

보도시점 2025. 7. 4.(금) 14:00
(2025. 7. 5.(토) 조간)

배포 2025. 7. 4.(금) 12:00

SK텔레콤 침해사고 최종 조사결과 발표

[민관합동조사단 조사결과]

- ▷ (조사방식) 국내 1위 통신사의 침해사고, 국민 우려 증가, 악성코드의 은닉성 등을 고려하여 SK텔레콤 전체 서버(42,605대) 대상 점검
- ▷ (감염 현황) 감염서버 총 28대, 악성코드 총 33종 확인 및 조치
※ ①이번 침해사고와 연관성은 없으나 공급망보안 관리 취약으로 악성코드 1종이 SK텔레콤 서버 88대에 유입 확인, ②'22.2월 SK텔레콤에서 악성코드 2종 자체 조치
- ▷ (정보유출 규모) 유심정보 25종 유출(9.82기가바이트<GB>, 가입자 식별번호<IMSI> 기준 2,696만건)
- ▷ (사고 원인 및 문제점) SK텔레콤의 계정정보 관리 부실, 과거 침해사고('22.2월) 대응 미흡, 주요 정보 암호화 조치 미흡 등을 원인으로 파악
- ▷ (재발방지 대책) 계정 비밀번호 관리 강화, 주요 정보 암호화, 정보보호 관리체계(거버넌스) 강화(최고경영자<CEO> 직속), 정보보호 인력·예산 확대 등

[위약금 면제 규정 적용 여부 검토결과]

- ▷ SK텔레콤은 유심정보 보호를 위한 주의의무를 다하지 않았고 관련 법령을 미준수 하였으므로, 이번 침해사고에 과실이 있는 것으로 판단
- ▷ SK텔레콤은 유심정보를 보호하여 이용자에게 안전한 통신서비스를 제공해야 할 사업자의 의무를 다하지 못한 것으로 판단
- ▷ 과기정통부는 SK텔레콤 과실이 발견된 점, SK텔레콤이 계약상 주된 의무를 다하지 못한 점 등 고려 시, 위약금 면제 규정이 적용 가능하다고 판단

과학기술정보통신부(장관 유상임, 이하 “과기정통부”)는 SK텔레콤 침해 사고 민관합동조사단(이하 “조사단”)의 조사 결과 및 SK텔레콤의 이용약관 상 위약금 면제 규정에 대한 검토결과를 7월 4일(금)에 발표하였다.

I. SK텔레콤 침해사고 원인분석 및 재발방지 대책

지난 4.18일 23시 20분, SK텔레콤은 평소 대비 대용량 데이터가 외부로 전송된 정황을 인지하고, 4.20일 16시 46분, 한국인터넷진흥원(원장 이상중)에 침해사고를 신고하였다.

※ 정보통신망법 상 사고인지 시점부터 24시간 이내에 신고를 해야 하며, 이를 위반 시 3천만원 이하 과태료 부과 대상

과기정통부는 SK텔레콤의 유심정보 유출을 중대한 침해사고로 판단하고 4.23일 민관합동조사단을 구성하여 피해현황, 사고원인 등을 조사하였다.

1. 조사 방식

조사단은 이번 SK텔레콤 침해사고가 ①국내 1위 이동통신사의 침해 사고, ②유심정보 유출로 인한 휴대폰 부정 사용 등 국민 우려 증가, ③악성 코드의 은닉성 등을 고려하여 전체 서버 42,605대를 대상으로 BPFDoor 및 타 악성코드 감염여부에 대해 강도 높은 조사(4.23~6.27)를 시행하였다.

또한, 조사 과정에서 확인된 감염서버는 디지털 증거수집(포렌식) 등 정밀 분석을 통해 정보유출 등 피해발생 여부를 파악하였다.

2. 감염서버 및 정보유출 규모

조사단은 이번 침해사고로 공격받은 총 28대 서버에 대한 디지털 증거 수집(포렌식) 분석 결과, BPFDoor 27종을 포함한 악성코드 33종*을 확인하였다.

* BPFDoor 27종, 타이니셀 3종, 웹쉘 1종, 공개 소프트웨어(오픈소스) 악성코드 2종(CrossC2 1종, 슬리버 1종)

확인된 악성코드 정보는 피해확산 방지를 위해 백신사, 경찰청, 국정원 등 주요 민간·공공기관에 공유하고, 악성코드 점검 지침(가이드)을 보호나라 누리집(www.boho.or.kr)을 통해 배포(조회수 : 약 12.9만건, 6.30일 기준)하였다.

유출된 정보는 전화번호, 가입자 식별번호(IMSI*) 등 유심정보 25종이며 유출 규모는 9.82기가 바이트(GB), 가입자 식별번호 기준 약 2,696만건이었다.

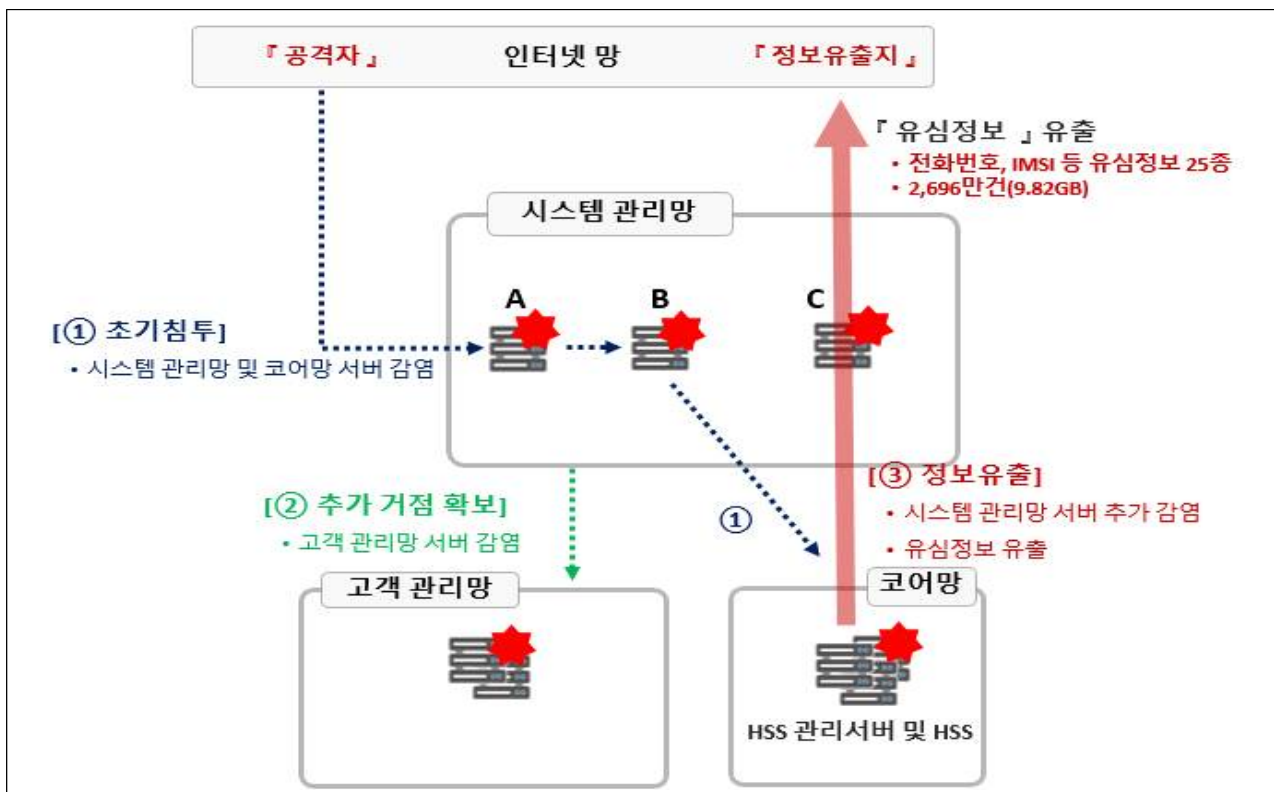
* International Mobile Subscriber Identity : 유심 내 저장되며, 통신사가 사용자 식별 시 사용

한편, 조사단은 감염서버 중 단말기식별번호(IMEI*), 개인정보(이름, 생년월일, 전화번호, 이메일 등)가 평문으로 임시 저장된 서버 2대와 통신기록(CDR**)이 평문으로 임시 저장된 서버 1대를 발견하였으나, 정밀 분석 결과 방화벽 로그 기록이 남아있는 기간(단말기 식별번호<IMEI> : '24.12.3~'25.4.24, 통신기록<CDR> : '24.12.9~ '25.4.20)에는 자료유출 정황이 없는 것을 확인하였다. 다만, 악성코드 감염시점부터 로그기록이 없는 기간(단말기 식별번호<IMEI> : '22.6.15~'24.12.2, 통신기록<CDR> : '23.1.31.~'24.12.8.)에는 유출여부를 확인하는 것이 불가능하였다.

* International Mobile Equipment Identity : 휴대전화 기기 식별 시 사용

** Call Detail Record : 통화 시간, 수발신자 전화번호 등 통신 활동 관련 정보

3. 사고 원인 분석



< 초기 침투('21.8월~) >

공격자는 외부 인터넷 연결 접점이 있는 시스템 관리망 내 서버A에 접속 후 타 서버에 침투하기 위해 원격제어, 백도어 기능 등이 포함된 악성코드(CrossC2)를 '21.8.6일에 설치*하였다.

* 조사 과정에서 확인된 감염서버 중 가장 빠른 시기에 감염

당시 서버A에는 시스템 관리망 내 서버들의 계정 정보(ID, 비밀번호 등)가 평문으로 저장되어 있었으며 공격자는 동 계정정보를 활용해 시스템 관리망 내 타 서버(B)에 접속한 것으로 추정*된다.

* (추정근거) 서버 A에 평문으로 저장된 ID, 비밀번호를 활용해 서버 B에 접속한 로그기록은 남아있지 않으나, 동일한 ID, 비밀번호로 시스템 관리망 내 타 서버에 접속한 기록을 확인하였음

또한, 당시 서버 B에는 코어망 내 음성통화인증(HSS*) 관리서버 계정정보가 평문으로 저장되어 있었으며, 공격자는 동 계정정보를 활용하여 음성통화인증 관리서버에 접속('21.12.24) 후, 음성통화인증 관리서버 및 음성통화인증에 BPFDoor를 설치하였다('21.12.24~'22.1.1).

* Home Subscriber Server

< 추가 거점 확보('22.6월~) >

공격자는 시스템 관리망을 통해 고객 관리망 내 서버에 접속한 것으로 추정*되며, 서버 접속 후, 악성코드(웹셸, BPFDoor)를 설치('22.6.15, 6.22)하였다.

* (추정근거) 조사단은 공격자가 시스템 관리망과 고객 관리망 간 통신한 기록을 확인하였고, 이를 근거로 공격자가 시스템 관리망 내 감염서버에서 고객 관리망으로 접속이 가능한 것으로 판단

< 정보유출('25.4.18일) >

공격자는 초기 침투과정에서 확보한 계정 정보*를 활용하여 시스템 관리망 내 여러 서버에 추가로 악성코드를 설치하였다('23.11.30~'25.4.21).

* SK텔레콤은 시스템 관리망 내 서버의 계정 패스워드를 장기간 미변경(패스워드 만료일이 설정 되어있지 않고, 변경한 이력이 없는 것으로 확인)

이후 공격자는 '25.4.18일 음성통화인증 3개 서버에 저장된 유심정보(9.82기가바이트<GB>)를 시스템 관리망 내 외부 인터넷 연결 접점이 있는 서버 C를 거쳐 유출하였다.

4. 문제점 및 재발방지 대책

조사단은 조사를 통해 SK텔레콤의 정보보호 체계에 문제점을 발견하고 재발방지 대책을 마련하였다.

< 유심정보 유출 관련 문제점 >

악성코드가 감염된 경위 및 침해사고 대처 등과 관련하여 SK텔레콤은 ①계정정보 관리 부실, ②과거 침해사고 대응 미흡, ③주요 정보 암호화 조치 미흡 등 3가지 문제점이 있었다.

① 계정 정보 관리 부실

SK텔레콤은 서버 로그인 ID, 비밀번호를 안전하게 관리*해야 하나 이번 침해사고에서 감염이 확인된 음성통화인증 관리서버('21.12.24, 12.30 감염) 계정정보를 타 서버에 평문으로 저장하였고, 조사단은 공격자가 동 계정정보를 활용해 음성통화인증 관리서버 및 음성통화인증을 감염시킨 것을 확인하였다.

* 종이, 파일, 모바일 기기 등에 비밀번호 기록·저장을 제한하고, 부득이하게 기록·저장하여야 하는 경우 암호화 등의 보호대책 적용(ISMS 인증기준 안내서)

⇒ (재발방지 대책) SK텔레콤은 서버 등에 비밀번호 기록 및 저장을 제한하고 부득이할 경우 암호화하여 저장하는 한편, 서버 접속을 위한 다중인증 체계를 도입해야 한다.

② 과거 침해사고 대응 미흡

SK텔레콤은 '22.2.23일 특정 서버에서 비정상 재부팅이 발생함에 따라 해당 서버 및 연계된 서버들을 점검하는 과정에서 악성코드에 감염된 서버를 발견하여 조치하였으나, 정보통신망 이용촉진 및 정보보호 등에

관한 법률(이하 “정보통신망법”)에 따른 신고 의무*를 이행하지 않았다.

* 당시 정보통신망법 제48조의3에 따라 침해사고가 발생하면 즉시 그 사실을 과기정통부 또는 한국인터넷진흥원에 신고하여야 하며 위반 시 3천만원 이하 과태료 부과 대상

또한, 당시 점검 과정에서 SK텔레콤은 이번 침해사고에서 감염이 확인된 음성통화인증 관리서버(‘21.12.24, 12.30 감염)에 비정상 로그인 시도가 있었던 정황도 발견하여 점검하였으나, 해당 서버에 대한 로그기록 6개 중 1개만 확인하여, 공격자가 서버에 접속한 기록을 확인하지 못하였다.

이로 인해 음성통화인증 관리서버 및 정보유출이 발생한 음성통화인증에서 BPFDoor 악성코드를 확인하지 못하였으며, 또한 침해사고를 신고하지 않아 정부가 조사를 통해 악성코드를 발견하여 조치하는 것도 이루어질 수 없었다.

※ 조사단은 감염서버뿐만 아니라 의심정황이 있는 서버까지 정밀분석(포렌식 등)하여 추가 악성코드 확인·조치

⇒ (재발방지 대책) SK텔레콤은 침해사고 발생 시 법령에 따른 신고의무를 준수하고 철저한 원인 분석을 통해 피해확산 방지 노력을 이행하여야 한다.

③ 주요정보 암호화 조치 미흡

유출 정보 중 유심 복제에 활용될 수 있는 중요한 정보인 유심 인증키(Ki) 값 암호화를 세계이동통신사업자협회(GSMA)는 권고하고 있으며, 타 통신사들(KT, LGU+)도 암호화하여 저장하고 있으나, SK텔레콤은 암호화하지 않고 저장하였다.

※ GSMA(Global System for Mobile Communications Association)

⇒ (재발방지 대책) SK텔레콤은 관계 법령 및 국제 권고에 따라 주요정보를 암호화하여 저장하여야 한다.

< 정보통신망법 위반사항 >

SK텔레콤은 침해사고 대응과정에서 ①침해사고 신고 지연 및 미신고, ②자료보전 명령 위반 등 망법상 준수 의무 2가지를 위반하였다.

① 침해사고 신고 지연 및 미신고

SK텔레콤은 정보통신망법 제48조의3에 따라 침해사고를 인지한 후 24시간 이내*에 과기정통부 또는 한국인터넷진흥원에 신고하여야 하나, 24시간이 지난 후 신고하였다. 또한 악성코드(타이니셀 2종)에 감염된 서버를 발견하고도 침해사고 신고를 하지 않았다.

* '24.8.14일부터 24시간 이내 신고 의무가 시행되었으며, 이전에는 구체적 신고 기한 없이 '즉시' 신고하도록 규정

⇒ (조치사항) 정보통신망법에 따라 과태료를 부과할 예정이다.

※ 정보통신망법 제76조에 따라 3천만원 이하 과태료 부과 대상

② 자료보전 명령 위반

과기정통부는 정보통신망법 제48조의4에 따라 SK텔레콤에 침해사고 원인 분석을 위해 자료 보전을 명령(4.21 17:42)하였으나, SK텔레콤은 서버 2대를 디지털 증거수집(포렌식) 분석이 불가능한 상태로 임의 조치(4.21 19:52) 후 조사단에 제출하였다.

⇒ (조치사항) 자료보전 명령 위반과 관련하여 수사기관에 수사를 의뢰할 예정이다.

※ 정보통신망법 제73조에 따라 자료보전 명령을 위반하여 자료를 보전하지 아니한 자는 2년 이하의 징역 또는 2천만원 이하의 벌금 대상

< 정보보호 활동 및 관리(거버넌스) 체계 미흡 >

조사단은 이번 침해사고 조사 과정에서 SK텔레콤이 ①보안 관리 미흡, ②공급망 보안 소홀 등 기본적인 정보보호 활동이 미흡했던 점과, ③SK텔레콤의 침해사고 대응이 체계적으로 가동되지 않는 사실도 확인하였다.

① 보안 관리 미흡

SK텔레콤은 자체 규정에 따라 연 1회 이상 서버 보안점검을 수행하고 있으나, 쉽게 탐지가 가능한 웹쉘은 점검항목에 포함하지 않아 이를 발견하지 못하였다.

또한, SK텔레콤은 전화번호의 마스킹 규칙이 담긴 정보를 통신기록(CDR)이 임시 저장된 서버에 저장하는 등 마스킹된 정보의 보안관리가 미흡하였다.

⇒ (재발방지 대책) SK텔레콤은 EDR*, 백신 등 보안 해결책(솔루션) 도입 확대, 철통인증(제로트러스트) 도입, 분기별 1회 이상 모든 자산에 대해 보안 취약점 정기 점검 및 제거 등 보안 관리를 강화해야 한다.

* Endpoint Detection and Response : 서버 등 네트워크가 연결되는 장치에서 발생하는 모든 활동을 감지·분석하는 도구

② 공급망 보안 소홀

SK텔레콤은 협력업체로부터 공급받은 소프트웨어를 면밀히 점검하지 않고 내부 서버 88대에 설치하여 해당 소프트웨어에 탑재되어 있었던 악성코드가 유입되었다.

※ 유입된 악성코드가 SK텔레콤 시스템에서 실행된 흔적은 없음

⇒ (재발방지 대책) SK텔레콤은 협력업체 공급 소프트웨어 등 외부 조직 및 서비스로부터 발생하는 위험에 대한 보호대책을 마련하여 이행하는 등 공급망 보안체계를 구축해야 한다.

③ 정보보호 관리(거버넌스) 체계 미흡

SK텔레콤은 정보통신망법 제45조의3 등에 따라 정보보호 최고책임자(CISO)가 정보보호 관련 업무를 총괄하여야 하나, 보안 업무를 정보기술 영역(자산의 57%)과 네트워크 영역(자산의 43%)으로 구분하고 정보보호책임자는 정보통신 영역만 담당하고 있다.

※ SK텔레콤 시스템은 정보기술 영역(업무망, 고객관리망 등)과 네트워크 영역(시스템 관리망, 핵심망<코어망> 등)으로 구분

⇒ (재발방지 대책) SK텔레콤은 정보보호 최고책임자가 전사 정보보호 정책을 총괄 관리할 수 있도록 정보보호 최고책임자를 최고경영자 직속 조직으로 강화하여야 한다.

< 기타 개선 필요사항 >

① 로그기록 단기 보관

SK텔레콤은 자체 보안규정에 따라 로그기록을 6개월 이상 보관해야 하나, SK텔레콤은 실제 운영 시 방화벽 로그를 4개월간만 보관 중이었다. 이로 인해 조사단이 중요 정보의 유출 여부를 면밀히 조사하는 데 한계가 있었다.

⇒ (재발방지 대책) 방화벽 로그기록을 6개월 이상 보관하고, 중앙로그관리 시스템을 구축하여 주기적인 점검과 사고 발생 시 분석에 적극 활용하여야 한다.

② 자산 식별의 어려움

조사단이 SK텔레콤 서버 전체 대상으로 점검 시, 전체 자산 종류, 규모, 유희·폐기 여부 등을 체계적으로 관리되고 있지 않음을 확인하였다.

⇒ (재발방지 대책) 전사 자산을 담당하는 정보기술 최고책임자(CIO)를 신설하고, 정보기술 자산관리 해결책(IT자산관리 솔루션)을 도입하여야 한다.

③ 타사 대비 정보보호 인력 및 투자 규모 부족

'24년도 정보보호 공시 기준 SK텔레콤의 가입자 100만명당 정보보호 인력은 15명, 투자액 37.9억 원(SKB 포함)으로 통신사 평균 대비 그 규모*가 작았다.

* 가입자 100만명 당 정보보호 인력(명) : SK텔레콤/SKB(15.0), KT(25.1), LGU+(14.3), 평균(17.7)
가입자 100만명 당 정보보호 투자액(억원) : SK텔레콤/SKB(37.9), KT(90.8), LGU+(57.5), 평균(57.4)

⇒ (재발방지 대책) SK텔레콤은 정보보호 강화에 필요한 인력 및 예산 규모를 타 통신사 이상의 수준(가입자 당 기준)으로 확대해야 한다.

5. 향후 계획

과기정통부는 SK텔레콤에 재발방지 대책에 따른 이행계획을 제출(7월)토록 하고 SK텔레콤의 이행(8~10월) 여부를 점검(11~12월)할 계획이다. 이행점검 결과, 보완이 필요한 사항이 발생하는 경우 정보통신망법 제48조의4에 따라 시정조치를 명령할 계획이다.

또한, 과기정통부는 인공지능 시대 국가 사이버보안 역량을 강화하지 않으면 큰 피해가 우려되는 상황에서 SK텔레콤 침해사고를 계기로 민간 분야 정보보호 전반의 체계를 개편할 계기가 되었다고 판단하였다.

이에 국민, 산업에 미치는 영향이 큰 통신망을 안전하게 보호하기 위한 별도의 법제도 방안, 민간 정보보호 투자 확대 및 정보보호 관리체계(거버넌스) 강화 등을 위한 제도 개선 방안 등을 국회 과학기술정보방송통신위원회 내 SK텔레콤 해킹사고 관련 전담조직(TF)과 논의를 거쳐 마련할 계획이다.

II. SK텔레콤 이용약관 상 위약금 면제 규정 적용 여부

1. 위약금 면제 규정 개요

SK텔레콤 이용약관은 '회사의 귀책 사유'로 이용자가 서비스를 해지할 경우, 위약금을 면제하도록 규정하고 있다.

< SK텔레콤 이용약관 제43조 (위약금 면제) >

- ① 다음 각호의 경우에는 제 42 조 제1항에 의한 위약금 납부 의무가 면제됩니다.
4. 회사의 귀책 사유로 인해 해지할 경우

2. 법률 자문 결과

SK텔레콤 침해사고 후 국회 청문회(5.8일), 언론 등에서 침해사고로 인해 이용자가 약정 기간 중에 해지할 경우 위약금을 면제해야 한다는 주장과 논란이 있었으며, 과기정통부는 SK텔레콤 이용약관상 위약금 면제 규정 적용 여부 검토를 위해 법률 자문을 진행하였다.

과기정통부는 사고 초기에 SK텔레콤 이용약관의 위약금 면제 규정을 동 침해사고에 적용 가능한지에 대해 법률 자문(4개 기관)을 받았으며, 당시 법률 자문기관들은 이번 침해사고 조사결과에서 SK텔레콤의 과실이 인정된다면 이용자가 계약 해지 시 위약금 면제 규정 적용이 가능하다는 공통된 의견을 제시하였다. 다만, 조사결과에 대한 구체적인 정보 없이 검토가 이루어진 한계가 있었다.

이후, 과기정통부는 조사단의 조사가 마무리되는 시점에 보다 정확한 판단을

위해 조사결과를 바탕으로 추가적인 법률 자문(5개 기관, 6.26일~7.2일)을 진행하였으며, 대부분 법률 자문기관(4개 기관)에서는 이번 침해사고를 SK텔레콤의 과실로 판단했고 유심정보 유출은 안전한 통신서비스 제공이라는 계약의 주요 의무 위반이므로, 위약금 면제 규정 적용이 가능하다는 의견을 제시하였다. 법률 자문기관 한 곳은 현재 자료로 판단이 어렵다고 판단을 유보하였다.

3. 주요 검토 내용 및 결과

과기정통부는 이번 침해사고로 이용자가 계약 해지 시, 위약금이 면제되는 SK텔레콤의 이용약관상 ‘회사의 귀책 사유’에 해당하는지에 대해 ① 침해 사고에서 SK텔레콤 과실 여부, ② 이용자에게 통신서비스를 제공(계약상) 하는데 있어 주된 의무를 위반하였는지 여부를 중점적으로 판단하였다.

① 침해사고에서 SK텔레콤의 과실

조사단의 조사결과에 따르면, 이번 침해사고와 관련하여 SK텔레콤에 ① 계정정보 관리 부실, ② 과거 침해사고 대응 미흡, ③ 중요 정보 암호화 조치 미흡 등의 문제점이 있었으며, 이 과정에서 SK텔레콤이 정보통신방법을 위반한 사실도 확인되었다.

따라서, SK텔레콤은 안전한 통신서비스 제공을 위한 유심정보 보호와 관련하여 일반적으로 기대되는 사업자의 주의의무를 다하지 못했을 뿐만 아니라 관련 법령이 정한 기준을 미준수하였으므로, 과기정통부는 이번 침해사고에서 SK텔레콤의 과실이 있는 것으로 판단하였다.

② 통신서비스 제공(계약상)에 있어 주된 의무 위반 여부

과기정통부는 법률 자문기관이 제시한 법리를 토대로 SK텔레콤의 입장, 침해사고로 인한 결과의 중대성 등을 종합적으로 검토하여 판단하였다.

정보통신망법상 통신 사업자에게는 안전한 통신서비스를 제공할 의무가 있으며, 국민 일상생활 전반이 통신서비스를 기반으로 이뤄지고 있는 점을 고려할 때 이용자는 사업자가 안전한 통신서비스 제공을 위한 적절한 보호조치를 할 것으로 기대할 수 있다. 따라서 안전한 통신서비스 제공은 통신사업자와 이용자 간 계약에서 중요한 요소로 볼 수 있다.

이번 침해사고로 유출된 유심정보는 이동통신망에 접속하고, 안전하고

신뢰할 수 있는 통신서비스를 위한 필수적인 요소이다. 유심정보의 유출은 다른 보호조치가 없다면 제3자가 유심 복제를 통해 이용자의 전화번호로 통신서비스를 이용하거나, 이용자에게 걸려온 전화문자를 제3자가 가로챌 수 있는 위험한 상황을 초래할 수 있다.

정보유출 당시 SK텔레콤은 유심정보 보호를 위해 부정사용방지시스템(FDS, Fraud Detection System) 1.0('23.8월~)과 유심보호서비스('23.11월~)를 운영 중이었으나, 유심보호서비스에는 약 5만명만 가입한 상태였으며, 부정사용방지시스템 1.0은 유심정보 유출로 인한 모든 유심복제 가능성을 차단하는 데는 한계가 있었던 상황이었다. 따라서, 과기정통부는 SK텔레콤이 유심정보를 침해사고로부터 보호해서 안전한 통신서비스를 제공(주된 채무)할 의무를 다하지 못한 것으로 판단하였다.

결론적으로, 과기정통부는 ①이번 침해사고에서 SK텔레콤의 과실이 발견된 점, ②SK텔레콤이 계약상 주된 의무인 안전한 통신서비스 제공 의무를 다하지 못한 점 등을 고려할 때, 이번 침해사고는 SK텔레콤 이용약관 제43조상 위약금을 면제해야 하는 회사의 귀책사유에 해당한다고 판단하였다.

다만, 과기정통부는 이러한 판단은 SK텔레콤 약관과 이번 침해사고에 한정되며, 모든 사이버 침해사고가 약관상 위약금 면제에 해당한다는 일반적인 해석이 아님을 명확히 하였다.

유상임 과기정통부 장관은 “이번 SK텔레콤 침해사고는 국내 통신 업계뿐만 아니라 네트워크 기반 전반의 정보보호에 경종을 울리는 사고였다.”면서, “SK텔레콤은 국내 1위 이동통신 사업자로 국민 생활에 큰 영향을 미치는 만큼 이번 사고를 계기로 확인된 취약점을 철저히 조치하고 향후 정보보호를 기업 경영의 최우선 순위로 두어야 할 것”이라고 말하였다.

이와 함께, “다가올 인공지능 시대에는 사이버위협이 인공지능과 결합하여 더욱 지능화, 정교화될 것으로 예상되는 만큼 정부는 사이버 위협 예방부터 사고 대응까지 전반적인 보안 체계를 개편하여 안전하고 신뢰받는 인공지능 강국으로 도약할 수 있도록 지원하겠다.” 고 밝혔다.

담당 부서 <조사결과>	과학기술정보통신부 사이버침해대응과	책임자	과장	최광기 (044-202-6460)
		담당자	사무관	김성환 (044-202-6461)
			사무관	이웅비 (044-202-6425)
담당 부서 <위약금>	과학기술정보통신부 통신이용제도과	책임자	과장	신대식 (044-202-6650)
		담당자	사무관	구희선 (044-202-6626)
관련 기관	한국인터넷진흥원 위협분석단	책임자	단장	박용규 (02-405-6620)
		담당자	팀장	김홍석 (02-405-4830)

내일을 만드는 과학기술
내일을 채우는 디지털·AI

대한민국
지책브리핑

