금융 메타버스(Metaverse), 사이버위협 동향과 대응방안

- 국내외 금융사 메타버스 사업현황, 사이버위협 분석, 대응방안 -

메타버스는 최근 정보기술(IT)업계에서 가장 큰 화두였고, 페이스북은 사명을 메타로 바꾸면서 메타버스에 대한 강한 의지를 보이고 있으며, 마이크로소프트 역시 기업용 메타버스 솔루션 '메시 포 팀스'(Mesh for Teams)를 발표하였습니다. 국내외 금융사들은 메타버스를 활용한 디지털금융을 실현시키기 위한 사업을 활발하게 추진하는 등 금융권에서도 메타버스는 매우 중요한 신사업 분야의 하나로 자리잡고 있습니다.

그러나, 지난해 5월 유명 메타버스 플랫폼인 '로블록스(Roblox)' 사용자들의 개인정보가 해킹을 당하는 등 메타버스도 해킹의 위험성을 피해갈 수 없는 것이 현실입니다. 과학기술정보통신부와 한국인터넷진흥원(이하 "KISA")은 「'21년 사이버위협 분석 및 '22년 전망 분석」에서 2022년 예상되는 주된 사이버 위협으로 '메타버스, NFT, AI 등 신기술 대상 신종위협'을 들었습니다.

이번 뉴스레터에서는, 금융권 메타버스의 동향과 함께 사이버위협 요소를 살펴보고, 향후 전망에 대해 설명드리겠습니다.

1. 금융사 메타버스 최신동향

메타버스는 금융권에서 디지털금융으로 가는 핵심 모멘텀 역할을 할 것으로 기대되고 있습니다. 메타버스를 활용해서 사내 행사를 개최하고 다양한 금융상품 등을 출시하고 있으며, 특히, 메타버스 영업점 개설까지 계획하고 있습니다. 즉, 가상세계인 메타버스안에 금융권 영업점 사무공간을 실제와 동일하게 옮겨 놓는 형태입니다. 영업점이 그대로 가상현실로 옮겨지는 만큼, 예적금 가입, 대출상담 등 물리적 공간인 실물 영업점에서 이루어지는 모든 금융거래가 메타버스상에서 이루어질 수 있는 획기적인 디지털금융 서비스라고 할 수 있습니다. 이미 글로벌 금융사는 메타버스 시대를 대비, 상담과 디지털 체험에 특화된 점포 구축에 돌입했으며 "메타버스 기술은 스마트폰의 한계를 넘어 온·오프라인 연결이라는 기술적 특성을 바탕으로 금융업의 업무방식, 고객 니즈, 서비스를 근본적으로 변화시킬 것"이라고 전망됩니다.

1) 국내 주요 금융사 메타버스 사업현황

구분	주요 동향
신한은행	자체 플랫폼 '신한 쏠버스', 바이브컴퍼니와 부동산 특화 메타버스 플랫폼 사업
IBK 기업은행	싸이월드제트 영업점 'IBK도로리은행'
NH농협은행	자체 플랫폼' 독도버스'
삼성화재	자체 플랫폼서 신규브랜드 '착' 출시
신한카드	제페토 네이버제트 특하 선불카드 출시

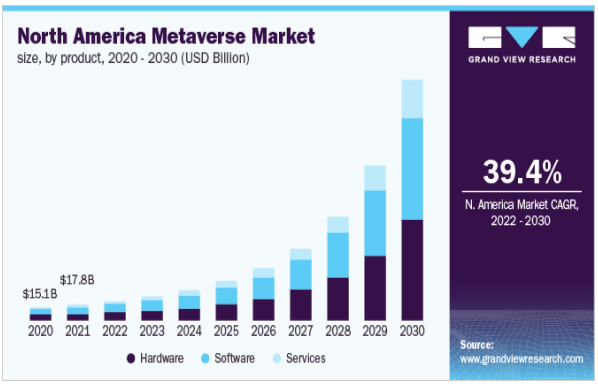
>> 다음페이지에 이어서

하나카드	제페토 하나카드 월드 개장
국민은행	KB메타버스 VR 브랜치 테스트베드 구축, 로블록스서 KB금융타운 베타 실험
하나은행	우리 소상공인 종합지원센터 메타브랜치 오픈
NH투자증권	나무 프리미엄 서비스 일환으로 'NH투자증권 메타버스' 오픈

2) 국외 금융권 메타버스 사업동향

지난 4월에는 미국 최대 은행인 JP모건이 블록체인 기술 기반 가상세계 디센트럴랜드(Decentraland)에 라운지 오픈하며, 메타버스에 최초로 진입한 대출기관이 되는 등 전세계 금융권에서 메타버스를 통한 디지털금융시장 개척은 앞으로 더욱 활발해질 것으로 전망됩니다. 글로벌 메타버스 시장 규모는 2021년 미화 388억 5천만 달러로 추산되었습니다. 2022년부터 2030년까지 연평균 복합 성장률(CAGR) 39.4%로 확장될 것으로 예상됩니다. 또한 UN에 따르면 2018년 글로벌 디지털 경제는 총 GDP의 15.5%를 차지했으며 2021년까지 15%에서 16.8%로 예측되었습니다. 주요 메타버스 솔루션 제공업체의 경영진에 따르면, 메타버스로 전환하는 디지털 경제의 비율과 전체 시장 확장의 비율에서 메타버스의 잠재적 시장 기회는 3조 7500억 달러에서 12조 4600억 달러 사이로 추정됩니다.

<JP모건 메타버스 디지털금융 런칭 화면>



<북미 메타버스 시장현황>

2. 금융사 메타버스 사이버위협 동향

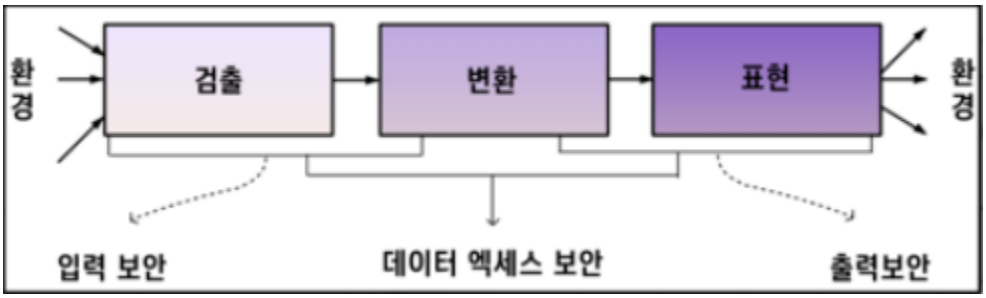
1) 메타버스 주요기술 보안 위험 요소

메타버스의 주요기술은 AR과 VR이고, 관련논문[1]에 따르면, 메타버스 정보보호를 입력보안, 데이터 엑세스보안, 출력보안의 3가지 항목으로 분류를 하고 있습니다. 첫째 입력보안은 AR과 VR에사용되는 HMD의 사용자 데스크톱 화면에서 중요한 정보 캡처가 가능하고, 주민등록증 또는 신용카드와 개인정보 유출 위험성이 존재합니다. 둘째, 데이터 엑세스 보안에서는 AR, VR의 대상을 변조하여 시스템으로부터 다른 반응을 이끌어내거나 서비스를 완전히 거부할 수 있는 위험성이 있습니다. 특히, 데이터 스토리지에는 변조, 무단 엑세스 및 스푸핑(Spoofing)[2] 과 같은 고유한 보안 위협성이 내재되어 있습니다. 셋째, 출력 보안에서는 사용자 안전을 저해할 수 있도록 출력이 변조되거나 스푸핑 될 수 있는 위험성과 함께, 서비스 거부 등의 위험성이 존재하고 있습니다.

1 Guzman J.A, Thilakarathna K & Seneviratne A, "Security and Privacy Approaches in Mixed Reality: A Literature Survey", ACM Computing Surveys, vol52, No 6, pp. 1-37, Jan. 2020.

2 공격자가 네트워크, 웹사이트 등의 데이터 위변조를 통해 정상 시스템인 것처럼 위장하여 일반 사용자를 속이는 해킹 기법.

>> 다음페이지에 이어서



<메타버스 주요기술 AR&VR 보안 파이프라인>

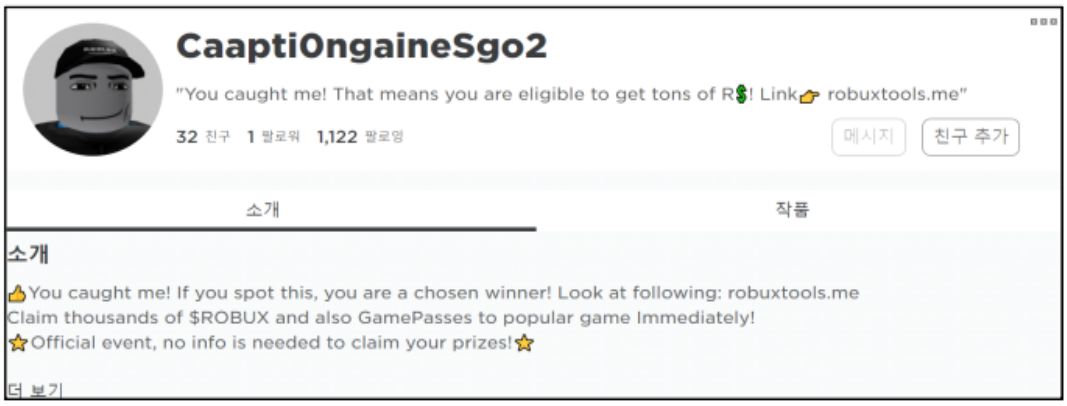
2) 메타버스 환경의 해킹 등 사이버 위협 요소분석

공격대상	내용
인프라 및 시스템	① 가상환경 플랫폼 및 시스템(AR·VR S/W, 플랫폼·데이터 관리 시스템 등)에 대한보안 위협 - 가상환경 S/W 및 플랫폼 시스템 등에 대한 Zero Day 공격, 악성코드/랜섬웨어 유포 등 ② 가상환경·메타버스 서비스 구축, 관리, 서버 등 인프라에 대한 물리적 및 S/W 보안 취약점에 따른 위협 ③ 메타버스 플랫폼 및 서비스 이용을 위한 WEB, 어플리케이션 등 취약점으로 인한 보안 위협
네트워크	① 가상환경·메타버스-서비스이용자 間 정보 송수신 네트워크 취약점을 이용한 정보탈취 및 시스템 해킹, 서비스 공격 - DoS/DDoS 공격, 웹(MAC Spoofing, DNS Spoofing 등) 및 클라이언트 취약점 등
데이터	① 가상환경·메타버스 플랫폼, 서비스 시스템에 저장된 개인정보, 콘텐츠 등 데이터 위·변조 및 유출, 개인정보 암호화 또는 가명처리 미흡 등 ② 아바타, 게임머니, 포인트, NFT 등 가상자산에 대한 탈취 및 불법 복제 등 보안 위협
서비스	⑦ 가상환경, 메타버스 이용 단말기·디바이스 펌웨어 취약점, 보안패치 미적용 또는 패치파일 자체 취약점에 따른 보안 위협 ⑧ 실시간으로 수집되는 개인정보, 위치정보, 민감정보 및 프라이버시(생체, 활동) 유출에 따른 사생활 침해 및 개인정보 보호, 데이터 변조(신원 사칭 등) 위협

< 메타버스 보안 위협 이슈 종류 및 내용(KISA자료) >

메타버스 환경의 정보보호 위협요소를 정리하면 위 표와 같습니다. 조금 더 구체적으로 메타버스 환경의 정보보호 위협요소를 설명하면, 메타버스는 개인정보 및 콘텐츠 등 그 대상이 되는 데이터에서 정보보호 위협이 발생하는데, 즉 메타버스 플랫폼의 인프라 및 시스템, 네트워크, 데이터(DB) 등에서 취약성을 이용한 악의적인 공격(해킹) 위협 발생이 가능하고, 구체적으로는 서비스 마비, 플랫폼 환경 조작, 시스템 탈취 등을 목적으로 하는 해킹기법이 메타버스 해킹위협 요소입니다. 특히, 메타버스 서비스 영역에서는 서비스 콘텐츠, 이용자정보 대상 해킹으로 개인정보의 유출, 콘텐츠 및 플랫폼 정보 위·변조 등의 위협이 발생가능한 상황입니다. 실제 주요 사례를 찾아보면 1) 기기 보안에서 메타버스 헤드셋, IoT 등 하드웨어 기기의 보안 취약점을 악용한 해킹과 2) 신원 사칭에서 메타버스 내 딥페이크 기술로 인한 정보 도용 및 가짜뉴스 3) 사이버 피싱으로 로블록스(Roblox) 내 피싱사이트 접속을 유도하는 봇 유저가 성행하고 있습니다.

>> 다음페이지에 이어서



<피싱사이트에 접속하도록 유도하는 봇 화면>

3) 국내 디지털금융 사이버위협 대응현황

금융당국에서는 금융산업이 디지털로 전환되는 과정에서 발생가능한 디지털 리스크로부터 사용자의 재산과 데이터를 안전하게 보호하고 안정적으로 금융기능을 수행하기 위해서 금융시스템 전반의 정보보호역량 강화를 강조하고 있습니다. 법률적으로는 전자금융거래법 개정안(21.11월)을 통해 디지털 리스크에 비례한 자율적 보안을 위해 원칙 중심의 규제(Principles-based regulation)를 선언하고, 금융보안 거버넌스 확립을 위한 이사회의 책무, 금융보안계획 수립·제출 의무, 금융보안 규제, 개선·합리화를 위한 금융보안 상시평가제 도입, IT아웃소싱 규제 강화 등의 내용을 추진하고 있습니다. 금융보안 강화를 위한 구체적인 사례로는 금융사 대상으로 '정보보호 상시평가제도','금융권 사이버위협 정보공유 체계운영'과 더불어 195개 금융회사 및 전자금융업자를 대상으로 '해킹침해사고 대응훈련' 실시하고, 자산규모가 2조원 이상이거나 IT 의존도가 높은 금융회사에 대해서는 'IT리스크 계량평가'를 실시하는 등 금융사의 안정적인 사이버위기 관리능력을 제고하기 위한 제도적, 기술적 대응방안을 추진하면서 메타버스 등 디지털금융 관련하여 적극적인 대응을 요구하고 있습니다.

3. 향후 전망: 안전한 사이버환경에서 구현되는 메터노믹스를 향하여

메타노믹스(Metanomics)는 Metaverse와 Economics의 합성어로 메타버스를 통해 일반화될 가상경제(Virtual Economy), 증강경제 (Augmented Economy) 및 그를 혼합한 혼합경제(Mixed Economy)를 함께 이르는 용어입니다. 구체적으로 금융분야와 관련하여 메타버스 내 독자적인 지급·결제 체계, 여·수신, 보험, 투자 등 새로운 금융서비스에 대한 수요 및 시장 형성으로 이어질 것이라고 전망하고 있습니다. 그에 따라 새로운 체계 내에서 개인 생체·민감정보의 안전한 관리에 금융사에서는 각별히 운영·관리 할 필요가 있습니다. 즉, 비대면·가상세계에 익숙한 Z세대 중심으로 인터넷뱅킹, 모바일뱅킹을 잇는 차세대 디지털금융 채널로서 메타버스는 앞으로도 더욱 주목받을 분야이면서 동시에 해킹 등 보안위협이 고스란히 존재하기 때문에 메타버스를 통한 디지털금융을 구현하고 운영할 때 인프라 및 시스템, 네트워크, 데이터, 서비스 각 분야별로 정보보호 직간접적인 해킹사고를 사전에 예측하고 각 기업에서는 정보보호체계 개선, 모의해킹, 보안취약점 점검 등 기술적 리스크 관리를 강화하기 위한 노력이 더욱 필요합니다. 특히, 개인정보보호법, 정보통신망법, 신용정보법 등 정보보호 관련 법률 정책적 리스크 관리는 사전에 철저하게 점검하고 검토하여, 만약에 불의의 해킹사고가 발생하더라도, 신속하게 기업의 정보시스템 및 서비스를 복구하고, 효과적인 전방위적 법률대응을 할 수 있도록 대응하는 것이 필요합니다.

>> 다음페이지에 이어서

법무법인(유) 화우 디지털금융팀은 금융의 디지털 전환과 관련하여 디지털 신기술, 신사업 등 다양한 영역에서 깊이 있는 자문을 제공하고 있습니다. 메타버스 등 디지털금융 등 신사업 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹진단, 보안취약점) 등 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 연락하여 주시기 바랍니다.

Contacts

이광욱 변호사
kwlee@yoonyang.com
02-6003-7535

이주용 변호사
jyleei@yoonyang.com
02-6003-7546

이근우 변호사
klee@yoonyang.com
02-6003-7558

최용호 변호사
yhchoi@yoonyang.com
02-6182-8396

주민석 변호사
msjoo@yoonyang.com
02-6003-7521

백재환 전문위원
jhb@yoonyang.com
02-6182-8366