A통신사 ,<과징금 1,347억 9,100만 원> 부과 사유 및 재발 방지 대책

1. 안전조치 의무 위반 및 유출 통지 위반으로
<과징금 1,347억 9,100만 원>, <과태료 960만 원> 부과

2. 2,300여만 명의 주요 디지털 개인정보 유출

- 이동통신 관련 핵심 네트워크 시스템에 대한 관리 소홀로 LTE·5G 서비스 **전체 이용자 23,244,649명***(알뜰폰 포함, 중복 제거)의 **휴대전화번호, 가입자식별번호(IMSI), 유심 인증키 (Ki, OPc) 등 25종의 정보**가 유출

3. 21년 최초 침투, 25년 개인정보 유출

21년 8월: 최초 침투

A통신사 내부망에 해커 최초 침투, 다수 서버에 악성프로그램 설치

22년 6월: 추가거점 확보

ICAS(통합고객인증시스템) 내 악성프로그램 추가 설치,
추가 거점 확보

25년 4월 18일~: 개인정보 유출

HSS(홈가입자서버) DB에 저장된 이용자의
개인정보 (9.82GB) 외부 유출

4. 9월 초, 대규모 개인정보 처리자 대상
'개인정보 안전관리체계 강화 종합 대책' 발표 예정

1. 기술적 보호조치 위반 사항
: 안전성 확보 조치 고시 위반 사항

위반 사항 1) 접근통제조치 소홀

- **시스템망·고객 관리망·코어망 미흡한 분리운영**
  불필요한 상호접속 허용, HSS DB 내 유심정보 탈취

- 22년 2월 이상행위 로그 탐지되었으나
  비정상 통신 여부, 추가적인 악성프로그램 설치 여부,
  접근 통제 정책의 적절성 등 미확인하여
  유출 사고 사전 방지 대응 소홀

위반 사항 2) 접근권한 관리 소홀

- 사내 2,365개 **서버 계정정보(ID/비밀번호 약 4,899개)가**
  저장된 파일을 관리망 서버에 미암호화 상태로 관리

- HSS 서버도 **별도 인증절차 없이** 계정정보만으로도
  개인정보 조회 가능하도록 운영

1. 기술적 보호조치 위반 사항
: 안전성 확보 조치 고시 위반 사항

위반 사항 3) 보안 업데이트 미조치

- **OS 보안 업데이트 미설치**

  ① 16년 10월: **OS 보안 취약점(DirtyCow) 보안 경보 발령 및 패치 공개**

  ② 16년 11월: 이를 인지한 상태로 **보안 취약점 발견된 OS 설치**

  ③ 해커는 **OS 보안 취약점 활용**하여 **악성프로그램 (BPFDoor) 설치**

  ④ 25년 4월: 유출 시점까지 **OS 보안 업데이트 미실시**

- **백신 프로그램 미설치**

  ① 20년도부터 각종 상용 백신 프로그램에서 해당 취약점 실행 탐지하고 있었으나, **25년 4월까지 백신 프로그램 미설치**

1. 기술적 보호조치 위반 사항
: 안전성 확보 조치 고시 위반 사항

위반 사항 4) 유심 인증키 미암호화, 평문 저장

- **유심인증키(Ki) 2,614만건 미암호화, 평문으로 HSS DB등에 저장**, 해커가 원본 그대로 확보
- 타 통신사 암호화(L사는 '11~, K사는 '14~부터 암호화) 확인하였음에도 미조치하여 유출 피해 예방 실패

위반 사항 5) 이외 미비 사항

- **내부 관리계획 수립/시행 및 점검 소홀, 접속기록 미보관** 등 안전조치의무를 미준수

2. 개인정보 책임자 업무수행 소홀 및 유출통지 지연

1) CPO 역할 미흡

- 개인정보 보호책임자(CPO)는
  IT영역에 한정되도록 구성 및 운영
- 유출사고 발생한 **인프라 영역**은 CPO가
  개인정보 처리 실태조차 파악하지 못하는 등
  관리감독 공백 상태

2) 개인정보 유출통지 지연

- 25년 4월 19일 유출 인지하였으나
  법령에서 정한 **72시간 내 통지의무 불이행**
  (* 25년 7월 28일 유출 확정 통지)

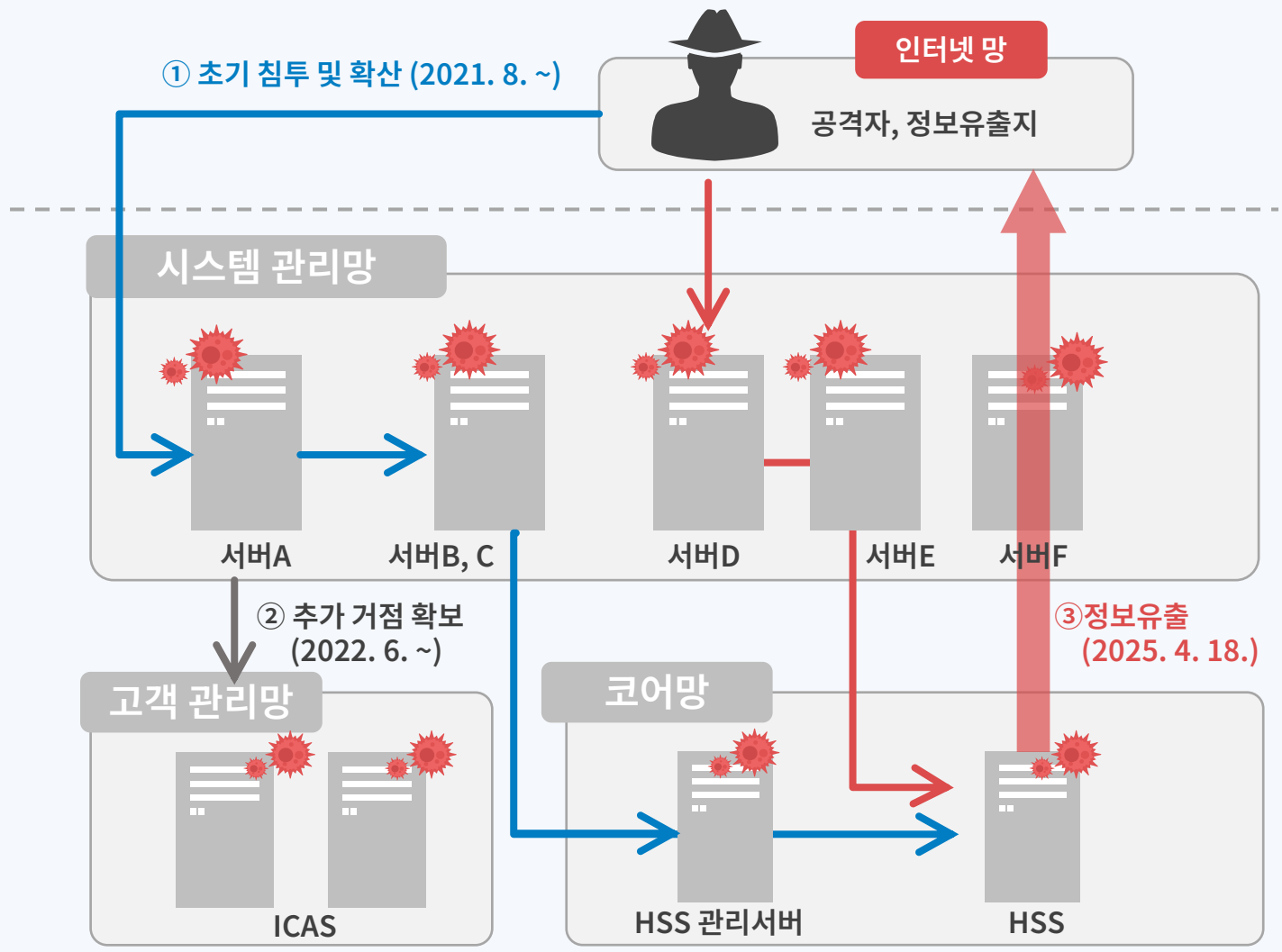
3. 재발 방지 대책: 기술적 보호조치

위반사항	재발 방지 대책	대책 예시
접근통제 정책소홀	• 시스템망, 고객관리망, 코어망 간 **논리적/물리적 망분리**	논리적 망분리 VD-i
접근권한 관리소홀	• DBMS 및 주요서버 접근통제, 계정관리 및 접속 기록 보관 **DB/서버 접근제어 솔루션**	DB/서버 접근제어 DB-i **서버접근통제 서버계정관리 솔루션**
	• 서버 내 무단 보관된 계정/인증 정보 검출 및 삭제 **서버 DLP 솔루션**	서버 DLP Server-i
보안 업데이트 미조치	• OS 취약점 점검 및 패치 주요 정보통신기반시설 취약점 점검 **서버 취약점 점검 솔루션**	서버 취약점 점검 Server-i
	• 서버 백신 설치	**서버 백신 솔루션**
유심 인증키 미암호화	• DBMS 및 주요서버 내 무단 방치된 개인정보 검출 및 삭제, 암호화 **서버 DLP 솔루션**	서버 DLP Server-i **DB 암호화 솔루션**

* 그 외: **개인정보보호관리체계 (ISMS-P) 인증 범위**를 **통신 이동통신 네트워크 시스템으로 확대**

4. 별첨: 상세 개인정보 유출 경위

악성프로그램 감염 및 개인정보 유출 경위



4. 별첨: 상세 개인정보 유출 경위

1) 초기침투 (2021.08.06.)

- 해커가 인터넷 연결된 **관리망 서버에 원격제어 프로그램 설치**
- **평문 저장된 계정정보(2,365서버, 4,899개) 탈취**하여 **코어망 서버 침투**
- 코어망 서버 운영OS **DirtyCow 취약점으로** 관리자 권한 획득 후 HSS DB에 **악성코드(BPFDoor) 설치**

2) 추가거점 확보 (2022.06.15.)

- ICAS 내 서버 2대 침투
- 초기침투와 동일한 **OS 취약점** 활용해 **관리자 권한 획득 및 BPFDoor 등 악성코드 설치**

3) HSS 서버 개인정보 유출 (2025.04.18.)

- 이미 설치된 BPFDoor 악성코드 통해 HSS DB에 명령어 입력하여 **개인정보 조회 · 파일 추출 · 압축 후 외부 유출**

* 감염된 ICAS 서버는 방화벽 로그 기록을 4개월만 보관하여 '24.12~'25.4 구간만 확인 가능, 해당 기간 유출 흔적은 없으나 '22.6~'24.12 기간 동안의 유출 여부는 확인 불가

5. 참고자료

해킹 사태' SKT 과징금 1천348억…역대 최대규모
https://biz.sbs.co.kr/article/20000255894?division=NAVER

[Privacy Report] BPFDoor 악성코드 분석 보고서
https://www.somansa.com/ko/security-report/security-note/2025-bpfdoor/

체계적인 기술적 관리적 보호조치 방안구축은
소만사 프라이버시 컨설팅을 통해 구현하실 수 있습니다
consulting@somansa.com

SOMANSA