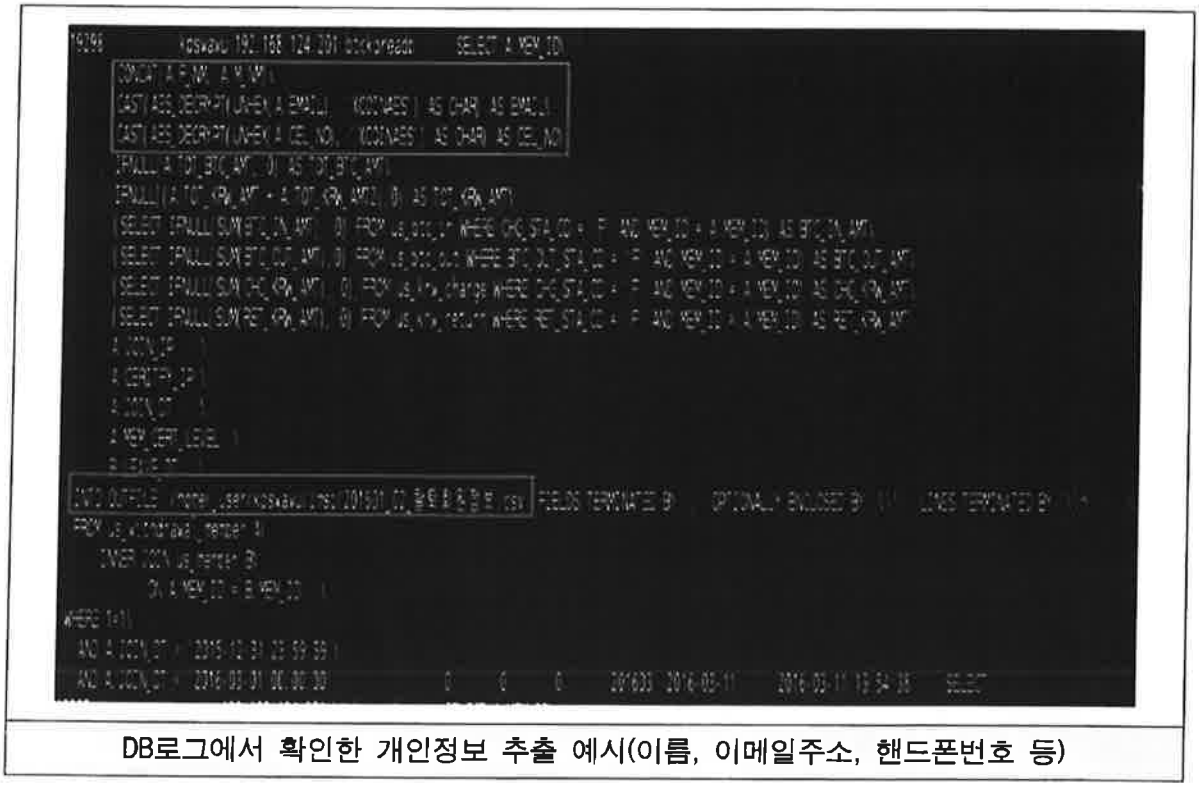
(2) 개인정보 유출경로

《 스피어피싱[2]을 통한 이용자 개인정보 파일 유출 관련 》

피심인의 개인정보처리시스템 담당 직원인 김OO은 .부터 까지 총 차례 개인정보처리시스템에서 CSV파일을 추출하였고, 그 중 560차례는 이용자 정보(이메일, 이름, 휴대전화번호, 거래관련 정보 등)를 추출하여 CSV 파일로 업무용 컴퓨터에 저장하였다.

2) 스피어피싱(Spear phishing)이란 특정한 개인들이나 회사를 대상으로 이메일이나 전자통신사기를 통해 수신자의 개인정보를 요청하거나 정상적인 문서파일을 위장한 악성코드를 실행하도록 하는 공격기법

<참고 5> ㈜ 김○○이 추출한 개인정보 CSV 파일

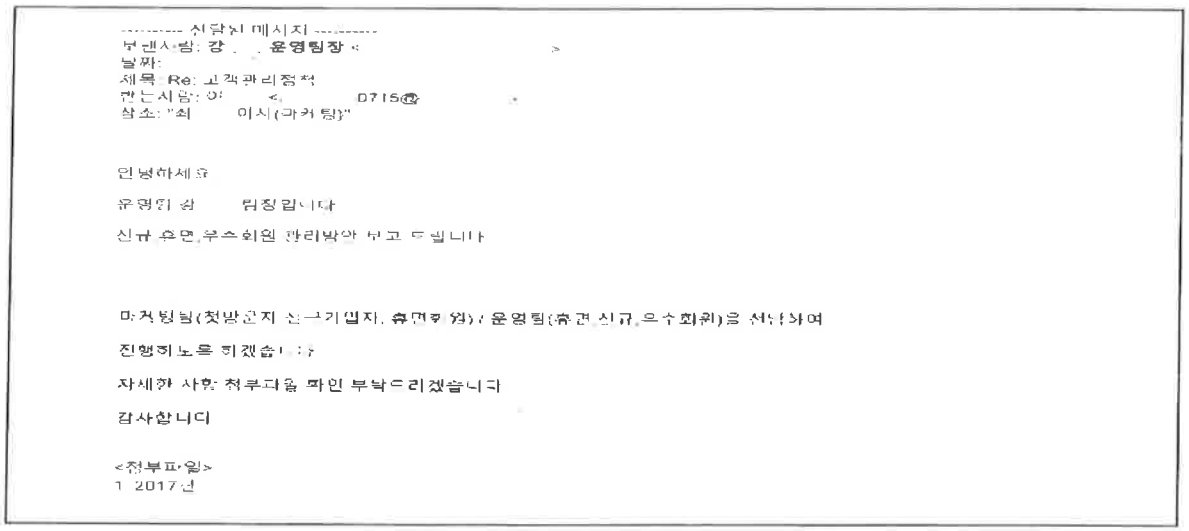


DB로그에서 확인한 개인정보 추출 예시(이름, 이메일주소, 핸드폰번호 등)

김OO은 추출한 개인정보 파일을 부터 수시로 피심인 회사의 운영 지원팀장 강OO에게 수신자의 이름과 날짜 등의 비밀번호를 설정하여 압축한 후 파일서버 및 USB로 전달하였다.

강OO은 김OO으로부터 전달 받은 고객정보를 가공하여, 이용자정보 건이 포함된 "2017년 .xlsx" 파일로 만들어 업무용 컴퓨터 등에 암호화 하지 않고 저장한 후, 자문계약에 따라 피심인의 경영관리 업무 전반을 자문하고 있는 이OO에게 개인 메일(*******0715@)로 전달하였고, e메일을 받은 이OO은 이전에 개인 컴퓨터에서 "2017년 .xlsx"을 열람 및 저장하였다.

<참고 6> ㈜I 강OO이 이OO에게 보낸 e메일


---------- 전달된 메시지 ----------
보낸사람: 강 . . 운영팀장 <
날짜:
제목: Re: 고객관리정책
받는사람: 이 <. 0715@
참조: "최 이사(과커팀)"

안녕하세요

운영팀 강 팀장입니다

신규 휴면 우수회원 관리방안 보고 드립니다

마케팅팀(첫방문지 신규기업지, 휴면후원) / 운영팀(휴면 신규 우수회원)을 선정하여

진행하도록 하겠습니다.

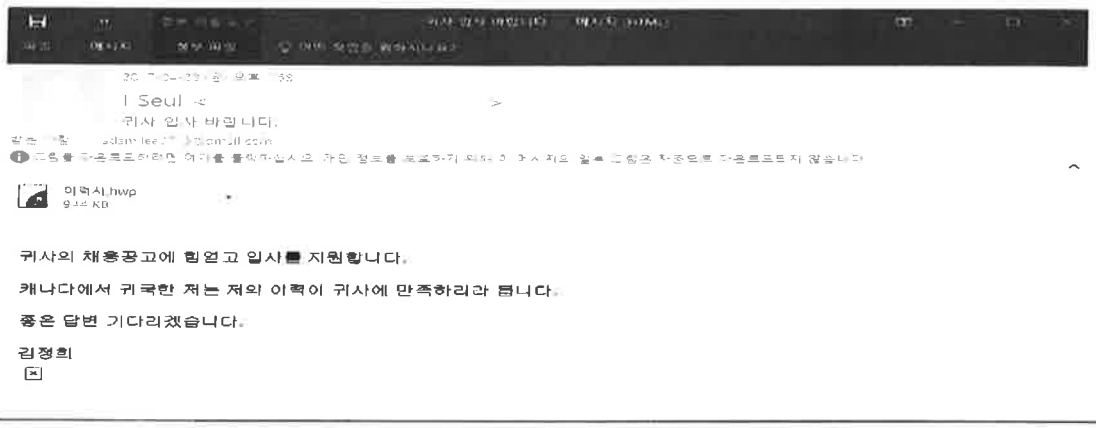
자세한 사항 첨부파일 확인 부탁드리겠습니다

감사합니다

<첨부파일>
1 2017년

미상의 해커는 피심인의 직원 채용기간( )에 맞춰 이OO의 메일주소(*******0715@)로 이력서를 위장한 한글파일 "이력서.hwp"을 전송( )하였으며, 첨부된 "이력서.hwp"파일은 한글워드 프로세서의 EPS(PostScript) 기능을 이용하여 악성코드를 드롭하는 악성한글 문서이다.

<참고 7> 미상의 해커가 이OO에게 보낸 e메일

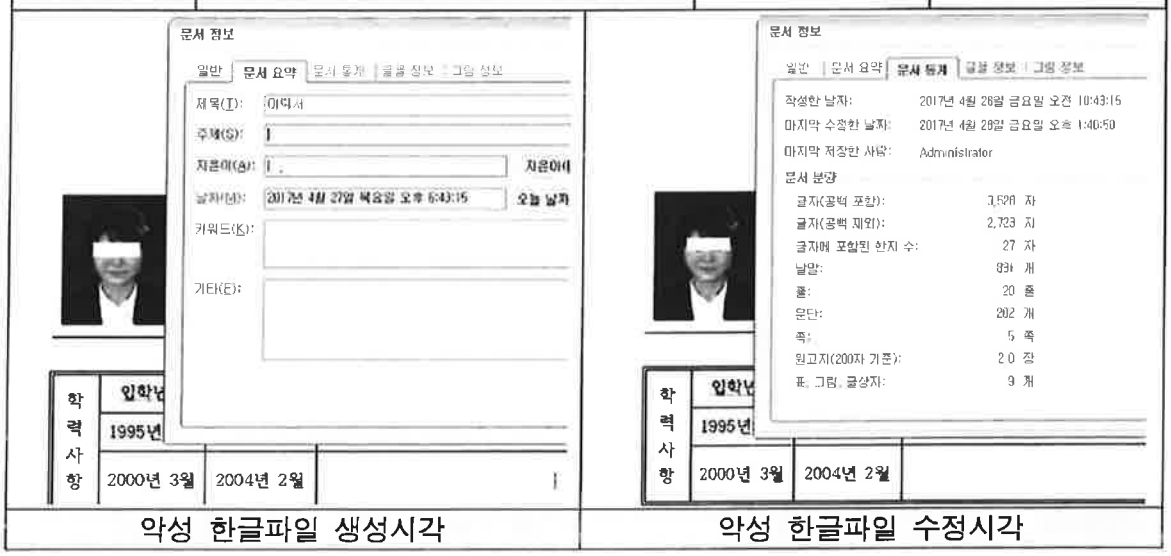

I Seul <
귀사 입사 바랍니다.
이력서.hwp
944 KB

귀사의 채용공고에 힘얻고 입사를 지원합니다.
캐나다에서 귀국한 저는 저의 이력이 귀사에 만족하리라 봅니다.
좋은 답변 기다리겠습니다.
김정희

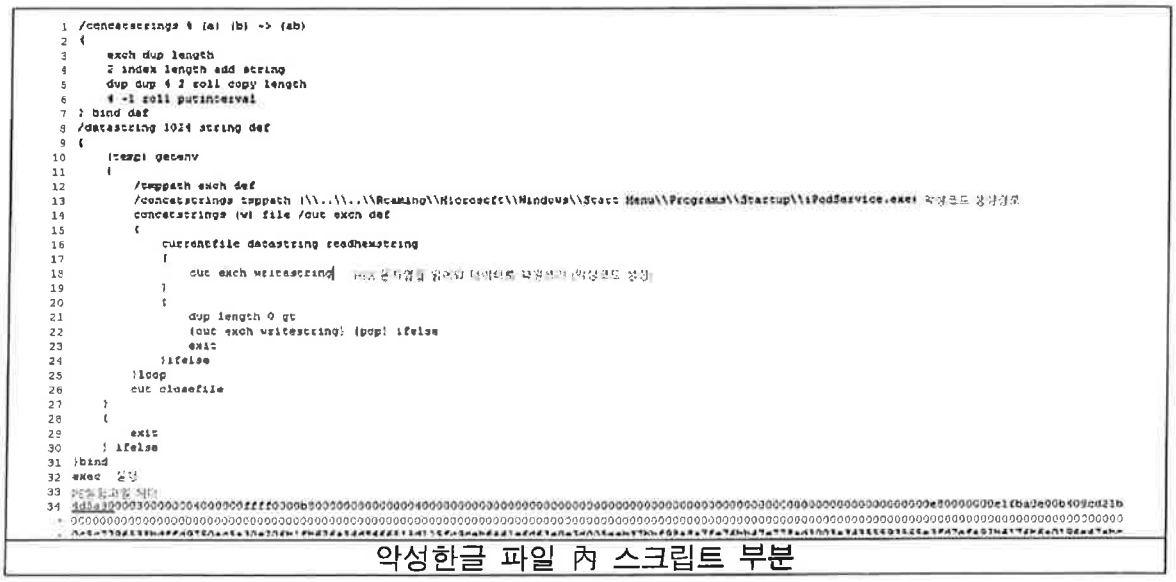
악성 한글파일이 포함된 스피어 피싱 이메일

<참고 8> 이력서 위장 악성 한글파일 내용

파일명	MD5	생성시각	수정시각
이력서.hwp			



악성 한글파일 생성시각 | 악성 한글파일 수정시각



악성한글 파일 內 스크립트 부분

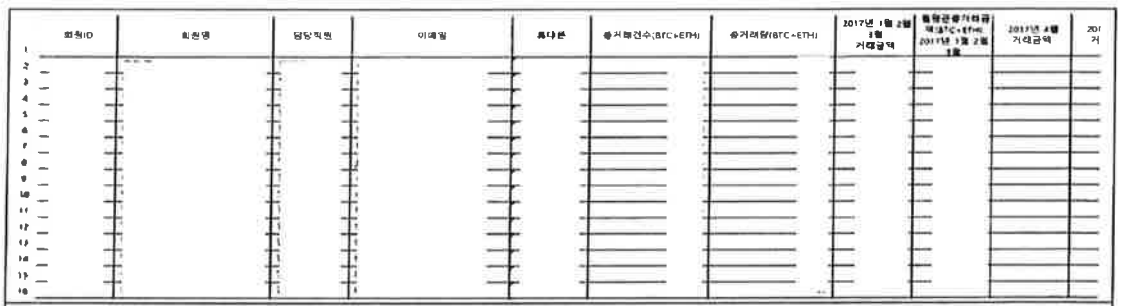
"이력서.hwp"파일에서 드롭된 악성코드는 C&C의 명령을 수행하는 원격제어형 악성코드( )로, 해당 악성코드 감염 시 원격지(C&C)의 명령을 받아 파일탐색, 파일업로드, 다운로드, 감염PC정보수집, CMD명령 실행 등을 수행 가능하다.

<참고 9> C&C 명령 악성코드 내용

파일명	MD5	컴파일 시각

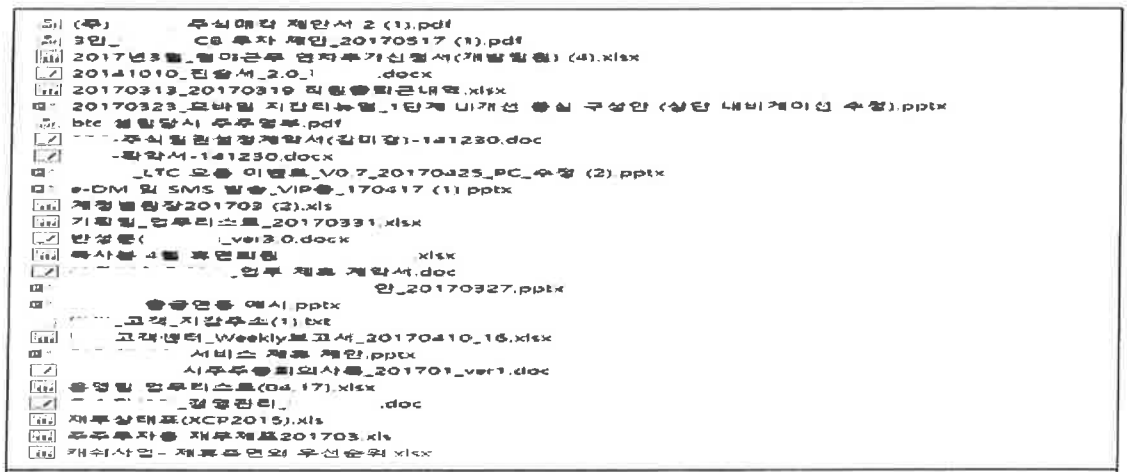
이OO이 해커로부터 온 e메일에 첨부된 "이력서.hwp"파일을 실행함에 따라 해당 컴퓨터가 원격제어형 악성코드에 감염되었고, 강OO으로부터 e메일로 받아 이전에 저장 중이던 "2017년 .xlsx"파일 또한 동일한 컴퓨터에 저장되어 있었기에, 이후 해커는 이OO의 컴퓨터에서 "2017년 .xlsx" 파일 외 다수의 파일을 원격제어에 의해 외부로 유출된 것으로 추정된다.

<참고 10> "2017년 .xlsx" 파일 개인정보 내용



유출된 회원정보 파일 내용

<참고 11> 이OO 컴퓨터 중 개인정보 파일 외 유출파일



개인정보파일 외 내부 문서

《 사전대입공격을 통한 이용자 계정 탈취 관련 》

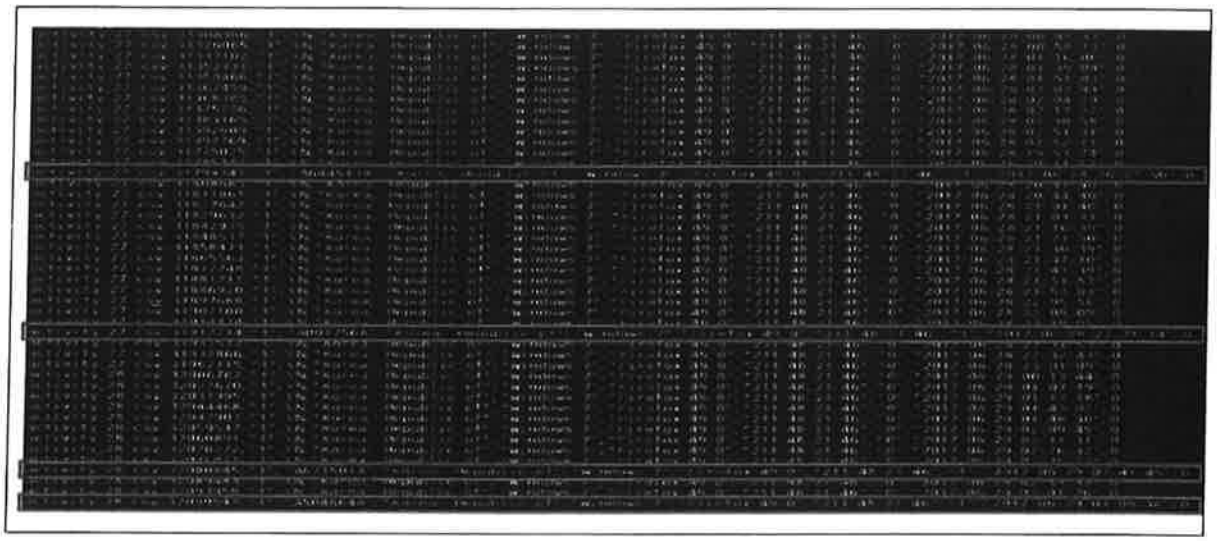
해커는 부터 까지 약 개의 IP주소(국외 개, 국내 개)에서 출처를 알 수 없는 아이디, 패스워드를 이용하여 피심인의 홈페이지의 사전대입 공격을 약 만번 시도하였다.

<참고 12> 해커의 공격내역(IP주소, 국가코드, 횟수)

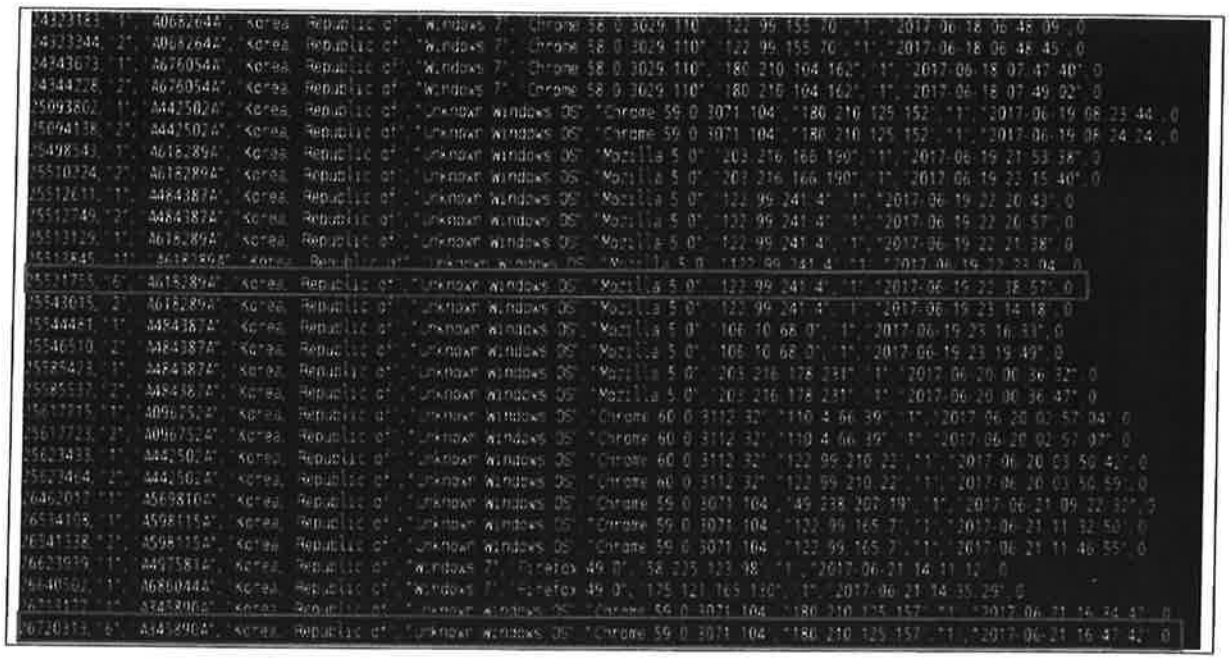
구분	IP주소	국가코드	공격횟수
1		KR	19,893
2		KR	19,151
3		KR	16,553
4		KR	16,500
5		KR	16,139
6		KR	16,102
7		KR	13,754
8		KR	13,717
9		KR	13,511
10		KR	13,401
사전대입 공격 상위 10개 IP			

해커의 사전대입 공격을 통해 로그인 성공으로 탈취된 계정은 개이며, 이중 이용자 피해신고 접수 계정 개, 가상통화가 출금된 미신고 계정 개 등 총 개에서 이용자 피해가 있는 것으로 확인되었다.

<참고 13> 해커의 사전대입 공격 시도 및 로그인 성공 로그



<참고 14> 해커의 로그인 성공 후 출금 로그



참고로 해커는 을 송금하지 않으면 피심인으로부터 탈취한 이용자의 개인정보를 공개하겠다는 내용으로 부터 까지 ㈜ 임직원에게 차례 걸쳐 협박메일을 발송하였다.

<참고 15> 해커의 협박 메일 발송 현황

구분	발송 일시	발송횟수	비 고
1차		1회	임직원
2차		1회	임직원 (이용자 26명 개인정보 포함)
3차		31회	임직원
계	-	33회	

다. 개인정보 유출경로 요약

○ 스피어피싱을 통한 이용자 개인정보 유출 관련

① 해커는 ㈜ 의 직원 메일로 '이력서.hwp'를 발송하여 해당 직원의 컴퓨터를 원격제어형 악성코드에 감염시키고,

② 해커는 직원 컴퓨터에 저장되어 있는 "2017년 .xlsx"외 다수 파일을 유출한 것으로 확인됨

○ 사전대입 공격으로 이용자 계정 탈취 관련

① 해커는 ㈜ 의 홈페이지에서 출처를 알 수 없는 아이디, 패스워드로 약 만번 로그인을 시도( )

② 이를 통해 홈페이지 로그인이 성공한 이용자 계정이 일부 유출

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 침입차단시스템( ) 및 침입탐지시스템( )을 설치·운영하고 있었으나, ' 까지 해킹 신고 등이 건* 접수되었음에도 불구하고 해커의 사전대입 공격으로 추정되는 시도(최소 번)에 대하여 이를 탐지하지 못한 사실이 있다.

* 신고 접수 된 건을 분석한 결과, 해킹피해(추정) 건(약 원), 고객IP 차단 요청 건, 명의도용 및 보이스피싱 건, 해킹 건 등임

나. 개인정보를 저장하면서 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**하지 않은 행위**

피심인의 직원 강OO은 김OO으로부터 전달 받은 고객정보를 가공하여, 이용자정보 건이 포함된 "2017년 .xlsx" 파일로 만들어 업무용 컴퓨터 등에 암호화하지 않고 저장한 후, 자문계약에 따라 피심인의 경영관리 업무 전반을 자문하고 있는 이OO에게 개인 메일(*******0715@)로 전달하였고, e메일을 받은 이OO은

이전에 개인 컴퓨터에서 "2017년 .xlsx"을 열람 및 저장하면서 이를 암호화 하지 않고 저장한 사실이 있다.

다. 개인정보를 안전하게 관리하기 위해 백신소프트웨어의 설치·운영{정보통신망법 제28조(개인정보의 보호조치) 중 백신소프트웨어 설치·운영 보호조치}에 대한 보호조치를 하지 않은 행위

한글문서에서 EPS(PostScript)기능을 이용하여 악성코드를 드롭하는 한글프로그램의 취약점은 에 패치가 완료되어 한글프로그램의 업데이트를 하였을 경우 해당 악성코드의 감염을 막을 수 있었음에도 불구하고, 피심인의 직원인 이OO은 이후 컴퓨터에 설치된 한글 프로그램에 대하여 업데이트를 실시한 사실이 없으며, 기준 이OO은 백신소프트웨어를 설치하거나 업데이트 한 사실이 없다.

라. 개인정보를 안전하게 관리하기 위해 출력·복사물{정보통신망법 제28조(개인정보의 보호조치) 중 출력·복사시 보호조치}에 대한 보호조치를 하지 않은 행위

피심인의 직원인 김OO이 강OO에게 개인정보파일을 전달하기 위해 사용한 USB 또는 파일서버를 경 피심인의 회사를 이전하면서 파기한 사실이 있으며, USB 또는 파일서버를 통해 개인정보파일을 전달한 기록 등을 남기지 않았다.

마. 처분의 사전통지 및 의견수렴

방송통신위원회는 2017. 11. 10. '개인정보보호 법규 위반사업자 시정조치(안) 사전 통지 및 의견 수렴' 공문을 통하여 이 사건에 대한 피심인의 의견을 요청하였으며, 피심인은 2017. 11. 27. 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)', '개인정보를 안전하게 저장·전송할 있는 암호화기술 등을 이용한 보안조치(제4호)', 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해방지 조치'(제5호), '그 밖에 개인정보의 안정성 확보를 위하여 필요한 보호조치(제6호)'를 하여야 한다."라고 규정하고 있다.

나. 정보통신망법 시행령 제15조제2항은 "개인정보에 대한 불법적인 접근을 차단하기 위하여 '개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영(제2호)' 등을 조치하여야 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, 제5항은 "정보통신서비스 제공자 등은 개인정보처리시스템 및 개인정보취급자가 개인정보에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다"라고 규정하고, 제6항은 "개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다"고 규정하고 있다.

다. 정보통신망법 시행령 제15조제6항에 따라 위 기준 수립·시행의 내용을 구체적으로 정하고 있는 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2015-3호, 이하 '고시') 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.

고시 제6조4항은 "정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화 해야 한다"라고,

고시 제7조는 "정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하고, 제1호에 보안프로그램의 자동 업데이티 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지, 제2호에는 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시하여야 한다"라고,

고시 제9조제2항은 "정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다"고 규정하고 있다.

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

고시 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.

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제4조제5항에 대해 ▲"정보통신망을 통해 개인정보처리시스템에 불법적으로 접근하는 행위를 방지·차단하기 위해 침입차단기능 및 침입탐지기능을 갖는 시스템 등을 설치·운영함으로써 네트워크 보안을 강화하여야 한다."라고,

▲"침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법으로, 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"라고,

▲"불법적인 접근 및 침해사고 방지를 위한 목적 달성을 위해서는 침입차단과 침입탐지 기능을 갖는 시스템 도입과 더불어 침입차단 정책 설정 및 침입탐지 로그 분석, 로그 훼손 방지 등 적절한 운영·관리가 중요하다."라고 설명하고 있다.

구 개인정보의 기술적·관리적 보호조치 기준(2015. 5. 19. 방송통신위원회고시 제2015-3호로 개정되기 전의 것) 제1조는 기술적·관리적 보호조치의 '구체적인 기준'을 정하는 것을 목적으로 한다고 규정하고 있었으나, 방송통신위원회는 2015. 5. 19. 개인정보 보호조치에 대한 사업자의 자율성·책임성을 강화하기 위하여 「개인정보의 기술적·관리적 보호조치 기준」 제1조를 개정하여 고시 상의 의무들이 사업자가 준수해야 할 '최소한의 기준'임을 명시적으로 규정하고, 고시 제1조제2항에 사업자들이 사업의 규모, 개인정보 보유 수 등을 고려하여 자발적으로 보호조치를 이행하도록 하는 규정을 신설하였다.

고시 제4조제5항의 입법 목적은 '정보통신망을 통한 불법적인 접근 및 침해

사고 방지'이고, 그 내용은 첫째 침입차단 및 침입탐지 기능을 포함한 시스템의 '설치'의무이고, 둘째 침입차단 및 침입탐지 기능을 포함한 시스템의 '운영'의무이다.

먼저 시스템 '설치' 의무에 대하여 살펴보면, 정보통신서비스 제공자등은 ①접속권한을 IP주소 등으로 제한하여 비인가 접근을 '차단'하는 기능(침입차단기능)과 함께 ②개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법유출시도를 '탐지'하는 기능(침입탐지기능)을 보유한 시스템을 설치하여야 한다.

'운영' 의무와 관련하여, 시스템의 '운영'은 단순히 시스템의 전원을 켜 놓은 상태를 의미하는 것이 아니라 목적(침입차단 및 침입탐지) 달성에 필요한 기능을 활용하는 것을 의미하므로, 단순히 시스템의 전원을 켜 놓은 상태나 침입차단 및 침입탐지에 필요한 기능을 활용하지 못한 상태 등은 '운영'이라고 할 수 없다.

특히 피심인은 미상의 해커가 부터 까지 약 개의 IP주소(국외 개, 국내 개)에서 출처를 알 수 없는 아이디, 패스워드를 이용하여 ㈜ 홈페이지의 사전대입 공격을 약 번 시도하였으며, 부터 까지 해킹 신고 등이 건 접수되었음에도 불구하고, 개인정보처리시스템에 접속한 IP주소 등을 재분석하지 않은 점에서 침입차단 및 침입탐지에 필요한 해당 기능을 포함한 시스템을 운영하였다고 볼 수 없다.

따라서 피심인은 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·운영하여 대규모 사전대입공격을 탐지해 내지 못함으로써 정보통신망법 제28조제1항제2호(기술적·관리적 보호조치 중 접근통제), 시행령 제15조제2항, 고시 제4조제5항을 위반하였다.

나. 개인정보를 저장하면서 암호화{정보통신망법 제28조(개인정보의 보호조치) 중 암호화}**하지 않은 행위**

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제6조제4항에 대해 고객의 개인정보를 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려받아 저장할 때에는 파일 암호화 제품 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 하고, 안전한 비밀번호나 보안강도 112비트 이상의 암호화 알고리즘을 사용해야 한다고 해설하고 있다.

피심인이 이용자정보 건이 포함된 "2017년 .xlsx" 파일을 안전하게 암호화 하지 않고 개인용 컴퓨터에 저장한 행위는 정보통신망법 제28조제1항제4호, 시행령 제15조제4항제4호, 개인정보의 기술적·관리적 보호조치 기준(이하 '고시'라 한다)제6조제4항에 위반된다.

다. 개인정보를 안전하게 관리하기 위해 백신소프트웨어의 설치·운영{정보통신망법 제28조(개인정보의 보호조치) 중 백신소프트웨어 설치·운영 보호조치}**에 대한 보호조치를 하지 않은 행위**

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제7조에 대해 악성프로그램은 계속해서 새롭게 만들어지고, 변화하고, 유포되고 있으므로 이에 대응하여 백신회사는 새로운 바이러스에 대하여 백신소프트웨어를 업데이트하고 있으므로, 새로운 유형의 악성 프로그램이 공지되면 자동 업데이트 기능을 이용하여 신속하게 긴급 업데이트를 실행하여야 한다고 해설하고 있고, 백신 소프트웨어는 항상 실행시켜 둔 채로 하루에 1회 정도 사용자 임의로 점검시간을 설정하여 악성프로그램 검사를 자동으로 실행할 수 있도록 설정하는 것이 필요하며, 최소 월 1회 이상 주기적으로 갱신 및 점검하여야 한다고 해설하고 있다.

피심인이 e메일을 통해 파일을 송수신하고 내려받은 개인정보를 저장하고 있는 컴퓨터를 수시로 사용하면서 이를 안전하게 관리하기 위해 악성 프로그램 등을

방지·치료할 수 있는 백신소프트웨어 등의 보안 프로그램을 설치·운영하지 않은 행위는 정보통신망법 제28조제1항제5호, 시행령 제15조제5항, 개인정보의 기술적·관리적 보호조치 기준(이하 '고시'라 한다)제7조에 위반된다.

라. 개인정보를 안전하게 관리하기 위해 출력·복사물{정보통신망법 제28조(개인정보의 보호조치) 중 출력·복사시 보호조치}에 대한 보호조치를 하지 않은 행위

「개인정보의 기술적·관리적 보호조치 기준 해설서」는 고시 제9조제2항에 대해 개인정보처리시스템에서 개인정보를 복사하여 외부 저장매체에 저장하는 경우 출력복사물의 생성, 이용, 전달, 파기 과정까지의 책임관계를 명확히 하여 사후 문서 유출 발생시 출처를 확인할 수 있도록 하고 임의적인 고객 개인정보 명단을 출력·복사하는 행위를 억제하여 개인정보 유출 위험을 최소화할 수 있다고 설명하면서, 필요한 보호조치를 하는 방법으로 업무의 상황에 따라 출력·복사물의 책임관계 및 출처를 명확히 하기 위해 관련정보를 기록하여 관리하도록 해설하고 있다.

피심인이 개인정보처리시스템에서 USB 또는 파일서버를 통해 개인정보를 복사하면서 이를 전달한 기록을 남기지 않아 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 하지 않은 행위는 정보통신망법 제28조제1항제6호, 시행령 제15조제6항, 고시 제9조제2항을 위반된다.

Ⅳ. 시정조치 명령

1. 시정명령

가. 피심인은 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고, 개인정보의 안전성을 확보하기 위하여 ①개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 및 탐지시스템 운영을 철저히 하여야 하며,

②개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치를 하여야 하며, ③악성프로그램 방지를 위해 백신소프트웨어 등의 보안 프로그램을 설치·운영하여야 하고, ④개인정보가 복사된 외부 저장매체 등 개인정보 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 하여야 한다.

나. 피심인은 제1항의 시정명령을 받은 사실을 시정명령을 받은 날부터 1개월 이내에 4단×10cm 또는 5단×9cm의 크기로 1개의 중앙일간지에 평일에 1회 이상 공표하고, 피심인의 홈페이지에 1주일 이상 게시한다. 이때, 공표내용 등은 방송통신위원회와 사전 협의를 거쳐야 한다.

<참고 16> 시정명령 공표(안) 예시

공표내용(안)
저희 회사(OOOO)는 방송통신위원회로부터 ①침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 행위, ③악성프로그램 방지를 위해 백신소프트웨어 등의 보안 프로그램을 업데이트 하지 않은 행위, ④개인정보가 복사된 외부 저장매체 등 개인정보 출력·복사물을 기록 관리하지 않은 행위가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반했다는 이유로 시정명령을 받은 사실이 있습니다.

2. 시정명령 이행결과의 보고

피심인은 시정명령에 따른 시정조치를 이행하고, 대표자를 비롯하여 개인정보보호 책임자 및 개인정보취급자를 대상으로 정기적인 교육을 실시하고, 그 실시 결과를 포함한 개인정보의 분실·도난·유출을 방지하기 위한 재발방지대책을 수립하여 처분통지를 받은 날로부터 30일 이내에 방송통신위원회에 보고하여야 한다.

※ 위 사항에서 정하지 않은 시정명령 이행계획 및 이행결과보고 등 추가 세부사항은 방송통신위원회와 협의하여 이행하도록 한다.

V. 과징금 부과

피심인의 정보통신망법 제28조제1항 위반에 대한 과징금은 같은 법 제64조의3 제1항제6호, 같은 법 시행령 제69조의2제1항과 제4항 [별표 8] (과징금의 산정기준과 산정절차) 및 '개인정보보호 법규 위반에 대한 과징금 부과기준(이하 '부과기준'이라 한다)'에 따라 다음과 같이 부과한다.

1. 과징금 상한액 및 기준금액

가. 과징금 상한액

피심인의 정보통신망법 제28조제1항을 위반한 과징금 상한액은 같은 법 제64조의3제1항, 시행령 제69조의2에 따라 위반행위와 관련된 정보통신서비스의 직전 3개 사업년도의 연평균 매출액의 100분의 3 이하에 해당하는 금액으로 한다.

나. 기준금액

1) 고의·중과실 여부

'부과기준' 제5조제1항은, 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리목적의 유무, 정보통신망법 제28조제1항에 따른 기술적·관리적 보호조치 이행 여부 등을 고려하여 판단하도록 규정하고 있다.

이에 의할 때, 피심인은 영리를 목적으로 가상통화 취급관련 웹사이트 ' '( )을 운영하는 정보통신망법 제2조제1항제3호에 따른 정보통신서비스 제공자로서 ▲피심인이 . 기준 보관·관리하고 있던 개인정보량이 명으로 매우 방대하고, ▲가상통화 특성상 이용자의 계좌정보

등 개인정보는 이용자에게 금전적 피해 등이 발생될 우려가 있어 이에 걸맞은 엄격하고 세밀한 개인정보 관리가 요구됨에도 ▲정보통신망법 제28조제1항제2호에 따른 접근통제의 기술적·관리적 보호조치 중 침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ▲정보통신망법 제28조제1항제4호에 따른 이용자의 개인정보를 암호화하지 않고 저장한 행위, ▲정보통신망법 제28조제1항제5호에 따른 한글 프로그램 등에 대해 백신 소프트웨어를 업데이트하지 않은 행위 등의 행위로 이 사건 해커에 의해 이용자의 개인정보가 유출되게 하는 빌미를 제공하였으므로, 피심인에게 중과실이 있다.

2) 중대성의 판단

'부과기준' 제5조제3항은, 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 '매우 중대한 위반행위'로 판단하도록 규정하고 있고,

'부과기준' 제5조제3항 단서조항은, 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 해당할 때에는 '보통 위반행위'로, 1개 이상 2개 이하에 해당할 때에는 '중대한 위반행위'로 감경하도록 규정하고 있다.

이에 의할 때, 피심인의 위반행위의 결과가 ▲위반행위로 직접적으로 이득을 취득하지 않은 점, ▲위반행위로 인한 개인정보의 피해규모가 피심인이 보유하고 있는 개인정보의 100분의 5 이내(기준, 피심인의 이용자의 개인정보 건 중 최소 건 유출)인 점, ▲이용자의 개인정보가 공중에 노출된 점 등을 종합적으로 고려할 때, 위반행위의 중대성을 감경하여 '중대한 위반행위'로 판단하였다.

3) 기준금액 산출

피심인의 위반행위와 관련된 ' ' 서비스의 사업개시( ) 이후 매출액을 연평균 매출액으로 환산한)원에 정보통신망법 시행령 [별표 8] 2. 가. 1)에 따른 '중대한 위반행위'의 부과기준율 1천분의 21을 적용하여 기준금액을 원으로 한다.

<참고 17> 정보통신망법 시행령 [별표 8] 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

'부과기준' 제6조와 제7조에 따라 위반행위의 기간이 2년 이상인( ) '장기 위반행위'에 해당하므로 기준금액에 100분의 50에 해당하는 금액인 원을 가중한 원이나,

최근 3년간 정보통신망법 제64조의3제1항 각 호에 해당하는 행위로 과징금 처분을 받은 사실이 없으므로, 기준금액에 100분의 50에 해당하는 금액인 원을 감경한 원으로 한다.

라. 추가적 가중 및 감경

'부과기준' 제8조에 따라 위반행위의 주도 여부, 위반행위에 대한 조사의 협조 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 추가적 가중·감경할 수 있으나 특별히 가중할 사유는 없으며, 개인정보 유출사실을 자진 신고하고 조사에 협력한 점 등은 인정되나 유출된 개인정보를 이용한

보이스피싱, 가상통화 출금 등 이용자 피해*가 발생한 점 등을 고려하여 추가적 감경하지 않은 금액인 원으로 한다.

* 부터 까지 해킹 신고된 건에 대한 업체 분석 결과, 해킹피해(추정) 건(약 원), 고객IP 차단요청 건, 명의도용 및 보이스피싱 건등임

2. 과징금의 결정

피심인의 정보통신망법 제28조(개인정보의 보호조치) 위반행위에 대한 과징금은 같은 법 제64조의3제1항제6호, 같은 법 시행령 제69조의2 [별표 8] 2. 가. 1)(과징금의 산정기준과 산정절차) 및 '부과기준'에 따라 상기와 같이 단계별로 산출한 금액인 원이나, 최종 과징금 산출액이 1억원 미만에 해당하여 십만원 미만은 절사한 원을 최종 과징금으로 결정한다.

<참고 18> 과징금 산출내역

기준금액	필수적 가중·감경		추가적 가중·감경	최종 과징금*
천원	기준금액의 50% (천원) 가중	천원	가중·감경 없음	천원
	기준금액의 50% (천원) 감경			

* 최종 과징금 산출액이 1억원 이상 10억원 미만에 해당하여 백만원 미만은 절사함

Ⅵ. 징계 권고

피심인이 개인정보 보호와 관련하여 이 법을 위반한 행위가 ①침입차단시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 행위, ③악성프로그램 방지를 위해 백신소프트웨어 등의 보안 프로그램을 업데이트 하지 않은 행위, ④

개인정보가 복사된 외부 저장매체 등 개인정보 출력·복사물을 기록 관리하지 않은 행위 등으로 안전하고 체계적인 개인정보 관리를 위한 정보보호에 대한 투자를 게을리 하여 이용자의 개인정보를 유출한 책임은 피심인의 최고 경영자 등 임원에게 있다.

이에 피심인에 대하여 정보통신망법 제69조의2제2항에 따라 개인정보 유출 및 정보통신망법 위반과 관련하여 피심인의 대표자 및 책임 있는 임원을 포함한 책임자에 대해 징계할 것을 권고한다. 피심인은 이를 존중하여야 하며 그 결과를 방송통신위원회에 통보하여야 한다.

Ⅶ. 과태료 부과

피심인의 정보통신망법 제28조(개인정보의 보호조치)제1항 위반에 대한 과태료는 같은 법 제76조제1항제3호, 같은 법 시행령 제74조의 [별표 9] '과태료의 부과기준' 및 「개인정보보호 의무위반자 과태료 부과 등 처리지침」(이하 '처리지침')에 따라 다음과 같이 부과한다.

1. 기준금액

정보통신망법 시행령 [별표 9]은 최근 3년간 같은 위반행위로 과태료 처분을 받은 경우에 위반 횟수에 따라 기준금액을 달리 적용하도록 규정하고 있고, 이번 피심인의 위반행위는 첫 번째에 해당하여 1회 위반 과태료를 적용한다.

<참고 19> 위반 횟수별 과태료 금액

위반사항	근거법령	위반 횟수별 과태료 금액(만원)		
		1회	2회	3회 이상
너. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조제1항 제3호	1,000	2,000	3,000

2. 과태료의 가중 및 감경

가. 과태료의 가중

처리지침 제9조는 ▲위반행위가 2개 이상인 경우(제1호), ▲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 경우(제2호)에는 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 가중하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 ▲기술적·관리적 보호조치 위반행위는 ①침입차단 시스템 및 침입탐지시스템의 설치·운영을 소홀히 한 행위, ②이용자의 개인정보를 개인정보취급자의 컴퓨터에 저장하면서 암호화하지 않은 행위, ③악성프로그램 방지를 위해 백신소프트웨어 등의 보안 프로그램을 업데이트 하지 않은 행위, ④개인정보가 복사된 외부 저장매체 등 개인정보 출력·복사물을 기록 관리하지 않은 행위 등 위반행위가 2개 이상(제28조제1항제2호·제4호·제5호·제6호)에 해당하므로 기준금액의 50%를 가중한 15,000,000원 부과한다.

나. 과태료의 감경

처리지침 제8조는 ▲위반행위의 결과가 과실에 의한 경우(제1호), ▲위반행위의 결과가 경미한 경우(제2호), ▲위 두 가지 규정에 해당하지 아니하는 경우로서 위반 행위자의 사업 규모, 위반의 동기 등을 고려하여 과태료를 감경 부과할 필요가 있다고 인정되는 경우(제3호)에는 처리지침 제7조에 따른 과태료 금액을 2분의 1까지 감경하여 부과할 수 있다고 규정하고 있다.

이에 의할 때, 피심인의 위반행위의 결과가 ▲개인정보가 포함된 파일의 암호화하지 않고 저장하고, 백신소프트웨어 업데이트를 하여 해커로 인한 개인정보

유출을 방지 할 수 있음에도 이를 게을리 하여 이용자의 개인정보가 유출된 것으로 과실에 의한 경우에 해당한다고 볼 수 없다는 점, ▲위반행위의 결과로 개인정보 유출의 피해규모가 경미하지 않다는 점, ▲기타 위반의 동기 등을 종합적으로 고려할 때, 특별히 과태료 금액을 감경할 만한 사유가 없다.

3. 최종 과태료의 결정

이에 따라, 피심인의 기술적·관리적 보호조치를 하지 않은 행위에 대하여 총 1,500만원의 과태료를 최종적으로 부과한다.

<참고 20> 과태료 산출내역

사업자명	과태료 금액				근거법령	
	기준 금액(A)	가중액 (B)	감경액 (C)	최종액(D) D=(A+B)-C	위반내용	처분근거
(주)	1,000	500	-	**1,500**	§28①2호 §28①4호 §28①5호 §28①6호	§76①3호

<참고 21> 위반행위별 과징금·과태료와 시정명령

위반 유형	과징금	과태료	시정명령	계
기술적·관리적 보호조치 §28①2·4·5·6호	만원	1,500만원	O	만원

Ⅷ. 결론

피심인의 정보통신망법 위반행위에 대하여 같은 법 제64조제4항(시정명령), 제64조의3제1항제6호(과징금), 제76조제1항 제3호(과태료)에 따라 주문과 같이 결정한다.

이의제기 방법 및 기간

피심인은 이 시정명령 및 과징금 부과 처분에 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 과태료 납입 의무를 부담한다.

위 원 장 이 효 성 

부위원장 허 욱 

위 원 김 석 진 

위 원 표 철 수 

위 원 고 삼 석