메타버스 기술과 보안 위협 및 대응방안

우성희 · 이효정*

한국교통대학교

Metaverse Technology and Security Threats and Countermeasures

SungHee Woo · HyoJeong Lee*

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr / leehj@ut.ac.kr

요 약

현재 다양한 분야에서 메타버스를 도입하고, 콘텐츠 또는 아이템 등의 거래에 NFT를 사용하는 가상융합경제가 등장하여 ‘메타버스 환경’으로 발전할 것으로 전망하고 있다. ‘메타버스 환경’은 앞으로 우리사회의 변화를 주도할 것이며 AI, 빅데이터, 클라우드, IoT, 블록체인, 차세대 네트워크 기술과 융합될 것이다. 하지만 메타버스 이용자가 서비스 이용을 위해 제공하는 개인정보, 기기정보, 행위정보는 주요 공격대상 된다. 따라서 사용자의 안전한 이용 환경 제공과 관련 기업의 비즈니스 기반 확대를 위하여 민·관 협력체계 구축 및 보안 가이드 개발이 선두과제이다. 따라서 본 연구에서는 메타버스 특징과 기술을 비교분석하며 이에 발생할 수 있는 보안 위협과 대응방안을 살펴본다.

ABSTRACT

Currently, the Metaverse is introduced in various fields, and a virtual convergence economy that uses NFTs for content or item transactions is expected to develop into a 'metaverse environment'. The ‘metaverse environment’ will lead the changes in our society in the future and it will be fused with AI, big data, cloud, IoT, block chain, and next-generation network technology. However, personal information, device information, and behavior information provided by Metaverse users to use the service are subject to major attacks. Therefore, in order to provide a safe environment for users to use and to expand the business base of related companies, building a public-private cooperation system and developing a security guide are the leading tasks. Therefore, in this study, we compare and analyze metaverse features and technologies, and examine possible security threats and countermeasures.

키워드

Metaverse, NFT, Information Security, AI

Ⅰ. 서 론

메타버스(Metaverse)란 아직까지 고정되거나 확립되어 있지 않지만 일반적으로 가상, 추상을 의미하는 ‘메타(meta)’와 현실세계를 의미하는 ‘유니버스(universe)’의 합성어로 통용되며 현실과 가상의 경계가 모호한 3의 경계지역을 의미한다. 지금 가상환경(VR), 증강현실(AR), 혼합현실(MR)을 아우르는 확장현실(XR)이 보편화되고 있다. MZ세대는 메타버스에서 자신의 아바타를 사용하여 친구를 사귀고, 물건을 구매, 게임, 대화, 모임을 넘어 경제·사회·문화적으로 많은 활동을 하고 있다. 비대면 소통이 확산, 온라인 활동이 줄어든 지금, 사람들은 현실 세계와 비슷한 사이버공간에서 간접적인 만족을 느끼고 있다[1][2].

정부에서 올해 메타버스 분야에 5,560억원을 투자하고 2026년 세계 5위를 목표로 한다는 신산업 선도전략을 발표하면서 메타버스 개발에 많은 관심을 가지고 있으며 미국은 일찍부터 XR 기술 관련 연구를 진행했으며, 국토안보부는 응급상황에 대한 대응 훈련인 가상훈련플랫폼 EDGE(Enhanced Dynamic Geo-Social Environment)를 사용하고 있다. 유럽에서는 EU 차원의 XR 기술개발을 진행하고 있으며, 특히 영국은 4대 디지털 핵심 기술로 XR

* corresponding author

을 선정하였다. 현재는 게임 및 미디어 산업뿐만 아니라 전시, 공연 산업부터 미디어, 패션 디자인 등의 분야까지 넓게 확장하고 있다. 이외에 중국과 일본도 XR 기술개발에 집중하고 있다. 하지만 이에 앞서 발생가능한 여러 측면에서의 보안체계나 가이드가 마련되어야 할 것이다[3][4]. 따라서 본연구에서는 메타버스 특징과 기술을 비교분석하며 이에 발생할 수 있는 보안 위협과 대응 방안을 살펴본다.

II. 메타버스 특징과 기술

메타버스는 현실과 동떨어진 세계가 아닌 다음과 같은 가상 세계(Virtual Worlds), 거울 세계(Mirror Worlds), 증강 현실(Augmented Reality), 라이프로깅(Lifelogging)으로 구분되며 또한 연계, 공존, 융·복합된 공간이다. 메타버스의 특징과 핵심기술을 보면 다음 표1, 표2와 같다.

표 1. 메타버스 특징

구분	특징	예
가상세계	- 현실과 유사하나 대체 세계를 디지털 데이터로 구축 - 사용자 모습이 투영된 아바타 간의 상호작용을 기반 - 아바타를 통해 현실 세계와 유사한 사회, 경제, 문화적 활동가능 - 실시간으로 다양한 콘텐츠를 생성, 공유, 유통가능 -구현에 그래픽 기술과 5G, 네트워크, 인공지능, 블록체인기술 사용	세컨드라이프, 마인크래프트(Minecraft), 로블록스, 제페토(Zepeto), 포토나이트, 동물의 숲
거울세계	- 디지털 트윈 기술을 활용, 현실 세계를 그대로 복제한 디지털 세계 - 복제의 대상은 현세상이고 여기에 3차원 공간에 대한 고정밀 매핑 - 데이터 처리 자동화를 위한 AI, 모델링 및 주석 도구, 라이프로깅 기술 등이 사용, 더욱 현실감 있는 정보 제공	- 디지털 세계에서 누릴 수 있는 사용자 경험을 극대화. - 카카오맵 - 구글어스 - 에어비엔비
증강현실	- GPS 정보와 네트워크를 활용해 현실 세계에 가상의 사물과 인터페이스를 덧씌워 만든 혼합 현실 - 현실과 가상의 결합, 실시간 상호작용, 현실 세계에서 가상의 대상물의 정확한 배치라는 3가지 특징 기반 - 실재를 대체하는 것이 아닌, 보완.	- 스카이 가이드, - 이케아 가구 배치 시뮬레이션 - 위치 기반 AR 게임인 포켓몬고
라이프로깅	- 인간의 신체와 감정, 행동, 의사소통, 관찰 등 일상생활 정보를 웨어러블 기기나 센서로 수집, 처리, 반영해 기록, 가상 공간에 재현하는 활동 - 개인의 정보를 디지털 및 데이터화 하여 가치 있는 정보로 만들기 위한 첫 단계.	- 페이스북 - 카카오스토리

표 2. 메타버스 핵심기술

핵심기술	특징	응용사례
XR	- 가상 현실(VR)과 증강현실(AR), 혼합 현실(MR)을 통칭하며, AR/VR 콘텐츠를 생성할 수 있는 소프트웨어와 하드웨어, 인터페이스를 모두 포함. - 상호작용을 통한 몰입감과 다양한 경험을 제공. XR 중에서도 365도 가상 뷰와 공간 음향은 현실과 가상 간의 인지적 부조화를 최소화하여 실제와 같은 환경'을 조성.	- 게임과 엔터테인먼트를 넘어 제조, 의료, 교육, 유통, 문화, 국방 등 많은 산업군에 적용
5G, MEC, 엣지컴퓨팅	- 기존 엣지 컴퓨팅이 다양한 네트워크 구조에 적합한 형태로 진화한 것. - 낮은 전송 지연과 짧은 응답 시간이 필수인 메타버스 개발을 위한 핵심 기술로 대두 - 중앙 클라우드에 집중되는 컴퓨팅 트래픽을 네트워크의 가장자리, 즉 최종 사용자와 근접한 곳으로 분산해 통신 데이터 처리 경로를 최소화.	- 초저지연, 초고속, 초연결이라는 5G의 특징이 극대화, - 외부와 분리된 독립망으로 개인정보보호 기능과 통신 안정성이 강화된 5G 서비스가 구현
블록체인	- 탈중앙화된 방식으로 변조 불가능하고 추적·감사 가능한 거래 장부를 만들어 거래, 행위 부인 및 내용 변조를 차단하는 기술	-메타버스에서 디지털 네이티브 상품을 만들 수 있고, 소유권을 증명하는 등 경제활동가능
디지털트윈	-현실에 존재하는 사물과 기계, 장비, 건물, 교통망 등 물리적 대상을 디지털로 똑같이 구현 .-컴퓨터 모델링과 시뮬레이션을 통해 특정 상황에 대한 결과를 예측할 수 있는 기술	- 잠재적 리스크를 예방하는 데 목적 - 미션 크리티컬한 산업에서 의사결정과 제어 서비스에 신뢰성 제공
사물인터넷	- 주로 데이터 생성 및 수집에 사용 - 메타버스를 구현하는 데에는 '지능형 IoT' 및 '자율 주행 - 개인이나 산업에 특정 사물의 상태 정보 전달, 취합한 데이터를 바탕으로 맞춤형 특화 서비스를 제공.	

III. 메타버스 보안위협과 대응방안

3.1 보안위협

메타버스 보안위협은 개인정보, 콘텐츠 등 데이터를 대상으로 발생한다. 메타버스의 환경 보안위협은 주로 서비스 마비, 플랫폼 환경 조작, 시스템 탈취 등을 목적으로 하는 해킹 위협이며 메타버스 서비스 영역에서는 서비스 콘텐츠, 이용자 정보 대상 해킹으로 개인정보의 유출, 콘텐츠 및 플랫폼 정보 위변조 등의 위협이 발생한다[1-4]. 보안 위협요소와 종류를 보면 다음 표3과 같다.

또한 보안 위협의 사례로 기기보안, 신원사칭, 사이버 피싱을 보면 다음 표4와 같다.

표 3. 메타버스 주요 사이버 위협 종류

사이버 위협		
대분류	중분류	세분류
공급자	시스템	- 가상세계(AR, VR S/W 등)시스템/플랫폼 보안 위협
	기기/인프라	- 가상세계 구축&관리 기기, 인프라 취약점 위협 - WEB 및 메타버스 어플리케이션 보안 취약점 등
	데이터	- 개인정보 침해 - 데이터 위·변조 및 탈취 - 아바타, 가상머니, 포인트 등 가상자산에 대한 탈취 및 불법 복제 위협 등
	네트워크	- 웹 취약점 공격(ARP Spoofing, MAC Spoofing 등)
이용자	서비스 이용 보안이슈	- AR, VR 기기(모바일 디바이스)의 보안 위협 - 프라이버시 위협(생체정보, 행동정보 등) 등

표 4. 보안 위협 사례

보안 위협 사례	설명
기기보안	메타버스 헤드셋, IoT 등 하드웨어 기기의 보안 취약점을 악용한 해킹
신원사칭	메타버스 내 딥페이크 기술로 인한 정보 도용 및 가짜뉴스 등
사이버피싱	로블록스(Roblox) 내 피싱사이트 접속을 유도하는 봇 유저

3.2 대응방안

메타버스는 새로운 패러다임의 주요 기술로 성장중에 있으며 현실 세계와 가상세계를 연결하는 기술에서 경제·사회·문화를 주도하는 핵심기술이 될것으로 기대된다. 다양한 분야에서 메타버스를 도입하고, 콘텐츠 또는 아이템 등의 거래에 NFT를 사용하는 가상융합경제가 등장하여 '메타버스 환경'으로 발전할 것으로 전망되며 '메타버스 환경'은 향후 우리 사회의 변화를 주도할 것으로 보이며 여기에 AI, 빅데이터, 클라우드, IoT, 블록체인, 차세대 네트워크 기술의 융합이 매우 중요하다고 볼수 있다. 하지만 증가하고 있는 메타버스와 NFT 대상 사이버 위협 및 보안 사고에 대한 조기 대응과 보안 위협 사례 공유·분석 및 대응책 마련을 위한 민·관 협의체 구성이 필요하다. 메타버스와 NFT 기반의 서비스가 출시되고 MZ세대를 중심으로 이용자가 증가함에 따라 이들을 대상으로 하는 공격 증가하고 있으며 경제·사회 전반에 메타버스·NFT 활용이 확대됨에 따라 관련한 보안 이슈 발굴 및 대응책 마련이 또한 필요하다. 즉, 가상세계와 현실세계에서 동일한 위협이 함께 발생하는 "위협의 동기화" 예방을 위한 법·제도적 검토 필요하다[1-4]. 따라서 보안 위협에 대한 고려 및 대응 방안을 살펴보면 다음 표5와 같다.

표 5. 대응방안

	대 응 방 안
메타버스 보안 위협 대응	- 메타버스 사용자 자신의 개인정보와 금융정보 보호 등에 주의 -기존 ICT 보안정책 및 기술을 적용, 메타버스 상호연계를 위해 특화되고 확장 가능한 유연한 보안관리 정책의 수립과 운영. -실감 콘텐츠 보안모델 및 정보통신기반시설 보호지침, ISMS-P 등 VR·AR과 정보시스템 보안강화
메타버스 가상생태계 보안 위협 대응 방안	- 가상세계의 아바타, UGC, 디지털 자산 등 가상 생태계에서는 이용자 개인정보 및 디지털 자산의 악용 방지를 위한 인증, 보안관리체계 강화와 이용자의 보안인식 제고
메타버스 플랫폼 보안 위협 대응 방안	- 메타버스 서비스의 개발 및 운영 과정에서 발생 가능한 보안위협 완화를 위해 SW 개발보안, 개발사 보안정책 수립, 관리자 접근제어 등의 서비스 제공 사업자의 보안 적용
메타버스 인프라 보안 위협 대응 방안	- 메타버스의 가상세계를 이용하기 위한 이용기기와 네트워크, IT인프라는 기존 정보시스템, IoT 보안 정책 적용, 데이터 및 서비스 보호를 위해 보안기술 적용.

Ⅳ. 결 론

정부에서 올해 메타버스 분야에 5,560억원을 투자하고 2026년 세계 5위를 목표로 한다는 신산업 선도전략을 발표하면서 메타버스 개발에 많은 관심을 가지고 있다. 현실세계를 가상세계로 옮겨 구현하는 메타버스는 사이버 범죄 및 위협의 다양한 유형이 존재한다. 따라서 메타버스라는 특성에 맞게 보안 프로세서는 물론 전략을 수립하고 메타버스화가 가속화 되는 상황에서 데이타 보호 체계를 갖추어야 한다. 즉, 메타버스 플랫폼을 많이 개발되고 있지만 결과적으로 프라이버시와 데이터 보호가 우선 과제라 할수 있다.

Acknowledgement

이 논문은 2022년 한국교통대학교 지원을 받아 수행한 연구임.

References

[1] "메타버스 정부의 기회와 도전", NIA D.gov 이슈분석, 2021.vol 4.
[2] "메타버스와 NFT, 사이버 보안 위협전망 및 분석", KISA Insight, 2022 vol.4.
[3] "가상융합경제의 확산과 보안이슈분석", KISA Insight, 2021. vol.4.
[4] "가상과 현실을 잇는 또 하나의 가능성", Tech Report, 2022.