



딥페이크 시대의 리스크 유형과 대응방안

Deloitte Insights

Deloitte.

Download on the
App Store

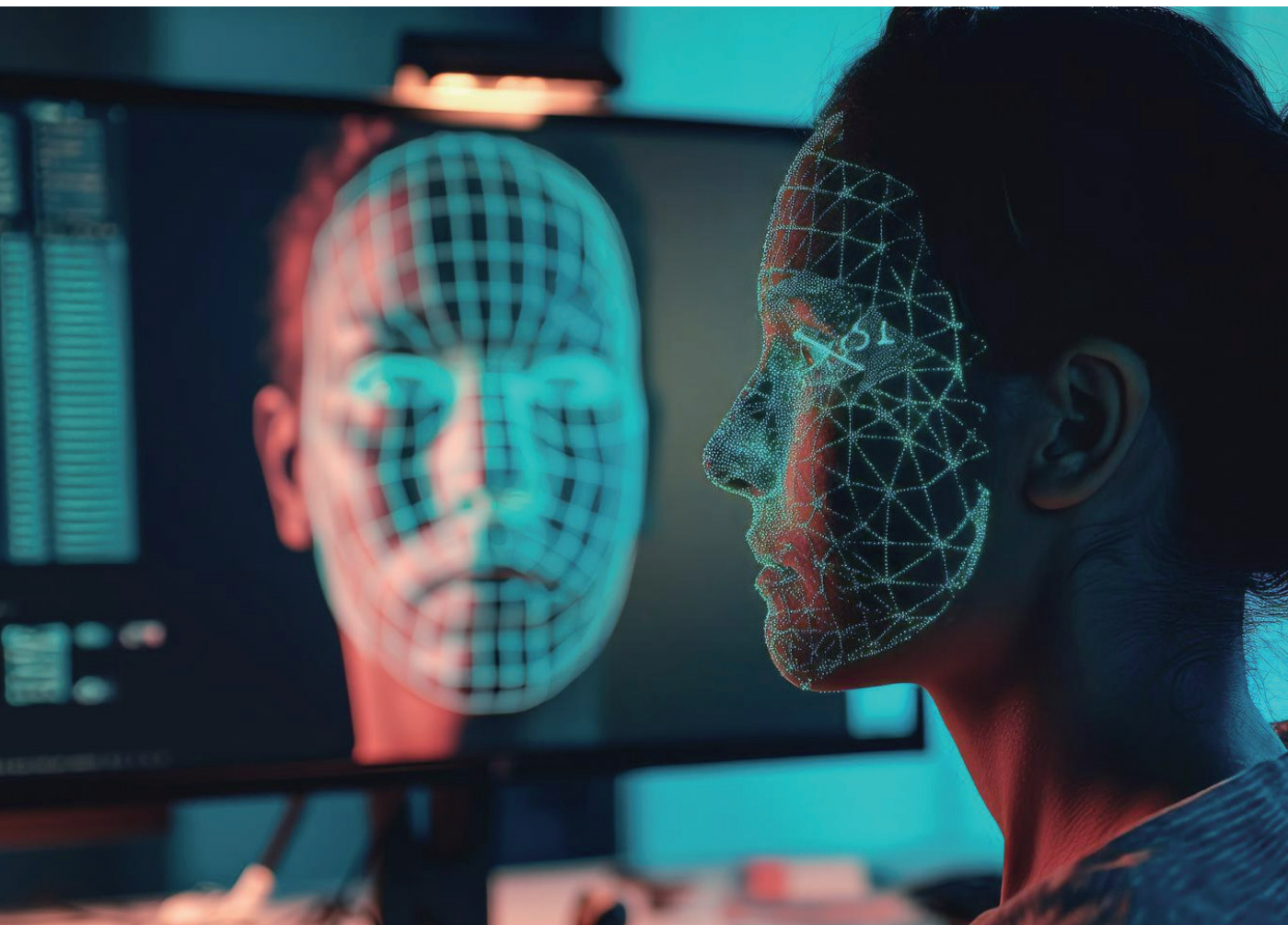
GET IT ON
Google Play



'딜로이트 인사이트' 앱에서
경영·산업 트렌드를 만나보세요!

들어가며

최근 들어, 한국에서 Deep Fake(딥페이크) 문제가 세계적으로 화두가 되고 있다. 한국의 K-pop 아이돌을 대상으로 한 딥페이크 조작 영상이 전 세계적으로 퍼지는 사례가 빈번히 발생했다. 딥페이크 기술을 활용해 아이돌들이 음란물 영상의 주인공이 되는 것처럼 조작되는 것이다. 뿐만 아니라, 한국 일반인 여성과 학생을 대상으로도 딥페이크 음란물 영상이 제작, 유포되면서 글로벌 외신들도 이 현상에 주목하고 있다. BBC는 “최근 미성년자를 포함해 성적으로 노골적인 딥페이크 이미지를 제작하고 공유하는 채팅 그룹이 다수 발견됐다.”고 전하며 한국의 디지털 성범죄가 큰 문제가 되고 있다며 고집었다. 심지어 다른 외신은 한국을 딥페이크 음란물 문제의 '진앙지'로 표현하기까지 했다. 그러나, Deep Fake(딥페이크)와 Synthetic Media(인공미디어 혹은 합성미디어)로 인한 문제는 비단 한국만의 문제는 아니다. 한국의 사례들이 유난히 더 부각되는 것일 뿐이다. 딜로이트와 벤처비트에 따르면, 딥페이크는 지난해 미국에서 무려 3,000%나 증가했다. 올해 딥페이크로 인한 사건은 전 세계적으로 14만~15만건 발생할 것으로 예측했다. 또한 2027년까지 딥페이크 때문에 발생하는 손실액이 연평균 32%증가할 것으로 전망돼 2027년에는 그 손실액이 55조 규모에 달할 것으로 보인다.¹



Deep Fake와 Synthetic Media가 악용될 수 있는 범죄 유형²

Deep Fake(딥페이크) 기술은 Synthetic Media로 가공되어 각 중 범죄를 유발시킨다. Synthetic Media를 활용해 가짜인 것을 사실로 만들고 이를 기반으로 사람을 속여 비밀 정보를 획득하는 범죄가 기하급수적으로 늘어날 수 있는 상황이다.

Synthetic Media가 활용된 여러 유형의 범죄가 발생할 수 있는데, 여기에는 피싱(Phishing), 딥페이크(Deepfake), 프롬프트 인젝션(Prompt Injection), 거짓정보(Misinformation) 등이 포함된다. 유형별로 어떻게 범죄가 발생할 수 있는지 알아보자.

01 발전된 피싱(Phishing) 수법

피싱은 가장 흔한 유형의 사이버 공격이다. 전 세계적으로 매일 34억 개의 스팸 이메일이 발송된다. 2021년 기준으로, 사이버 범죄자들은 피싱 공격을 통해 약 4,420만 달러를 탈취한 것으로 나타났다. 기존의 피싱 공격은 일반적으로 피싱 콘텐츠가 고품질이기 때문에 성공하는 것이 아니라, 대량으로 발송되기 때문에 피싱에 성공하는 경우가 대다수다. 수십억 개의 이메일 중 몇 개는 결국 목표를 달성하게 되는 방식이다. 대부분의 피싱 메일 수신자는 일반적으로 피싱 시도를 알아차릴 수 있는데, 그 이유는 문법과 철자가 부정확하거나 발신자가 수신자를 분명히 모른다는 점 때문이다.

하지만 생성형AI를 바탕으로 한 Synthetic Media 구현 기술이 발전하면서, 피싱을 기획하는 사기꾼들은 설득력 있고 오류가 없는 메시지를 빠르고 쉽게 작성할 수 있게 됐다. 피싱 메일의 내용이 일괄적이지 않고 이메일 내용의 맥락을 정교하게 재구성해, 각 수신자에게 맞춤형으로 메시지를 보낼 수 있게 됐다. 또한 Synthetic Media 콘텐츠를 결합해 피싱을 진짜인 것처럼 조작하는 것이 더 쉬워진다. 이로 인해, 수신자들을 피싱 메일을 쉽게 걸러낼 수 없게 됐고 이러한 상황은 개인과 조직에 막대한 피해를 줄 수 있다.

02 딥페이크(Deepfake)를 활용한 사기

딥페이크 기술은 수년간 존재해 왔지만, 최근까지는 사이버 범죄에 사용될 만큼 충분한 고도화된 수준이 아니었다. 그러나 최근 들어, 영상 및 음성 조작 기술이 발전하면서 대규모 딥페이크 범죄가 발생하고 있다. 예를 들어, 영국에 본사를 둔 모 에너지 기업의 CEO가 딥페이크 AI 음성 기술을 사용하여 회사 모기업의 대표를 사칭한 사기꾼들에 의해 24만 3천 달러를 넘겨주는 사례가 발생했다. 이 사건은 딥페이크를 만드는 각 중 도구들의 수준이 더욱 발전하고 있음을 보여주는 사례다. 앞으로도 딥페이크 구현 기술이 더 빠르게 발전될 가능성이 높아, 일반 사람들이 자신이 누구와 소통하고 누구와 거래하고 있는지 확인하는 것이 더욱 어려워질 전망이다. 시장조사 업체 가트너는 2026년까지 기업의 약 3분의 1이 AI로 생성된 딥페이크로 인해 신원 확인 및 인증 솔루션을 신뢰할 수 없게 될 것이라고 예상하기도 했는데, 이는 딥페이크가 초래할 수 있는 문제의 심각성을 잘 보여준다.³



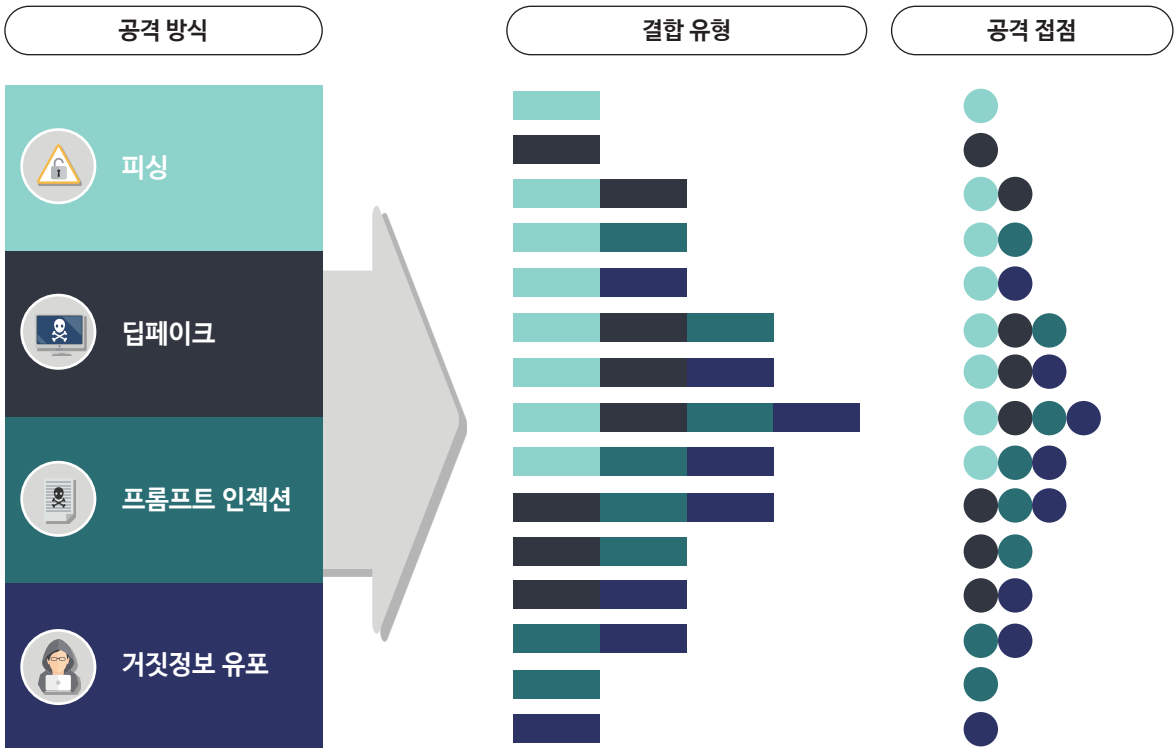
03 프롬프트 인젝션(Prompt Injection)

프롬프트 인젝션은 대형 언어 모델(LLM)에 대한 사이버 공격의 한 유형이다. 범죄자는 생성형AI 툴에 입력되는 악의적인 명령을 합법적인 프롬프트로 위장하여 민감한 데이터를 유출하도록 유도한다. 또한 생성형AI 툴을 조작하거나 잘못된 정보를 유포하기도 한다. 조작된 프롬프트는 각종 정보(연락처 목록, 은행 정보 및 건강 데이터 등)를 전달하도록 지시해 악성 범죄를 유발시킨다. 쉽게 말해 AI 알고리즘에 거짓 데이터를 공급하는 방식이다.

04 거짓정보 유포(Misinformation)

생성형AI 툴은 대규모의 거짓 Synthetic Media 콘텐츠를 신속하게 생성하는 데 악용될 수 있다. 악의적인 행위자들은 이 도구들을 이용하여 특정 기업을 표적으로 삼아 기업 평판을 손상시키거나 주식 가격을 위협할 수도 있다. 과거에는 공격자들이 직접 메시지를 작성해야 했지만, 거짓 콘텐츠 생성을 위한 AI 도구들은 이제 대규모로 잘못된 정보를 만들어내어 대중과 메시지를 실험하고 테스트할 수 있는 능력을 갖게 됐다. 기존에는 거짓 정보 유포를 위해 막대한 비용과 전문인력이 소요됐지만, 이제는 큰 비용이나 전문적 기술 없이도 누구나 기업의 자금과 데이터를 빼앗기 위해 설득력 있는 콘텐츠를 만들 수 있는 것이다. Synthetic Media를 악용해 발생할 수 있는 4가지의 범죄 유형을 알아봤다. 이 범죄 유형들의 더 큰 문제는 특정 유형의 범죄가 개별적으로 발생하는 차원을 넘어서고 있다는 점이다. 4가지 유형이 서로 결합되어 여러 새로운 유형의 범죄가 생겨난다. 이에 따라 사이버 공격을 당하는 점점도 더 증가하게 된다(그림1 참조).

그림1. Synthetic Media가 악용되어 발생할 수 있는 범죄 및 결합 유형



출처: Deloitte (2024), Tech Trend 2024

이와 같이 AI로 인해 Synthetic Media 기술이 나날이 발전해감에 따라 사람들이 진실과 거짓을 구별하는 것이 점점 더 어려워지고 있다. 대다수의 사람들은 AI가 생성한 콘텐츠와 인간이 생성한 콘텐츠의 차이를 구별할 수 있다고 말하지만, 이들은 자신의 판단을 과신하는 경향이 있다. 가까운 미래에, 인간이 만든 콘텐츠와 AI가 만들어낸 콘텐츠를 거의 구별하지 못하는 시대가 올 것으로 예상된다. 그렇다고 해서 Synthetic Media의 등장과 확산을 무조건적으로 억제할 수는 없는 것이 실정이다. Synthetic Media로 인한 긍정적 영향도 크기 때문이다. 결국, 개인과 기업이 Synthetic Media로 인한 부정적 영향에 대응하려면 강력한 기술 개발 및 보안 전략 수립이 필수적이다.



어떻게 대응할 것인가?

AI 기술의 발전으로 Synthetic Media가 확산되면서 많은 위협 요인들이 새롭게 등장하고 있다. 기업들의 정보, 기술, 보안 관련 책임자들은 이러한 변화를 감지하고하고 자신의 기업들이 처한 잠재적 위협 요인에 대해 명확히 인식해야 한다. 기존의 사이버 공격과 Synthetic Media가 시너지를 만들어, 향후에는 더 다양한 유형의 공격이 발생할 것이다.

이 문제들에 대처하기 위해서는 사이버 보안 생태계 파트너들과의 협력이 중요하다. 기업이 자체적으로만 사이버 보안 역량을 증대시켜 잠재적 위협에 대응하는 것은 더욱 어려워지기 때문이다. 기업들은 사이버 보안 측면에 있어, 파트너십과 생태계를 견고히 구축해 날로 다양해지고 규모가 커지는 위협에 미리 대비해야 한다.

이러한 대비는 기업의 고위 경영진에게 있어 매우 시급한 어젠다이다. 2025년까지 온라인 콘텐츠의 최대 90%가 Synthetic Media 콘텐츠로 구성될 것으로 추정된다.⁴ 이 중 많은 부분은 마케팅 및 고객 참여와 같은 합법적인 목적을 위해 사용될 수도 있지만, 사이버 범죄자들은 생성형 AI 도구를 활용해 Synthetic Media를 악용할 가능성이 높다. 기업들은 지금 즉시 Synthetic Media의 확산에 대해 연구하고 대응 전략을 수립해야 한다.

장기적인 관점에 봤을 때도 사이버 보안을 강화하려는 기업들과 Synthetic Media를 악용하려는 범죄자 집단 간의 '고양이와 쥐' 게임은 계속될 것으로 전망된다. 즉, 상호 경쟁이 이뤄지며 Synthetic Media와 관련된 범죄의 확장과 진화는 거듭될 것이라는 의미다.

기업들은 장기적인 관점에서 양자컴퓨팅과 같은 첨단 기술에도 적극 투자해 잠재적 범죄를 미리 예방하는 방안도 고려해야 한다. 양자 기계 학습은 더 적은 양의 훈련 데이터로도 더 정확한 예측 모델을 생성할 수 있는 잠재력을 보여주었다. 양자컴퓨팅이 널리 사용 가능해지기까지는 몇 년이 소요될 것으로 보이나 빠른 속도로 성장하고 있기 때문에, 해커와 기업 모두의 선택 도구로 자리 잡을 가능성이 크다. 철저한 보안전략 수립과 보안 기술 투자로 기업들은 앞으로 직면하게 될 '사이버 팬데믹'을 극복하고 보다 안전하고 신뢰할 수 있는 미래로 나아가는 기반을 다져 나가야 한다.



Deep Fake와 Synthetic Media가 불러일으킬 긍정적 변화

앞선 챕터에서 Deep Fake와 Synthetic Media가 유발시키는 각 중 부정적 영향과 대응 전략에 대해서 알아보았다. 이와는 반대로, 긍정적인 변화에도 주목해야 한다. 특히 미디어/엔터테인먼트 분야에서는 Deep Fake와 Synthetic Media가 적극적으로 활용되면서 긍정적인 변화를 불러일으키고 있다.

툼 행크스가 치아 보철을 홍보하는 광고를 본 적이 있을지도 모른다. 이 광고는 실제로 배우 자신이 촬영에 참여한 것이 아니었다. 누군가 그의 외모를 딥페이크(Deepfake) 기술을 활용해 마치 그가 광고에 출연한 것처럼 보이게 한 것이다.

Synthetic Media의 제작은 딥페이크 기술을 바탕으로 이뤄진다. 딥페이크란 인공지능과 딥러닝 기술을 활용해 실제인지 가상인지 구분하기 어려운 영상, 이미지 등의 콘텐츠를 만들어 내는 기술이다. 딥페이크 시장은 향후 5~6년간 비약적인 성장을 이룰 것으로 보인다. 시장 분석 기관 마켓앤마켓(Markets and Markets)의 보고서에 따르면, 딥페이크 AI 시장은 2024년 약 5억 6,400만 달러에서 연평균 성장률(CAGR) 44.5%를 보이며, 2030년 약 51억 3,400만 달러 규모로 크게 성장할 것으로 전망된다.⁵

딥페이크 콘텐츠를 주축으로 한 Synthetic Media의 확산은 미디어/엔터테인먼트 산업에 긍정적인 변화를 불러일으킬 것으로 보인다. 영화, 드라마를 비롯한 수많은 영상 콘텐츠 제작 과정에서 많은 비용을 절감할 수 있다. 예를 들어 출연료가 매우 비싼 연기자를 섭외하는 대신, 가상의 인물을 AI로 제작해 콘텐츠를 만드는 것이 가능해진다. 또한 배우의 외모를 변형하거나, 특정 장면에서 배우를 대체하는 것도 가능해진다.⁶

미디어와 결합된 커머스 분야에서도 Synthetic Media가 더 큰 역할을 할 것으로 보인다. 최근 화두가 되고 있는 몰입형 고객경험을 제공하는 데에도 있어도 Synthetic Media는 큰 도움이 된다. 특정 고객의 성향과 특성을 반영하고 빠르게 맞춤형 콘텐츠를 제작해 고객 참여도와 브랜드 인지도를 높일 수 있다. 또한, 인플루언서의 이미지를 합성하여 이전보다 더 효과적인 광고 및 프로모션 캠페인을 진행할 수 있을 것으로 보인다.

이러한 단편적인 장점들을 넘어, Synthetic Media의 등장을 새로운 미디어 시대의 서막이라고 평가하기도 한다. Synthetic Media의 등장과 함께 '미디어 3.0 시대'가 열린 것이다. 과거 미디어 1.0 시대에는 소수의 전문 제작자들만 콘텐츠를 생산할 수 있는 시대였다. 미디어 2.0은 여러 콘텐츠 생산 인프라가 발전하면서 제약 없이 누구나 콘텐츠 크리에이터이자 1인 미디어가 될 수 있는 기회를 얻는 시대를 가리켰다. 더 나아가 미디어 3.0은 AI 기술이 더해지면서 콘텐츠와 미디어가 더 다양화되고 새로운 시장이 만들어지는 Synthetic Media의 시대가 열리는 걸 의미한다.⁷

기업들은 Deep Fake와 Synthetic Media가 불러일으키는 각 중 부정적 영향에 사전적으로 대응할 수 있는 전략을 수립하고 실행해야 한다. 정반대의 측면에서, Deep Fake와 Synthetic Media 덕분에 새롭게 열리는 미디어 3.0의 시대에 어떻게 새로운 부가가치를 창출할 지 고민해야 하는 시점이다.



주석

1. AI 타임즈 (2024.07.02), "딥페이크 손실 규모 2027년 55조 추정...연평균 32% 급증"
2. Deloitte (2024), Tech Trend 2024
3. CIO Korea (2024.05.03), '다가온 사이버 팬데믹'... AI 딥페이크와 보안 및 신원 확인의 미래
4. Deloitte (2024), Tech Trend 2024
5. Markets and Markets (2024.07.04), Deepfake AI Industry worth \$5.13 billion? by 2030
6. GTT Korea (2024.07.07), AI와 개인화 콘텐츠 급증 '딥페이크 AI' 시장 파죽지세
7. 언론중재위원회 (2023), 합성 미디어의 부상과 미디어 3.0



딜로이트 산업 전문가

사이버 보안 및 리스크, 통신·미디어·엔터테인먼트, 디지털 고객경험(DCX) 및 마케팅

딜로이트는 사이버 리스크 대응을 위한 정보보호 및 개인정보보호 자문, 정보보안 인증, 기술적 취약점 진단 및 대책 수립, 정보보호 전략 수립, Cyber Incident 대응 등의 서비스를 제공하고 있습니다. 수많은 유형의 리스크를 사전에 방지해 기업 운영의 든든한 조력자 역할을 수행합니다. 딜로이트는 또한 통신·미디어·엔터테인먼트 분야에서도 기업들의 전략적 과제와 혁신을 함께해왔습니다. 다양한 배경을 가진 구성원들로 이뤄진 팀은 심도있는 인사이트를 제공하고 있습니다.

사이버 보안 및 리스크



서영수 파트너

Cyber 본부 |
Cyber Risk & Compliance

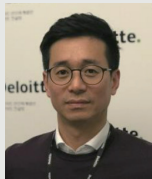
Tel: 02 6676 1929
Email: youngseo@deloitte.com



유선희 파트너

Cyber 본부 |
Cyber Risk & Compliance

Tel: 02 6676 2956
Email: sunhyou@deloitte.com



이상훈 이사

Cyber 본부 |
Cyber Risk & Compliance

Tel: 02 6676 2937
Email: sanghunlee@deloitte.com

통신·미디어·엔터테인먼트



박형곤 파트너

통신·미디어·엔터테인먼트 산업 리더 |
컨설팅 부문

02 6676 3684
Email: hypark@deloitte.com



구나경 이사

통신·미디어·엔터테인먼트 산업 |
컨설팅 부문

02 6676 3888
Email: nkoo@deloitte.com

디지털 고객경험(DCX) 및 마케팅



김태환 파트너

디지털 고객경험 |
컨설팅 부문

02 6676 3756
Email: taehwankim@deloitte.com



이대의 파트너

디지털 고객경험 |
컨설팅 부문

02 6099 4892
Email: daelee@deloitte.com



김윤석 이사

디지털 고객경험 |
컨설팅 부문

02 6676 2408
Email: younskim@deloitte.com



강윤정 파트너

디지털 홍보마케팅 |
PR GATE

02 792 2633
Email: yunjekang@deloitte.com



앱



카카오톡 채널



'딜로이트 인사이트' 앱과 카카오톡 채널에서
경영·산업 트렌드를 만나보세요!

Download on the
App StoreGET IT ON
Google Play

Deloitte.

Insights

성장전략부문 대표

손재호 Partner

jaehoson@deloitte.com

딜로이트 인사이트 리더

정동섭 Partner

dongjeong@deloitte.com

딜로이트 인사이트 편집장

박경은 Director

kyungepark@deloitte.com

연구원

양원석 Senior Consultant

wonsukyung@deloitte.com

디자이너

박근령 Senior Consultant

keunrpark@deloitte.com

Contact us

krinsightsend@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

본 보고서는 저작권법에 따라 보호받는 저작물로서 저작권은 딜로이트 안진회계법인("저작권자")에 있습니다. 본 보고서의 내용은 비영리 목적으로만 이용이 가능하고, 내용의 전부 또는 일부에 대한 상업적 활용 기타 영리목적 이용시 저작권자의 사전 허락이 필요합니다. 또한 본 보고서의 이용시, 출처를 저작권자로 명시해야 하고 저작권자의 사전 허락없이 그 내용을 변경할 수 없습니다.