삼정 KPMG

GOVERNANCE WATCH

생성형 AI를 활용한 사이버 공격과 대응방안: 딥페이크 공격을 중심으로

2026.10.15

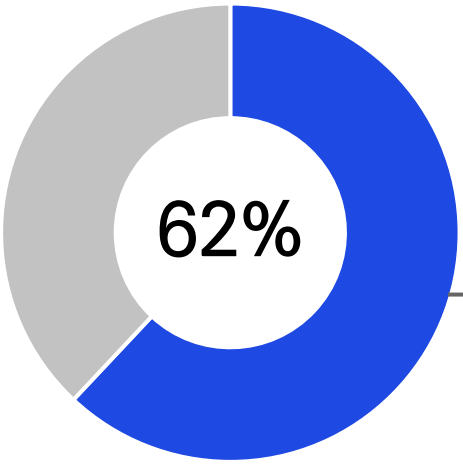
감사위원회 지원센터
(Audit Committee Institute)

생성형 AI를 활용한 사이버 공격과 대응방안:
딥페이크 공격을 중심으로

생성형 AI를 활용한 사이버 공격의 확산(1)

생성형 AI를 통해 정교하게 제작된 딥페이크가 사이버 공격에 활용되는 비중이 증가하고 있음

사이버 공격을 받은 적이 있습니까?



설문 응답 기업의 62%가 지난 12개월 동안 딥페이크 공격을 경험(2)

"사회 공학(social engineering) 기법이나 자동화된 프로세스의 취약점을 악용한 딥페이크 공격을 경험"

(1) AFC, “Fraud and Emerging Tech: Deepfakes”, 2026.4
이번 거버넌스 와치는 상기 AFC 자료를 바탕으로 한국 실정에 맞게 일부 수정하여 작성함

(2) Gartner, “Gartner Survey Reveals GenAI Attacks Are on the Rise”, 2025.9.22

삼정 KPMG
© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

생성형 AI를 활용한 사이버 공격과 대응방안:
딥페이크 공격을 중심으로

딥페이크의 정의와 유형

딥페이크(Deepfakes)는 인공지능을 사용해서 인위적인 조작으로 생성된 합성미디어(가짜 콘텐츠)의 형태

딥페이크의 정의

- 인공지능(AI) 심층 학습을 뜻하는 '디프 러닝(deep learning)'과 '가짜'를 뜻하는 '페이크(fake)'의 합성어로, 타인을 속이거나 비방할 의도로 콘텐츠를 조작하거나 생성하는 기술

딥페이크의 유형

① 텍스트	• 특정 개인이나 조직의 문체, 어조, 메시지 전달 방식을 모방하여 거짓 정보를 더욱 설득력 있게 만드는 것
② 이미지	• 당사자의 동의나 고지 없이 특정 인물의 외모를 모방하거나, 실제로 존재하지 않는 장면이나 사건을 묘사
③ 동영상	• 특정 인물의 표정과 신체 언어를 모방, 실제로 발생하지 않은 사건을 묘사, 또는 실시간 영상회의 중 다른 사람인 것처럼 보이게 하는 것

삼정 KPMG
© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

딥페이크를 통한 공격 방식

딥페이크(Deepfakes)는 금전적 손실 뿐만 아니라 파급효과가 큰 사회적 피해와 광범위한 평판 훼손을 야기할 수 있음

01 허위 금융거래

- 딥페이크로 경영진을 사칭하여 제3자 계좌로 자금 이체 유도
- 딥페이크로 만든 가짜 송장, 계약서로 부적절한 금융거래를 승인하도록 유도

02 허위 청구 증빙

- 사진, 영수증 등을 위조하여 허위 보험금 청구, 제품 보증 청구, 환불 및 보상 요구 등의 근거로 활용

03 허위 신원 증빙

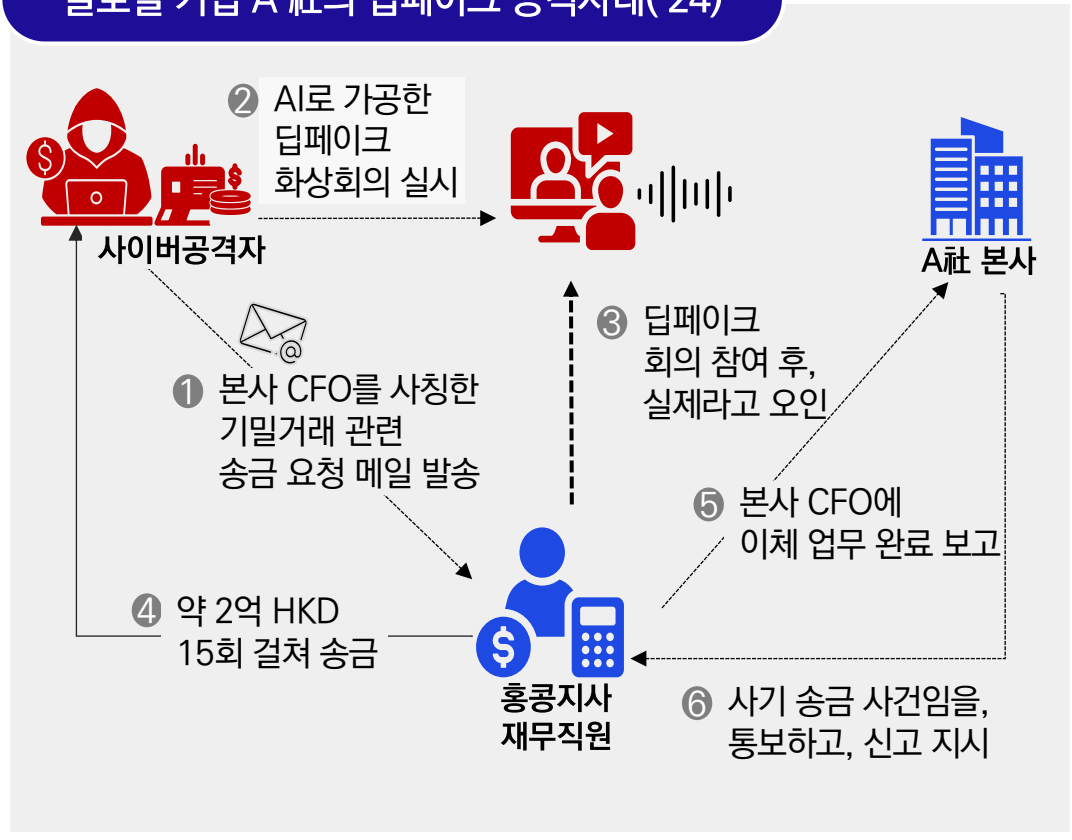
- 주민등록번호와 같은 개인정보에 허위 정보를 결합하여 일반적인 보안절차 또는 고객확인제도를 우회

삼정 KPMG
© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

딥페이크를 통한 허위 금융거래 사례(1)

글로벌 기업 A社 홍콩 지사의 재무직원을 대상으로 ① 본사 CFO를 사칭하는 메일을 발송하고 ② 본사 CFO와 동료를 가짜로 생성한 다자간 영상회의를 통한 사기 수법으로 약 2억 HKD가 인출되는 피해가 발생

글로벌 기업 A 社의 딥페이크 공격사례('24)



(1) World Economic Forum, "'This happens more frequently than people realize': A社 chief on the lessons learned from a $25m deepfake crime", 2025.2.4

삼정 KPMG
© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

GOVERNANCE WATCH

생성형 AI를 활용한 사이버 공격과 대응방안:
딥페이크 공격을 중심으로

사이버 침해로 인한 자금사고 예방을 위한 감사위원회의 질문사항

AI가 확산되는 시대의 내부통제는
독립적으로 검증가능한 프로세스로 구현되어야 합니다.

01	고액이나 비정상 송금이 발생하는 경우 기존의 연락처 등 독립된 채널로 재확인하는 과정을 거치는가?
02	고액의 자금이체가 한 사람의 승인과 판단만으로 완료되지 않도록 복수의 승인절차를 구비하고 있는가?
03	최고 경영진의 긴급한 업무지시도 정상적인 승인절차를 밟도록 내부통제가 설계되고 운영되고 있는가?
04	AI를 활용한 기만이나 사칭 사례들이 지속적으로 임직원 교육에 반영되고 있는가?
05	내부감사부서는 조직 내 잠재적인 딥페이크 취약점을 선제적으로 식별하기 위한 위험평가를 실시하고 있는가?

삼정 KPMG

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.