개인정보보호 및 정보보안교육

SW공급망과 정보보안 관리체계

New

진짜

CONTENTS

- NEW 이슈 탐방

1 우리 곁에서 일어나는 SW 공급망 보안 사고

2 SBOM, SW를 분해해 본다?

3 나도 공급망 보안을 위해 할 일이 있다고?

4 정보보안 정책, 지침, 프로세스

- SMART 시큐의 노트

NEW 이슈 탐방

클라우드서비스 중단

- 2024.7.19 의료, 공항, 항공, 여행, 방송사, 이동통신 등 세계 곳곳의 많은 서비스에서 중단 또는 장애가 발생함
- 미국, 독일, 영국, 프랑스, 인도, 호주 등 세계 곳곳에서 다양한 서비스의 장애가 발생하였음
- 장애가 발생한 서비스의 공통점은 세계 클라우드 시장점유율 2위인 MS의 클라우드 서비스 애저(Azure)를 사용하는 서비스였음

NEW 이슈 탐방

원인과 장애

- 팔콘 오류 → 팔콘이 실행된 약 850만 대 윈도 시스템(PC, 서버) 비정상 종료 → MS 애저 중단/장애 → 항공사, 여행사 등의 서비스 중단/장애 → 이용자
- 국내에서는 팔콘이나 MS 클라우드 서비스 이용자가 적어서 피해가 크지 않았음

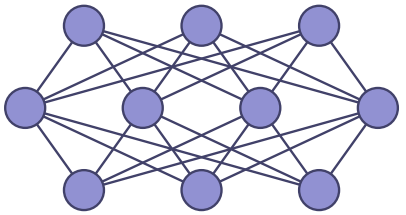
시사점

- 세계가 SW로 촘촘히 연결되어 있음
- SW 공급망에 포함된 구성 요소의 장애는 실시간으로 예측할 수 없을 정도로 광범위하게 확산할 수 있음
- 최종 이용자도 실시간으로 피해를 당함
  - ✓ HW에서는 부품의 결함이 발생하면, 부품 구매처를 찾아서 리콜 수행
- 이 사건은, SW공급망 관리, 그중에서도 SW품질관리의 중요성을 일깨워줌
- HW공급망 관리는 이미 1980년 대 초반부터 경영의 중요한 일부로 다뤄져 왔으나, SW공급망 관리는 중요성이 부각된 지 그리 오래 되지 않음

01 우리 곁에서 일어나는 SW 공급망 보안 사고

공급망 vs. 공급사슬

- 공급망은 Supply-chain의 우리말 번역인데, 정확한 번역은 '공급 사슬'임.
  - ✓ 먹이 사슬(Food chain)의 '사슬'을 생각하면 됨
  - ✓ 공급 사슬은 공급 관계에서 '선-후' 또는 '공급하는 자'와 '공급받는 자' 사이의 관계가 명확하고, '사슬'의 한 부분에서 발생한 품질 문제나 보안 취약점이 사슬을 타고 최종 SW나 서비스까지 한 방향으로 이어지는 어감임. 이러한 어감을 '망' 또는 '네트워크'가 주지 못함
- 이미 공급망이란 표현이 대중화되어 있어서 여기서도 '공급망'이란 표현을 씀. '공급망'이라고 쓰고, **'공급 사슬'**을 생각하면 이해하기 쉬움

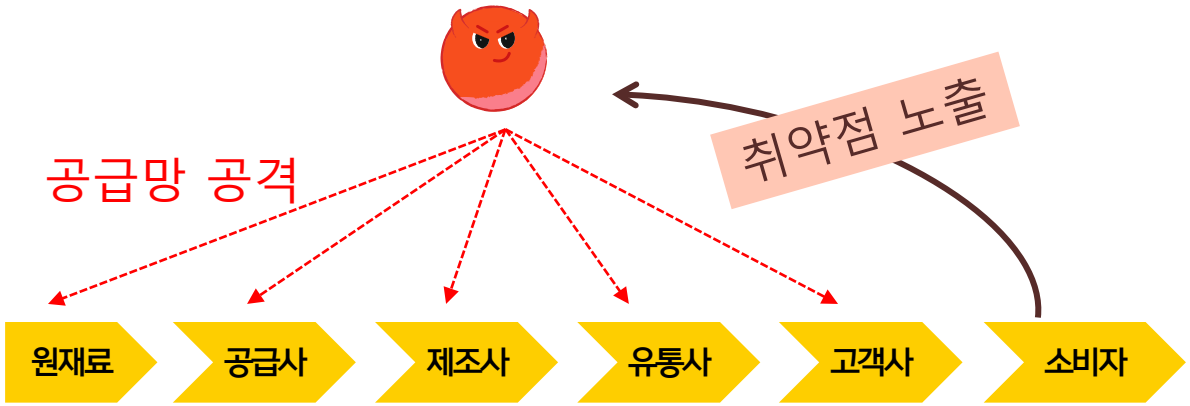


원재료 → 공급사 → 제조사 → 유통사 → 고객사 → 소비자

01 우리 곁에서 일어나는 SW 공급망 보안 사고

공급망 공격의 특징

- 공격 당한 대상과 최종 피해자가 일치하지 않음
- 최종 피해자는 공격 대상보다 훨씬 많은 경우가 대부분임



01 의료·통신으로 확장되는 마이데이터사업

공급망 공격 사례: PC 업데이트 서버 해킹을 통한 악성코드 배포

2019년 3월, 대만의 PC업체 에이수스의 온라인 업데이트 시스템이 해킹
분석 결과, 업데이트 서버에 접속하는 수백만 대의 PC 중
약 600대의 Mac에 대해서만 이 악성코드가 작동하도록 구현되었음
에이수스가 2018년 5월~11월에 해킹되었을 것으로 추정됨

공급망 공격 사례: 국내

금융용 보안인증 SW 해킹되는 바람에
SW가 설치된 PC를 해킹하고 악성코드가 유포됨
PC 사용 기관과 개인 피해

01 의료·통신으로 확장되는 마이데이터사업

공급망 공격 사례: 도메인이름 서비스 공격으로 인터넷 서비스 접속 불가

2016년10월 21일, 도메인이름 서비스업체 Dyn이 디도스(DDoS) 사이버 공격으로
다운되는 바람에 이를 이용하는 아마존, 트위터, 비자, 페이팔 등
미국의 많은 서비스가 거의 하루 동안 접속되지 않거나 장애가 발생하여 이용자 피해가 컸음.
불특정 다수에 대한 공격

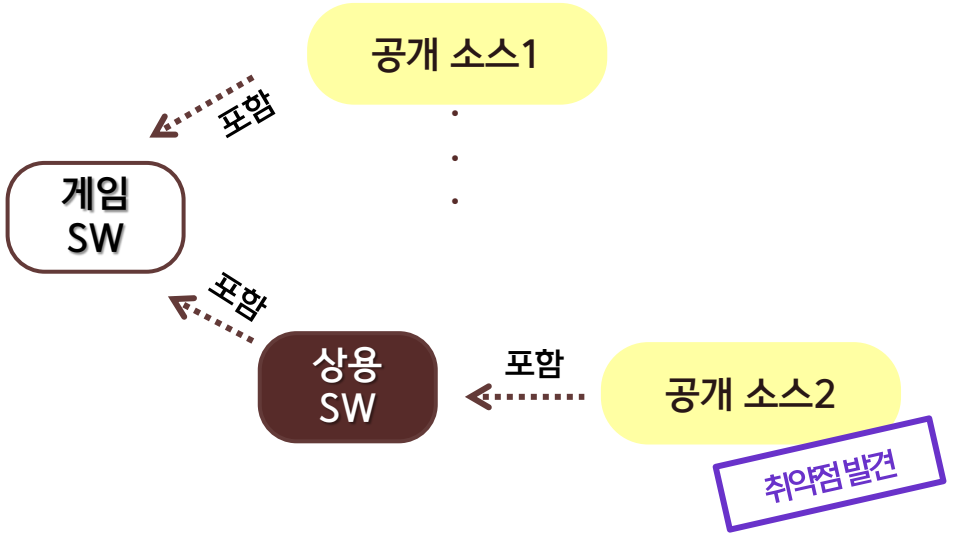
출처: 2016년 다인 사이버 공격, https://ko.wikipedia.org/wiki/2016_다인_사이버_공격, 2024.11.18

02 SBOM, SW를 분해해 본다?

소프트웨어 구성요소 명세서(Software Bill of Materials, SBOM)

“SBOM”란 SW 구성요소를 서술하는 SW 전체의 구성요소를 목록화한 것

- SW에 포함되어 있는 외부 공개 소스나 바이너리(실행파일, 라이브러리) 등을 관리, 추적할 수 있도록 함
- SW 보안취약점이 발견됐을 경우, 이를 사용하는 다른 SW를 추적하는 데 활용



02 SBOM, SW를 분해해 본다?

SW 구성요소 명세서 기본 데이터 항목

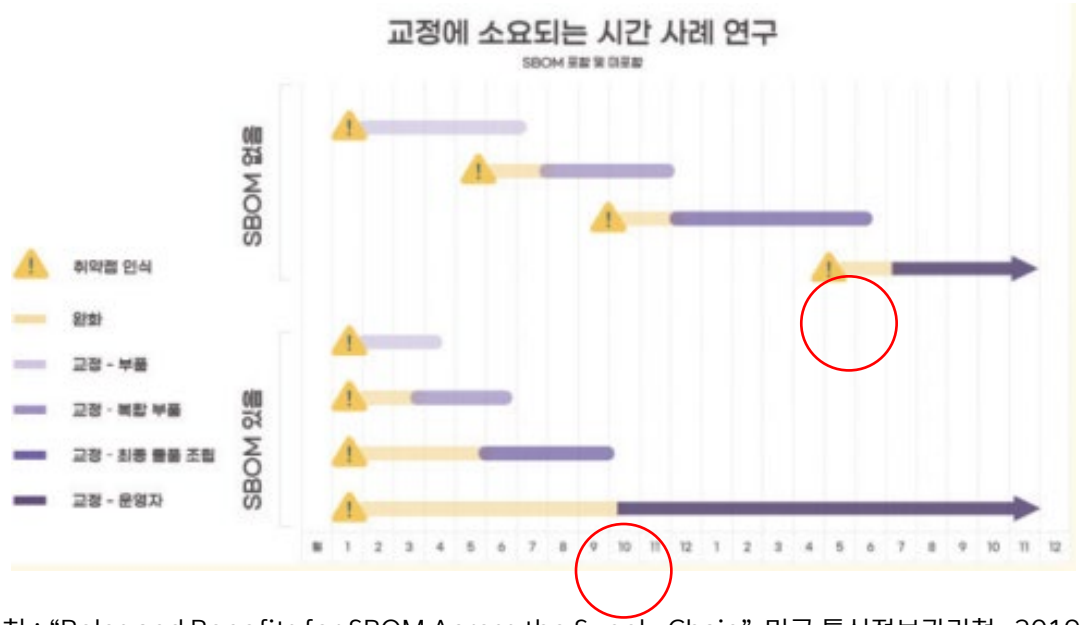
- 개인정보의 전송 요구권 행사 지원
- 정보주체의 권리행사를 지원하기 위한 개인정보 전송시스템의 구축 및 표준화
- 정보주체의 권리행사를 지원하기 위한 개인정보의 관리 · 분석

항목	설명
공급자명	구성요소를 생성하고, 정의 및 식별한 주체의 이름
타임스탬프	SBOM 데이터로 변환(Assembly)한 날짜 및 시간 기록
저작권자	구성요소에 대한 SBOM 데이터를 생성한 주체의 이름
구성요소명	최초 공급자에 의해 정의된 SW 단위에 할당된 명칭
버전	이전 버전으로부터 SW의 변경 사항을 지정하는 데 사용하는 식별자
고유식별자	구성요소를 식별하는 데 사용되거나 관련 DB의 조회 키(Look-up Key) 역할을 하는 기타 식별자
종속성 관계	구성요소 X가 SW Y에 포함된다는 관계를 특정함

02 SBOM, SW를 분해해 본다?

SW 구성요소 명세서 도입 효과

SW공급망 내에서 SW취약점이 발생했을 때 최종 소프트웨어를 구매한 소프트웨어 운영자가 취약점을 인식하는 데 걸리는 시간이 **최대 18개월에서 9개월로 절반으로 줄어듦**



출처 : “Roles and Benefits for SBOM Across the Supply Chain”, 미국 통신정보관리청 , 2019.11.

02 SBOM, SW를 분해해 본다?

SBOM 의무화에 관한 세계적 흐름

유럽연합

- 2024년 10월 사이버복원력법(Cyber Resilience Act) 제정, 36개월 후(2027년) 전면 시행
- **디지털 제품에 대해 SBOM 제출 의무화**
- **EU에 판매하는 디지털 제품(디지털 요소가 있는 제품)에 적용**
  - ✓ 최종 사용자 기기(End devices)
    - 랩탑, 스마트폰, 센서, 카메라
    - 스마트 로봇, 스마트카드, 모바일 기기
    - 스마트 스피커, 라우터, 스위치, 산업제어시스템(ICS)
  - ✓ 소프트웨어: 펌웨어, 운영체제, 모바일앱, 데스크톱 앱, 비디오 게임
  - ✓ 부품(SW, HW): 컴퓨터처리유닛(computer processing units), 비디오카드, 소프트웨어 라이브러리

02 SBOM, SW를 분해해 본다?

SBOM 의무화에 관한 세계적 흐름

미국 식품의약국(FDA)

- 2023년 10월, 의료기기 인허가 시 SBOM 제출 의무화

미국 육군

- 2024년 9월, 신규 구매 또는 구축 SW에 대한 SBOM 의무화하기로 결정
- 이후 구현 가이드 수립

미국 연방정부

- 2022년 12월에 연방정부에 납품하는 모든 SW에 SBOM을 적용할 계획이었으나 연기됨
- SBOM을 요구하는 시정부, 주정부가 있음

03 나도 공급망 보안을 위해 할 일이 있다고?

개발사의 공급망 보안 활동

- **안전한 제품 기준 관리**
  - ✓ SW 개발 보안 정책과 절차 정의 및 관리
- **안전한 코드 개발**
  - ✓ 안전한 SW 개발 및 소스 코드 보호
- ✓ **공개 소스의 안전한 관리**
  - ✓ 보안취약점 수집 및 대응

03 나도 공급망 보안을 위해 할 일이 있다고?

개발사의 공급망 보안 활동

- **외부 구성요소 검증**
  - ✓ 외부 바이너리 취약점 점검
  - ✓ 신뢰할 수 있는 공급사 선택
- **빌드 환경 보안**
- **코드 배포 시 보안**
  - ✓ SW 패키지 및 업데이트 보호
  - ✓ 배포 시스템 보호

03 나도 공급망 보안을 위해 할 일이 있다고?

공급사의 공급망 보안 활동

- **제공되는 SW 무결성 유지**
  - ✓ 개발사에게서 전달 받은 SW 무결성 유지
  - ✓ SW 출시 버전의 보관·보호
- **SW 패키지·업데이트 유효성 검사**
  - ✓ 실행 파일 테스트를 통해 보안 요구사항 준수 점검
- **보안취약점 관리**
  - ✓ 알려진 취약점 관리
  - ✓ 운영사의 보안취약점 신고를 접수 및 개발사 통보

03 나도 공급망 보안을 위해 할 일이 있다고?

운영사의 공급망 보안 활동

- **조달 및 인수**
  - ✓ **제품 보안 평가**
  - ✓ **구매 계약에 공급망 보안 요구사항** 추가
- **적용 및 배포**
  - ✓ **공급사의 SW 배포 인프라 및 제품 무결성 검증**. 인수한 제품과 SBOM 비교
  - ✓ 제품 기능 및 보안 테스트
  - ✓ **운영에 필요한 보안 활동 수행, 악성 행위 모니터링**
- **제품 업그레이드**
  - ✓ 적용 및 배포 시 보안 활동

03 나도 공급망 보안을 위해 할 일이 있다고?

전사적 다단계 위험 관리

- **수준 1 (전사)**
  - ✓ 전반적인 C-SCRM 전략, 정책, 구현 계획을 통해 전사에서 C-SCRM이 관리되는 데 필요한 기조
  - ✓ 거버넌스 구조, 경계를 설정. 경영진의 역할
- **수준 2 (미션 및 비즈니스 프로세스)**
  - ✓ 수준 1에서 결정한 전사적인 상황(context)과 방향을 가정
  - ✓ 그것을 특정한 미션 및 비즈니스 프로세스에 맞게 조정
- **수준 3 (운영)**
  - ✓ C-SCRM 계획은 정보시스템이 비즈니스·기능·기술 요구사항을 충족
  - ✓ 적절하게 조정된 통제를 포함하는지 여부를 결정하기 위한 기반을 제공
  - ✓ 수준 2에서 제공하는 상황과 방향에 큰 영향을 받음

03 나도 공급망 보안을 위해 할 일이 있다고?

소프트웨어공급망 보안 국내 활동

2021.5. 미국 바이든 행정부 행정명령(EO)

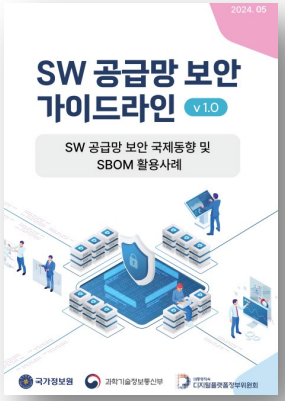
- -14028, '국가 사이버보안 개선에 관한 행정명령'
  - ✓ 미국 정부에 소프트웨어 납품 시 SBOM 제출 의무화 검토

2023.12. 공급망 안정화법

- **('경제안보를 위한 공급망 안정화 지원 기본법'**(2024.6.27. 시행, 소관부처: 기획재정부)
  - ✓ **소프트웨어 공급망 포함**

03 나도 공급망 보안을 위해 할 일이 있다고?

소프트웨어공급망 보안 국내 활동



- 공급망 보안 가이드라인〉 발간
  (국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회)
- 2024.9. 민관합동 SW공급망 보안 TF 발족, 활동
  - ✓ 국가적 대응 체계 및 제도 수립, 기업 등 민간 활동 지원

04 정보보안 정책, 지침, 프로세스

GRC

- **거버넌스(Governance)**: 조직 거버넌스는 조직의 목표를 달성하기 위해 경영진과 이사회가 의사결정을 내리고, 그것을 수행하기 위한 체계(ISO 26000)
- **위험 관리(Risk management)**: 조직의 활동이 품고 있는 다양한 리스크, 특히 사업 목표를 달성하기 위해 나아갈 때 발생할 수 있는 리스크를 관리하는 것.
- **규제 준수(Compliance)**: 법규와 규제 내에서 조직의 활동이 이뤄질 수 있도록 하는 것

정보보안 정책 (정보보안 규정)

- 조직이 수행하는 정보보안 활동의 근거를 포함하는 최상위 수준의 문서로서 다음 내용을 포함
  - ✓ 조직의 정보보안에 관한 CEO 등 최고경영진의 의지 및 방향
  - ✓ 조직의 정보보안을 위한 역할·책임 및 대상·범위
  - ✓ 조직이 수행하는 관리적·기술적·물리적 정보보안 활동의 근거

04 정보보안 정책, 지침, 프로세스

정보보안 지침

- 정보보안 정책에 명시된 정보보안 사항을 구체적으로 시행하기 위하여 필요한 세부 방법 등을 규정한 문서로서 보호 대상이나 수행 주체 관점에서 작성
  - ✓ **보호 대상 관점**: 서버 보안 지침, 네트워크 보안 지침, 데이터베이스 보안 지침 등
  - ✓ **수행 주체 관점**: 임·직원 보안 지침, 개발자 보안 지침, 운영자 보안 지침 등

정보보안 프로세스(절차)

- 임직원이 담당 업무를 수행하면서 정책, 지침을 준수하기 위해 구체적으로 수행해야 하는 절차로서 관련 업무 절차에 정보보안에 필요한 절차를 삽입
  - ✓ 입사·퇴사 시 보안 프로세스
  - ✓ 외주 업체 선정 및 관리 시 보안 프로세스

04 정보보안 정책, 지침, 프로세스

정보보안 프로세스(절차) : 퇴직 프로세스

- **퇴사 면담**
  - ✓ 퇴사 사유 및 개선점 피드백
  - ✓ 퇴직금 및 필요 서류 확인
- **퇴사자 경험 청취**
  - ✓ 2주 정도의 기간
- **장비 수거 및 보안 유지 서약**
  - ✓ 기업의 모든 접근 권한 종료
  - ✓ 기밀 유지 서약서 작성
- **연락처 제공**
  - ✓ 퇴사 이후 전달할 수 있는 내용을 위한 연락처

04 정보보안 정책, 지침, 프로세스

회사 구성원이 함께 지켜야 할 10대 정보보안 수칙

- 1. 소프트 웨어 최신화
  - ✓ 업무에 사용하는 운영체제와 소프트웨어를 자동 업데이트 설정을 통해 최신 상태로 유지
- 2. 백신 및 보안 설정
  - ✓ 실시간 검사, 자동 업데이트, 정기적인 전체 검사 설정을 활성화
    회사에서 제공하는 보안 프로그램을 사용하는 것이 안전
- 3. 회사 이메일 사용 주의
  - ✓ 회사에서 제공하는 이메일 계정만 업무에 사용
    스팸 메일이나 의심스러운 이메일은 열지 말고 삭제

04 정보보안 정책, 지침, 프로세스

회사 구성원이 함께 지켜야 할 10대 정보보안 수칙

- **4. 의심스러운 사이트 방문 금지**
  - ✓ 보안이 확보되지 않은 사이트나 허가되지 않은 웹사이트에 방문 금지
- **5. 강력한 비밀번호 사용**
  - ✓ 개인 서비스 비밀번호를 업무용으로 사용 금지
  - ✓ 대문자, 소문자, 숫자, 특수문자를 포함해 최소 10자리 이상의 비밀번호를 만들어 사용
- **6. 2단계 인증 활성화**
  - ✓ 문자 메시지, 인증 앱, 생체 인증 등 2단계 인증 방식을 통해 보안을 강화

04 정보보안 정책, 지침, 프로세스

회사 구성원이 함께 지켜야 할 10대 정보보안 수칙

- **7. 피싱 공격 주의**
  - ✓ 피싱 공격은 악성 프로그램을 설치하거나 정보를 탈취하기 위해 신뢰를 가장해 진행되니 의심스러운 이메일이나 링크는 주의 깊게 확인하고 대응
- **8. 업무 데이터 백업**
  - ✓ 업무 데이터를 회사 서버에 저장하고, 정기적으로 백업을 진행하여 데이터 손실을 예방
- **9. 보안 정책 준수**
  - ✓ 회사의 보안 지침과 프로세스를 철저히 준수하고 관련 규정을 숙지하여 데이터 보호를 위한 최선의 방법을 따름
- **10. 정보 유출 사고 신고**
  - ✓ 피싱 이메일, 개인정보 유출, 데이터 손실 등이 발생하면 즉시 정보보안팀에 신고하여 피해를 최소화

SMART 시큐의 노트

우리 곁에서 일어나는 SW공급망 보안 사고

- 소프트웨어 공급망 보안 사고는 한 단계의 취약점이 전체 공급망과 최종 이용자에게 실시간으로 광범위한 피해를 유발하며, 대규모 서비스 중단 사례로 이어질 수 있음
- 소프트웨어 공급망은 하드웨어보다 통제 범위가 넓고 복잡하여 보안 관리와 예방 조치가 더욱 어려우며, 이를 위한 체계적인 관리가 필수

SBOM, SW를 분해해 본다?

- SBOM(소프트웨어 구성 요소 명세서)은 소프트웨어 구성 요소를 기록해 공급망 취약점을 빠르게 인식하고 대응할 수 있도록 설계된 도구로, 보안 관리 투명성을 강화
- 유럽연합과 미국 등은 SBOM 의무화를 통해 디지털 제품 및 의료기기 분야에서 보안을 강화하고, 취약점 대응 시간을 최대 절반으로 단축하는 효과를 입증함

SMART 시큐의 노트

나도 공급망 보안을 위해 할 일이 있다고?

- 소프트웨어 공급망 보안을 위해 운영사는 조달, 배포, 업그레이드 단계에서 보안 요구 사항을 철저히 검토하고, 개발사와 공급사는 각각 안전한 소스 코드 작성과 소프트웨어 무결성 유지를 통해 역할을 분명히 함
- 전사적 관리 체계는 경영진의 보안 목표 설정, 중간 관리자의 프로세스 점검, 실무자의 시스템 운영으로 구성되며, 모든 단계에서 공급망 보안을 고려해 통합적으로 관리

정보보안 정책, 지침, 프로세스

- 정보보안 정책은 회사의 보안 목표와 경영진의 의지를 반영한 최고 권위의 문서이며, 서버, 네트워크, 임직원 등 분야별 지침과 업무 과정에서 이를 반영한 보안 프로세스를 가지고 운영해야 함
- 모든 구성원이 정보보안 정책과 지침을 준수하고 협력해야 조직이 보안 위협으로부터 보호받을 수 있으며, 안정적이고 지속 가능한 성과를 유지할 수 있음

개인정보보호
정보보안교육

|생체정보, 인공지능, 딥페이크

New

신

짜

마트한

CONTENTS

- NEW 이슈 탐방

1 생체정보의 활용과 규제

2 인공지능과 딥페이크

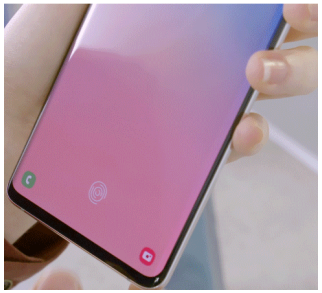
3 딥페이크 부작용과 대응 방안

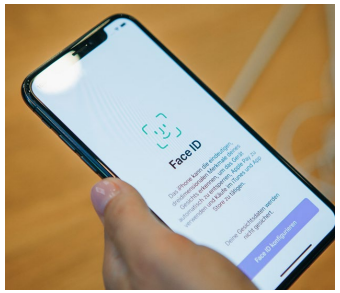
- SMART 시큐의 노트

NEW 이슈 탐방

스마트폰의 사용자 인증

- 생체인증은 스마트폰의 사용자 인증뿐 아니라 노트북, 건물 출입 시 사용자 인증에 지문인증, 얼굴인증 등 생체인증기술이 대중화되었음
- 보안성과 편의성 측면에서 비밀번호 인증보다 뛰어남



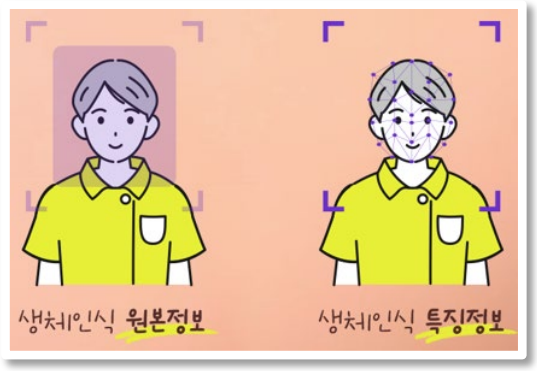


출처: “다양해지는 생체 인식 센서, 어떤 것들이? 영화에서 일상이 된 ‘생체 인식 기술’”, 삼성디스플레이 뉴스룸, 2020.1.14.

01 생체정보의 활용과 규제

생체인식정보

- **생체인식 원본정보**: 생체인식정보 중 입력장치(카메라, 스캐너 등) 등을 통해 수집·입력된, 특징정보 생성에 이용되는 정보
- **생체인식 특징정보**: 생체인식 원본정보로부터 특징점을 추출하는 등의 일정한 기술적 수단을 통해 생성되는 정보 (개인정보보호법 시행령 제18조 제3호에 따른 민감정보)



01 생체정보의 활용과 규제

생체인식정보를 이용자 기기의 안전한 저장소에 저장

- **생체인식정보 등록**

  ✓ 이용자 A의 스마트폰에서 생체인식정보 등록

  → 스마트폰에서 비밀키와 공개키 한 쌍을 생성

  → 생체인식정보와 비밀키는 트러스트존 등 스마트폰의 안전한 HW 저장소에 보관

  → 외부 서버에 공개키를 전달

- **사용자 인증**

  ✓ A 로그인

  → 서버에서 1회용 난수와 인증 대상을 스마트폰에 전달

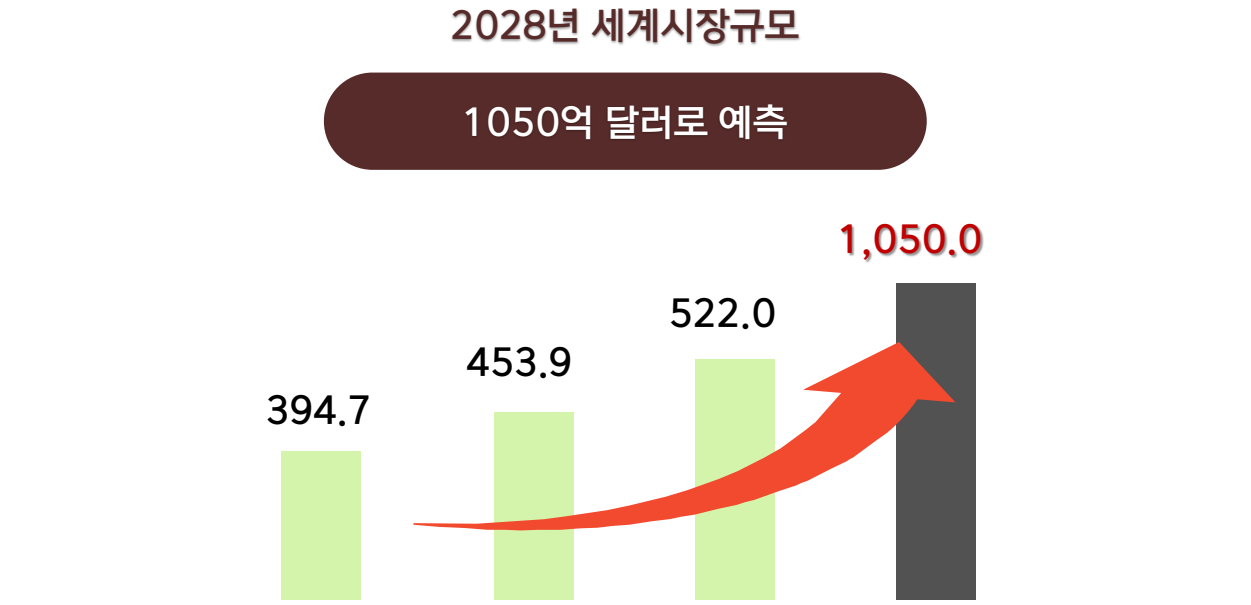
  → 스마트폰에서 A의 비밀키로 디지털 서명하여 서버에 보냄

  → 서버에서 A의 공개키로 서명 검증

01 세계 생체인식시장의 성장

생체인식정보를 이용자 기기의 안전한 저장소에 저장

- 2028년 세계 시장 규모를 1050억 달러(140조 원 정도)로 예측



분류	2021	2022	2023	2028	CAGR (21~28)
생체인식	395	454	522	1050	15%

01 세계 생체인식시장의 성장

생체인식 기술 규제의 배경

- **생체인식정보의 특징**
  - ✓ 유일성, 불변성
  - ✓ 유출 등 사고 발생 시 정보주체의 피해가 크고 복구하기 어려움
- **악용 가능성**
  - ✓ 얼굴 인식을 통한 감시, 프라이버시 침해
  - ✓ 기업에서 임직원 감시에 활용

01 세계 생체인식시장의 성장

글로벌 법령에서 보는 생체인식정보 보호

- 생체인식정보를 개인정보(민감정보)의 한 종류로 규제
  - ✓ 한국 개인정보보호법
  - ✓ 유럽연합 개인정보보호법(GDPR: General Data Protection Regulation)
  - ✓ 미국 '캘리포니아 프라이버시 권리법'(CPRA: The California Privacy Rights Act of 2020)
  - ✓ 미국 '버지니아 소비자데이터 보호법'(VCDPA: Virginia Consumer Data Protection Act)
  - ✓ 미국 '콜로라도 프라이버시법'(CPA: Colorado Privacy Act)

01 세계 생체인식시장의 성장

유럽연합 인공지능법(AI Act)

- **원격 생체식별시스템(Remote biometric identification system)**

  ✓ **원격 생체식별시스템**(Remote biometric identification system)

  - 한 사람의 생체 정보와 기준 데이터베이스에 포함된 생체 정보를 비교하여 원거리에 있는 **자연인을 식별하기 위한 AI 시스템**. 그 사람이 존재할 것인지, 식별할 수 있을 것인지 AI 시스템 사용자가 사전에 알지 못함

  ✓ **'실시간'(Real-time) 원격 생체식별시스템**

  - 생체 인식 데이터의 캡처, 비교 및 식별이 모두 **상당한(significant) 지연 없이 이루어지는** 원격 생체식별시스템.

  - 즉각적인 식별뿐만 아니라 우회 방지를 위한 제한된 짧은 지연이 제한되는 것도 포함

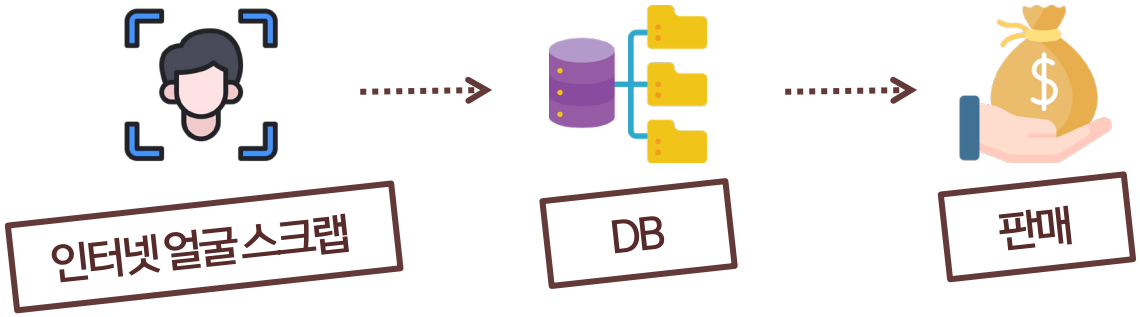
  ✓ '사후'(Post) 원격 생체식별시스템: 실시간 원격 생체식별시스템이 아닌 원격 생체식별시스템

  ✓ **공개된 장소**(Publicly accessible spaces): 특정 접근 조건의 적용 여부 및 잠재적인 수용 인원 제한에 관계없이 대중이 접근할 수 있는 모든 공공 또는 개인 소유의 **물리적 장소**를 의미

01 세계 생체인식시장의 성장

미국 일리노이주 BIPA 위반 사건

SNS 등 인터넷에 공개된 사진 자료를 가공하여 얼굴인식정보를 확보한 뒤
이를 민간 또는 경찰 같은 법 집행기관에 판매

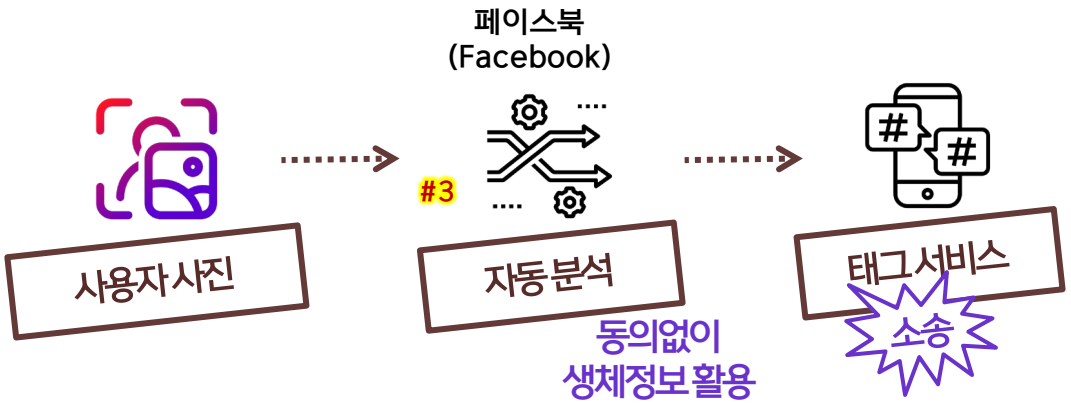


- GDPR 위반으로 그리스는 260억 원의 대규모 과징금과 함께 자국민의 얼굴인식정보 삭제를 명령
- 영국, 프랑스, 이탈리아 등 각국에서 클리어뷰 AI에 비슷한 행정처분
- 그것을 정보주체의 동의 없이 수집, 처리하여 상업적 목적으로 이용하는 것은 GDPR에 위반

01 세계 생체인식시장의 성장

미국 일리노이주 BIPA 위반 사건

2010년 페이스북은 사진과 동영상 속 사용자 얼굴을 자동으로 인식해 태그를 제안하는 기능을 선보임
2011년 6월 7일부터 세계 대부분 국가에서 이를 기본 설정으로 도입
2015년 일리노이 주민 3명이 개인 생체정보 보호법에 위배를 이유로 연방법원에 소장 제출



- 일리노이주는 2008년 이미, 기업이 안면 형태·지문·홍채 등 개인 생체정보를 수집할 경우 당사자에게 사용 목적과 보관 기간 등을 상세히 설명 및 사전 동의 실시
- 소송의 합의에 따라 2019년 9월 얼굴 자동 인식 기능의 기본 설정을 '꺼짐'으로 전환하고 사용자 동의 없이 저장된 안면 인식 템플릿을 삭제

01 세계 생체인식시장의 성장

정부 얼굴인식 기술 도입 현황

- **행정안전부**
  - ✓ 정부청사 얼굴인식 출입 시스템, 4대 정부청사 공무원, 방문객 등 얼굴인식 출입
- **법무부·과기정통부**
  - ✓ 인공지능 식별추적시스템, 공항 자동출입국심사 등에 활용
- **과기정통부**
  - ✓ 인공진능융합프로젝트 민간 지원사업, 실종 아동, 치매노인 등 조기 대응 및 얼굴 결제 시스템 등 개발

얼굴인식 기술의 도입·활용에 있어서 인권 보호를 위한 권고 및 의견표명

- 얼굴인식 기술의 도입·활용에 있어서 인권 보호를 위한 권고 및 의견표명

02 인공지능과 딥페이크

인공지능 활용 분야

- 예술, 글쓰기. 의료, 패션 디자인, 고객서비스, 연구개발, 제조업, 금융업, sw 개발, 생산성 도구와 연결 등

최초로 완전히 AI가 생성한 영화

텍스트 시나리오를 영상으로 제작

출처: https://www.youtube.com/watch?v=KhQnnISdDIU, TCLtv+, 2024.04.12

02 인공지능과 딥페이크

적대적 생성 네트워크(GAN): 경찰 vs 위조지폐범

- 두 개의 인공신경망을 적대적으로 학습시키며 실제 데이터와 비슷한 데이터를 생성해내는 딥러닝 생성 모델
- GAN은 생성자(Generator)와 판별자(Discriminator)라는 두 개의 인공신경망으로 이루어짐
- 생성자는 실제(진짜)와 유사한(가짜) 데이터를 생성, 판별자는 주어진 데이터가 진짜인지 가짜인지 구별
  - ✓ ㅊ, 생성자는 이와 비슷한 가짜 이미지를 생성하고,
    판별자는 진짜 이미지와 가짜 이미지를 학습하여 생성자가 만든 가짜 데이터를 식별하기 위해 노력
    →이러한 적대적 경쟁을 통해 진짜와 가짜를 식별하기 어려운 데까지 이르게 됨

02 인공지능과 딥페이크

딥페이크(DeepFake)

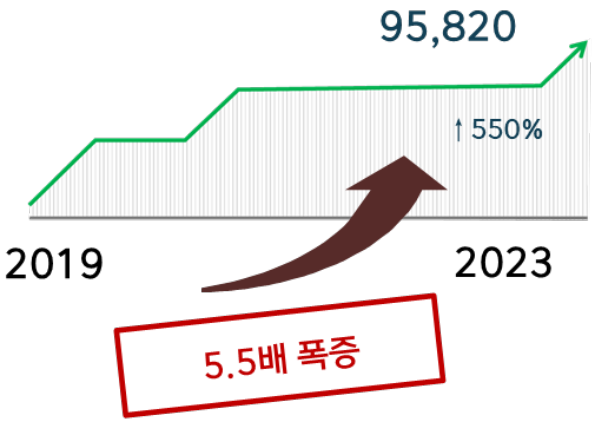
- 딥러닝(Deep Learning) + 가짜(Fake), 즉 딥러닝 기술을 이용하여 진짜와 비슷한 가짜를 생성하는 기술
- 2017년 미국의 대형 커뮤니티 사이트인 레딧(Reddit)의 한 운영자가 '딥페이크'라는 서브레딧을 만들어 유명인의 얼굴로 바꾼 딥페이크 성착취물을 올린 것이 그 시작
- 국내에서는, 2024년 8월, 텔레그램에서 딥페이크 성범죄물이 수년 간 유포되어 왔다는 사실이 알려지면서 피해자가 급증함에 따라 사회 문제가 되고, 경찰 수사와 국회에서 법 개정이 신속하게 추진되었음

02 인공지능과 딥페이크

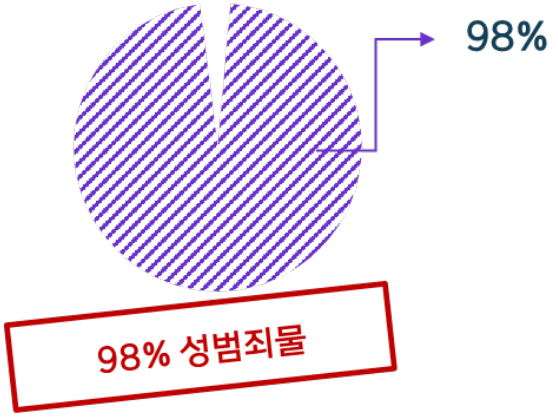
글로벌 딥페이크 현황 (미국 보안업체 시큐리티히어로의 조사)

- 2023년 온라인 딥페이크 비디오는 모두 95,820개
  - 2019년보다 5.5배 폭증, 이중 98%가 성착취물
- 피해자의 99%가 여성
- 피해자의 53%가 한국인
- 피해자 직업은 가수, 여배우를 합치면 90%가 넘음

온라인상의 딥페이크 영상(2023년)



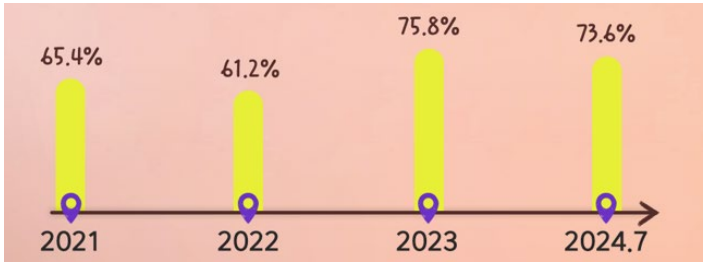
딥페이크 포르노그래피는
전체 온라인 딥페이크 영상의 98%를 차지



02 인공지능과 딥페이크

딥페이크 성범죄 국내 현황

- 학교 딥페이크 피해 현황(초, 중, 고), 교육부
  - ✓ 2024.1.1.~10.18. 피해신고 건수: 533건, **피해자 수 학생 841명, 교원 33명**, 직원 등 1명
- **딥페이크 성범죄 피해자** 중 미성년자 수, 경찰청
  - ✓ 2021년 53명, 2023년 181명, 2024년(10.18.까지, 초중고만 포함) 841명
- **딥페이크로 검거된 피의자 중 10대 비율**, 경찰청
  - ✓ **2021년 65.4%, 2022년 61%, 2023년 75.8%**
    - 2023년-검거된 피의자 120명 중 10대가 91명(75.8%)
  - ✓ **2024년 73.6%(1월~7월)**



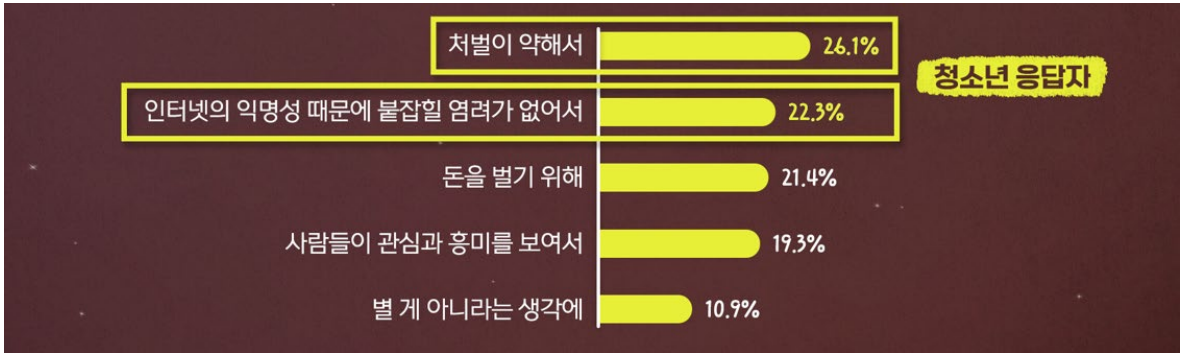
03 인공지능과 딥페이크

디지털 성범죄 확산 및 재생산 원인

- 2022년 방송통신위원회 조사에선 응답 청소년의 절반 가까이가 '디지털 성범죄 확산 및 재생산 원인'으로 **'약한 처벌'과 '붙잡힐 염려 없음'을 꼽음**

- 청소년들이 딥페이크 성범죄를 놀이처럼 인식한다는 분석이 있음

  ✓ 범죄를 저질러도 검거되지 않거나 검거되더라도 처벌되지 않을 거라는 '믿음'이 있는 것으로 보임



출처: 방송통신위원회, 한국지능정보사회진흥원, 「2022 사이버폭력 실태조사」, 2023

03 인공지능과 딥페이크

국내 딥페이크 성범죄 처벌 법규

- [성폭력처벌법 제14조의2(허위 영상물 등의 반포 등), 2024.10.16. 개정]
  - ✓ 딥페이크 성범죄물을 제작하거나 배포하는 자는 7년 이하의 징역 또는 5천만원 이하의 벌금
- 성폭력 처벌법 제14조 2 (2024.10.16. 개정)
  - ✓ **영리를 목적**으로 영상물을 배포하는 자는 **3년 이상의 유기징역**
- 성폭력 처벌법 제14조 2 (2024.10.16. 개정)
  - ✓ 제작 또는 유통을 하지 않더라도 **소지, 구입, 저장 또는 시청한 자**는 **3년 이하의 징역** 또는 **3천만원 이하의 벌금**

03 인공지능과 딥페이크

종합적인 대책 필요

- **수사, 행정, 플랫폼사업자 등 신속한 대응이 가능한 종합 대응 체계 수립**
  - ✓ 딥페이크 성범죄는 악성 디지털 성폭력 범죄라는 관점에서 신속한 강제 수사와 증거 확보, 무거운 처벌 필요
  - ✓ 디지털 성범죄물에 대한 위장 수사와 국내외 플랫폼 사업자 등에 대한 긴급 차단, 삭제 명령 등의 응급 조치가 가능하도록 법률의 개정 필요
- **법률 취지에 따른 법원의 무거운 판결**
  - ✓ 법원의 인식 전환과 함께 대법원 양형의 변경이 무엇보다도 중요
- **청소년에 대한 교육**
  - ✓ 청소년기는 교육과 지도를 통해 세계관을 형성하고 잘못을 바로잡을 수 있는 좋은 시기임
  - ✓ 인터넷이 도입된 초기부터 인터넷 중독이나 지식재산권 침해와 같은 인터넷의 역기능에 대해 주목하고 어렸을 때부터 인터넷 윤리 교육이 필요하다는 의견이 있었고, 일부 교육이 이뤄지고 있음
  - ✓ 디지털 성범죄가 심각한 현 상황을 고려하면, 디지털 성인지 교육, 성평등교육, 인권 감수성 교육 등 공교육 과정에서 적절한 교육이 있어야 할 것 같음
  - ✓ 시청자 중 자녀가 있는 분들이라면, 우리 가정은 어떤지 살펴보는 것도 좋겠음

SMART 시큐의 노트

생체정보의 활용과 규제

- 생체정보는 지문, 얼굴 등 개인의 생체 인식 정보를 활용해 편리한 인증 기술로 발전하고 있음
- 생체정보 유출 시 복구가 어렵고 악용 가능성이 높아, 세계적으로 이를 보호하기 위한 규제가 강화되고 있음
- 우리나라는 개인정보보호법에서 생체정보를 민감정보로 규정해 보호하며, 유럽연합 GDPR 및 미국 일부 주법과 유사한 방식으로 규제하고 있음

인공지능과 딥페이크

- 인공지능은 예술, 의료, 고객 서비스, 영화 제작과 같은 창의적 영역 등 다양한 분야에서 활용
- 딥페이크는 GAN 기술로 생성된 실제와 유사한 가짜 데이터로, 선거 및 범죄 등 사회적으로 심각한 영향을 미칠 수 있음
- 특히 딥페이크 성범죄는 청소년 피해가 증가하고 있어, 처벌 강화와 함께 청소년 대상 성인지 및 성평등 교육이 요구됨

SMART 시큐의 노트

딥페이크의 부작용과 대응 방안

- 딥페이크 성범죄는 피해자의 99%가 여성, 범죄자의 70% 이상이 10대로 나타나 심각한 사회적 문제가 되고 있음
- 법적으로 딥페이크 제작·배포에 대한 처벌이 강화되었으나, 실제 양형 규정과 판결에서는 한계가 있어 개선이 필요
- 단순한 처벌을 넘어 디지털 성인지 및 인권 감수성 교육과 함께 플랫폼 사업자와 행정기관의 신속 대응 체계 구축이 중요