PEOPLE.
TECHNOLOGY.

침해사고 대응절차 및 사후관리대책

2021

kt ds

I. 침해사고 통지내용 및 방법과 사전대응

1. 침해사고 통지내용 및 방법

- 클라우드 서비스 침해사고가 발생한 것으로 확인된 때에는 정당한 사유 없는 한 5일 이내에 다음 사항을 알려야 한다.
  1) 유출된 개인정보 항목
  2) 유출된 시점과 경위
  3) 피해 확산 방지 초치 현황 및 피해 구제절차
- 클라우드 서비스 침해사고 중 이용자 정보침해, 사전통보 없이 장애발생시 사용자 대상으로 전화, 휴대전화, 전자우편, 문자메시지, 클라우드서비스 접속화면 게시등 이와 같은 방법 중 어느 하나 이상의 방법으로 진행하며, 다만, 클라우드 서비스 접속화면을 통하여 알리는 경우에는 15일 이상 게시 한다.
- 천재지변이나 그 밖의 불가피한 사유로 통지가 곤란한 경우 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고로 갈음 한다

2. 사전 대응

- 국내최고사업자인 KT ds Cloud의 노하우 기반의 공공기관전용 보안클라우드 구축
- 공공기관전용의 사용자청약인증 (G-Cloud 전용포털)
- 물리적으로 분리된 공공전용시스템 구축
- 이용기관별 네트워크 가상화 분리 클라우드 서비스
- H/W 기반 침입탐지(IPS) 및 Firewall 기본제공 과 보안매니지드제공

3. 침해사고시 대응

- 행정공공기관 민간 클라우드 이용 가이드라인을 준수하여 구축 및 운영

  → URL : https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=75072

I. 침해사고 통지내용 및 방법과 사전대응

4. 침해사고 통지 메일 내용 및 폼

안녕하십니까. KT ds 입니다.

아래와 같이 KOS에 저장되어 있는 암호화된 회원님의 결제정보(암호화된 카드번호, 암호화된 이름)가 유출 되었음을

안내 드리며, 깊은 사과 드립니다.

KOS 는 KT ds 고객 정보를 관리 하는 시스템으로 데이터가 저장된 위치는 국내 전산센터 입니다.

20xx 년 x월 xx일부터 x월 xx일 사이 KOS 시스템이 사이버공격을 받아 시스템에 저장 되어 있던 회원님의 결제정보(암호화된 카드번호, 암호화된 이름)가 유출 되었습니다.

KOS 에서 사고 인지 후 전문가와 협력하여 사이버 공격을 차단했으며, 원인 분석 등을 진행 하고 있습니다.

유출된 카드의 카드발행사와 공조하여 2차 피해 예방을 위한 보호조치를 완료 하였습니다.

유출된 카드 정보는 안전하게 암호화 되어 있으며, 카드사 FDS(이상 금융거래 시스템)을 통해 부정 결제를 예방하고 관리 될 수 있도록 조치되어 부정 결제가 발생할 가능성이 매우 낮습니다만, 회원님의 카드 유출 여부를 아래 보안센터로 연락하여 확인해 주시고, 혹시 모를 도용 예방을 위해 카드 재발급 또는 결제 알림서비스 가입을 당부 드립니다.

개인정보 악용으로 의심되는 전화, 문자메시지 등을 받으시거나 기타 궁금하신 사항은 아래 피해 접수 담당 부서로 연락해 주시면 친절하게 안내 드리고 신속하게 대응하도록 하겠습니다.

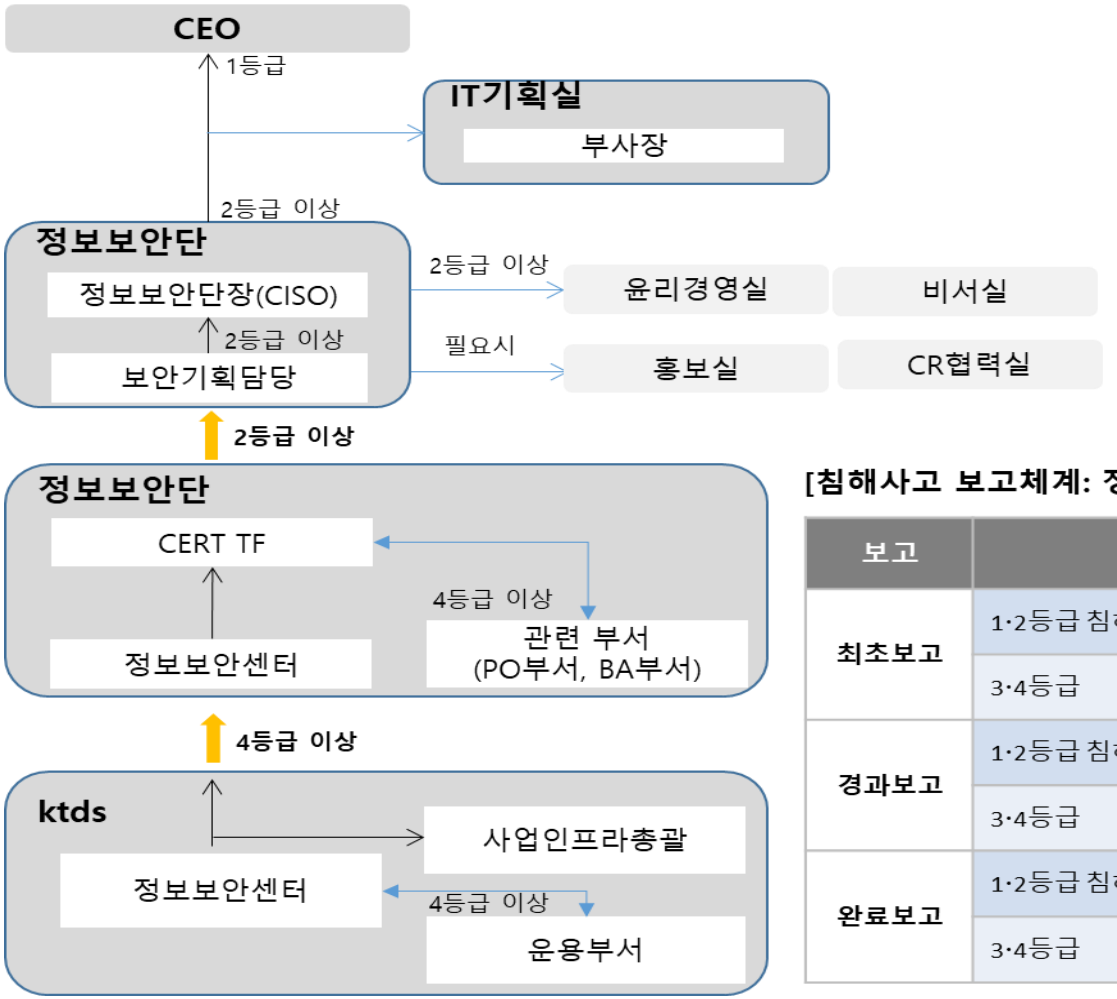
- 피해 접수 담당 부서 : 침해대응센터 (운영시간 24시간)
- 침해대응센터 : 02-3679-9981
- 이메일 : ktds-cloud@kt.com
- 한국인터넷진흥원: 국번 없이 118

KT ds 믿고 이용해 주신 회원님께 심려를 끼쳐드린 점에 대해 진심으로 사과 드리며, 앞으로 개인정보보호에 더욱 만전을 기할 것을 약속 드립니다.

II. 침해사고 대응절차 및 사후관리 대책

1) 침해사고 원인분석 및 대응절차

가. 보고체계



[침해사고 보고체계: 정보보안센터 → 정보보안단]

보고	대상	시기
최초보고	1·2등급 침해사고	발생 즉시
	3·4등급	발생 즉시
경과보고	1·2등급 침해사고	1일 4회
	3·4등급	매일
완료보고	1·2등급 침해사고	최종 완료 시
	3·4등급	최종 완료 시

II. 침해사고 대응절차 및 사후관리 대책

나. 조직 구성

단위보안장비 운영	사이버보안센터	KT ds ds

정보보안센터
- 센터장 : 김동욱

보안기획담당
- 담당 : 홍원규

네트워크인프라팀
- 팀장 : 정인업
- 방화벽 : 최규환, 양원모, 이민욱
- 네트워크 : 김성찬, 김두희, 박형규, 하년홍
- DNS : 김두희, 조순호

보안침해대응팀
- 팀장 : 손원일
- InBound 분석 : 조명기
- OutBound 분석/apt/스플렁크 : 이우승
- SSLVA/ESM/포렌식 운영 : 정진영,유정훈
- 스플렁크 운영 : 송정훈
- 그룹사 관제 : 박상욱
- 보안관제 1선 : 박지원,정귀용,오광렬
- IPS/WAF 운영 : 인창일
- IMO/융합기술원 관제 대응 : 이호승
- 블루코트/N-DLP : 정준식

CERT TF
- 팀장 : 김현신
- 사내IT/CDC/SDSC : 이윤오

보안운영팀
- 팀장 : 정승우
- V3(윈도우) : 남시휴
- 웹쉘/V3(리눅스) : 권도현

EPC 사업수행팀
- 팀장 : 최문종
- 운영 : 장영권, 전재일

보안관제
- WINS : 김정모 포함 19명

도메인보안담당자 (KT ds ds ds)

팀정보보호담당자

※ **통합고객 :** 마이올레, 올레멤버십, 올레샵, 올레샵 전략단말, 스마트명세서, 온라인신청서, 스마트신청서, 통합로열티, BSS-CRM, BSS-PRM

※ **OSS :** 기업고객지원, NeOSS시설관리, NeOSS개통, 개통AS, OSS-OM현장작업, OSS-OM 개통관리, OSS-OM 포털

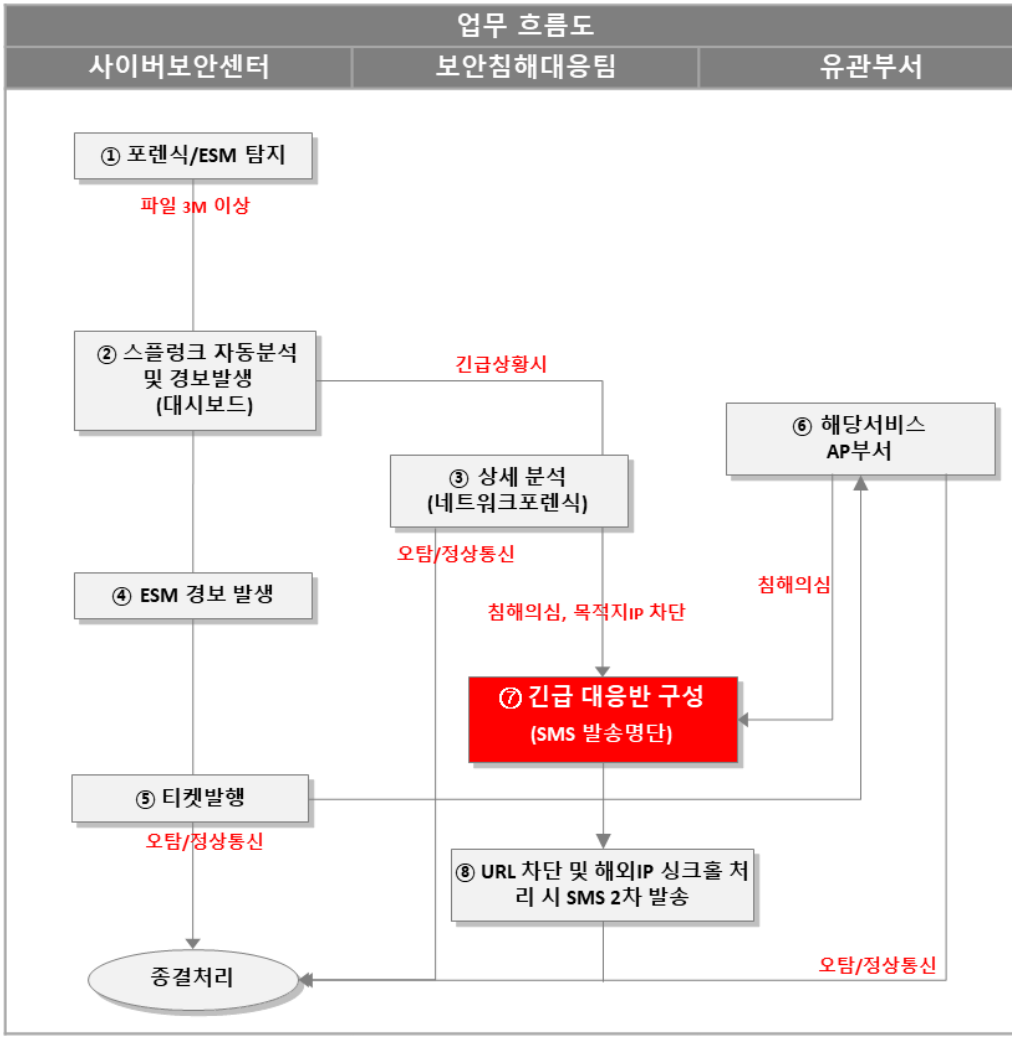
※ **유선BSS :** A4S, i115전보, 나라사랑카드, 수수료통합결제, KT ds ds카드영업, 통화사실제공, 고객정보자산화, 캠페인관리

※ **무선BSS :** 대리점경영지원, 고객신청서스캔, PDF명세서, 멤버쉽인증, 개인정보이용내역열람/통지, MVNE플랫폼, MVNO-사이버명세서, 사이버/모바일청구서,

※ **sDSC :** CASS, KHUB, MMSC, NFC비즈홀, PSSO, SILK, 검색컨텐츠, 모카, 본인확인, 상품권, 아이서치, 올레마켓, 완전자유존

II. 침해사고 대응절차 및 사후관리 대책

다. 원인 분석 및 차단 플로우



세부업무 절차

① 탐지 : 네트워크 포렌식 / ESM / 스플렁크 탐지
- 포렌식 : 확장자(xls/xlsx/csv/txt/zip/gzip/tar/rar) 탐지
- ESM : 1) 3M/10,000패킷 이상 ICMP Outbound 탐지
  2) 20회/1분 OR Request >=10 이상
  private information leakage 탐지
- 스플렁크 : 15초 동안 2M 이상 탐지

② 스플렁크 메타데이터 연동 및 경보발생 or ESM 경보발생
- 실시간 자동 이메일 발송 or ESM 경보
- 컨콜/SMS

③ 상세 분석(네트워크포렌식)
- 사이버보안센터(수시)
- 보안침해대응팀 CERT파트(긴급상황시)
- 정보유출시 신속(20분내) 목적지IP 차단

④ ESM 경보 발생
- 출발지IP / 목적지IP / 목적지PORT 정보 파악

⑤ 티켓발행
- 30분내 (출발지IP AP부서 담당자 즉시 확인 가능시)
- 1시간내 (출발지IP AP부서 담당자 확인 지연시)

⑥ 해당서비스 AP부서 확인

⑦ 긴급대응반 구성 (SMS 발송명단)
- 이상 징후가 포착 및 중요 시스템 침해가 의심되는 경우 긴급 대응반 구성
- 초동보고서 : 긴급대응반 구성 후 2시간 이내
- 최종보고서 : 종결처리 후 24시간 이내 (개선사항 포함)

⑧ SMS 2차 공유
- URL 차단 및 해외IP 싱크홀 처리 시 SMS 2차 발송

II. 침해사고 대응절차 및 사후관리 대책

라. 재발방지를 위한 분야별 점검

순번	점검 항목	관리 현황
1	외부자 계약 시 보안요구사항 명시	계약 및 협정서 상에 보안요구사항 명시 요청 시 협의 후 수용 가능함
2	계약 시 명시된 보안요구사항 이행관리	계약 시 명시된 보안요구사항에 대한 이행자료 제공 가능(정보보호서약서 등)
3	외부자 대상 연1회 이상 교육 시행	KT가 자체 정보보호교육계획에 의거하여 연2회 이상 보안교육을 시행하고 있음
4	정보시스템에 대한 접근 통제 절차 이행	고객의 서비스영역에 설치한 보안시스템의 사용자 계정 등록 및 접근권한 등록·변경·삭제는 작업관리시스템(ITSM)을 통해 수행하며 시스템화된 SOP의 절차를 따르고 있음, 퇴직자는 퇴직신청 시 처리 과정에서 계정을 확인하여 삭제하고 있음
5	정보시스템의 관리자 권한에 대한 접근통제 절차 이행	특수권한을 포함한 모든 계정은 작업관리시스템(ITSM)을 통해 생성되며 ITSM의 SOP에 따라 승인과정을 거침. 분기 1회 접근권한에 대한 타당성을 검토하고 있음
6	정보시스템에 대한 접근통제 방안	정보시스템에 대한 접근은 접근통제시스템(KTACS)을 통해 통제하고 있으며 KTACS에서 5회 인증 실패 시 접속을 차단함. 접속 시 사용자의 ID, Password, PC의 MAC+OTP의 다중인증을 받도록 하고 있음
7	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자 할당	접근제어시스템(KTACS)과 인사시스템을 연동하여 1인 1계정 사용 정책으로 계정을 부여함
8	정보시스템 및 웹서비스의 계정 및 패스워드 관리절차 수립▪이행	포탈의 이용자 패스워드는 안전한 일방향 암호화 알고리즘(SHA-256)을 적용하고 있으며 3가지 문자 조합으로 8~15자로 입력하여야 함
9	네트워크 영역의 분리 및 접근통제	서비스 네트워크와 운용망 네트워크는 물리적으로 분리되어 있으며 고객서비스를 위한 방화벽 자체로의 접근은 운영자PC만 접근하도록 접근을 제한함

II. 침해사고 대응절차 및 사후관리 대책

마. 재발방지를 위한 모의훈련

구분	주요 내용
훈련 대상	ㅇ 개인 정보를 대량으로 보유하고 있는 사이트 ㅇ 외부에서 접속 가능한 사이트
훈련 시기	ㅇ 연중 2회 이상
훈련 항목	ㅇ DDoS 공격 ㅇ SQL Injeciton 공격 ㅇ XSS 공격 ㅇ 포트, 웹스캔 공격 ㅇ 파일 업로드/다운로드 공격 ㅇ ID/PW 무작위 대입 공격 등

PEOPLE. TECHNOLOGY. kt ds