Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 9 pp. 32-38, 2022

https://doi.org/10.5762/KAIS.2022.23.9.32
ISSN 1975-4701 / eISSN 2288-4688

메타버스 환경에서의 정보보호 및 개인정보 보호를 위한 보안모델

홍성욱[1], 박재표[2*]
[1]숭실대학교 대학원 금융기술융합학과, [2]숭실대학교 정보과학대학원

A Security Model for information Security and Personal information Security in the metaverse environment

Sung Wook Hong[1], Jae-Pyo Park[2*]
[1]Department of Financial Technology Convergence, Graduate School of Soongsil University
[2]Graduate School of Information Science, Soongsil University

요 약 코로나19로 인해 가상현실에서 이루어지는 다양한 서비스들이 메타버스 환경에서 구현중이다. 하지만, 기존의 정보보호 및 개인정보보호 보호모델에서는 메타버스 환경에서의 정보보호, 개인정보보호, 공공업무 보호 관점에서의 보호모델이 정립되어 있지 않은 문제점이 발생하였다. 이러한 문제점을 개선하기 위하여 본 논문에서는 메타버스 환경에서의 정보보호 모델, 개인정보보호 모델, 공공업무 보호를 위한 보호모델을 제시하였다. 첫째, 이용자 간 주고받는 데이터에 대한 암호화 기준을 제시하였다. 둘째, 개인정보의 처리와 미성년자 보호를 위한 점검 기준을 제시하였다. 마지막으로 공공기관에서 고려해야 하는 보안요구사항을 반영 할 수 있는 보호모델을 제시하였다. 제시된 보호모델을 통한 사례 비교를 통해 메타버스 환경에서의 정보보호, 개인정보보호, 공공업무 보호 관련 문제점의 검증을 위한 보호모델의 타당성을 검증하고자 한다. 본 논문은 향후 여러 분야의 메타버스 환경 구축 시 발생할 수 있는 정보보호, 개인정보보호, 공공업무 보호 관련 문제점을 개선할 수 있는 근거로 활용될 수 있을 것이다.

Abstract Due to COVID-19, various services in virtual reality are being implemented in a metaverse environment. However, in the existing model for information protection and personal information protection, a problem occurs in that the model was not established from the viewpoint of information protection, personal information protection, and public work protection in a metaverse environment. In order to improve these problems, this paper presents an information protection model, a personal information protection model, and a protection model for public work protection in a metaverse environment. First, encryption standards for data exchange between users are presented. Second, inspection standards for processing personal information and protecting minors are presented. Finally, a protection model that can reflect the security requirements that public institutions should consider is presented. By comparing cases through the proposed protection model, we intend to verify its validity for verification of problems related to information protection, personal information protection, and public work protection in a metaverse environment. The results could be used as a basis for improving such problems that may occur when constructing a metaverse environment in various fields.

Keywords : Metaverse, Information Security, Personal Information Security, Protection Model, Cloud

*Corresponding Author : Jae-Pyo Park(Soongsil Univ.)
email: pjerry@ssu.ac.kr
Received June 13, 2022 Revised July 13, 2022
Accepted September 2, 2022 Published September 30, 2022

1. 서론

정보통신기술의 발달과 코로나19에 따른 비대면 추세 가속화로 현실세계와 같은 사회·경제·문화 활동이 이루어지는 3차원 가상 세계인 메타버스 환경을 이용한 서비스들이 급속히 사용되고 있다. 교육, 회의, 의료, 소셜 네트워크 서비스(Social Networks Service, 이하 SNS), 게임 등의 다양한 서비스들이 메타버스 환경에서 구현되어 서비스 되고 있거나 구현을 위한 노력이 진행 중이지만 메타버스 환경에 대한 정보보호, 개인정보보호, 공공업무 보호 관련 보호모델은 정립되어 있지 않아 메타버스 환경에 부합하는 보호모델의 정립이 필요한 상황이다.

본 논문에서는 기존의 정보보호 및 개인정보보호 점검 기준을 검토하여 메타버스 환경 구축 시 정보보호, 개인정보보호, 공공업무 보호를 위한 점검을 수행할 수 있는지 살펴보고 메타버스 환경에서 적용할 수 있는 정보보호, 개인정보보호, 공공업무 보호의 문제점을 개선할 수 있는 보호모델을 제시하고자 한다.

2. 관련연구

2.1 메타버스 개요

2.1.1 메타버스 환경에서의 정보보호 및 개인정보 보호를 위한 점검 기준 필요성

메타버스 환경은 비대면·온라인 환경을 기반으로 하고 있으나 SNS, 의료, 교육, 회의, 게임 등의 서비스를 통해 현실과 같은 사회·문화적 활동은 물론, 신용카드와 암호화폐 등을 통한 결제까지 모두 수행할 수 있게 된다. 이에 따라 개인정보의 위·변조나 유·노출, 암호화, 금융정보보호, 의료정보, 생체정보, 메타버스 환경 구축을 위한 디지털트윈 보안, 메타버스 콘텐츠(폭력물, 성인물 등)에서의 미성년자 보호 등 다양한 정보보호 및 개인정보 보호의 필요성이 발생하게 되고 이를 위한 점검 기준 방안 마련이 필요하게 되었다.

2.2 해외 정보보호 및 개인정보보호 유사 점검기준 사례

2.2.1 ISO/IEC 27001

ISO/IEC 27001:2013은 조직의 정보보안 관리시스템을 구축, 구현, 유지 및 지속적으로 개선하기 위한 보안 요구사항을 지정하며, 조직의 요구에 맞게 조정된 정보보안 위험의 평가 및 처리에 대한 요구사항이 포함되며 11가지 평가 항목을 정의하고 있다[1]. ISO/IEC 27001의 주요 평가 분야는 Table 1과 같다[2].

Table 1. Main areas of evaluation of ISO/IEC 27001

No	Division	Evaluation items
1	A.5 Security Policy	2
2	A.6 Organization of Information Security	11
3	A.7 Asset management	5
4	A.8 Human Resource Security	9
5	A.9 Physical and Environmental Security	13
6	A.10 Communications & Operations Management	32
7	A.11 Access control	25
8	A.12 Information Systems Acquisition, Development & Maintenance	16
9	A.13 Information security incident management	5
10	A.14 Business continuity management	5
11	A.15 Regulatory compliance	10

2.2.2 ISO/IEC 27701

ISO/IEC 27701:2019은 조직의 개인정보 관리를 위한 ISO/IEC 27001 및 ISO/IEC 27002의 확장 형태로 개인정보관리시스템(PIMS)을 설정, 구현, 유지관리 및 지속적으로 개선하기 위한 지침을 제공하고 있다[3]. ISO/IEC 27701의 주요 평가 분야는 Table 2와 같다[4,5].

Table 2. Main areas of evaluation of ISO/IEC 27701

No	Division	Evaluation items	sub items
1	A.4 General Rules	4	
2	A.5 PIMS-specific requirements related to ISO/IEC 27001	8	25
3	A.6 PIMS-specific guidance related to ISO/IEC 2700	15	36
4	A.7 Additional ISO/IEC 27002 guidance for PII controller	5	32
5	A.8 Additional ISO/IEC 27002 guidance for PII processor	5	19

2.3 국내 정보보호 및 개인정보보호 유사 점검기준 사례

2.3.1 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)

ISMS-P 인증제도는 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합하게 운영되고 있음을 인증기관이 증명하는 제도로서 정보보호 중심의

ISMS 인증과 개인정보의 흐름과 정보보호 영역을 모두 인증하는 ISMS-P 인증 두 가지 유형이 있다. ISMS는 16개 domain의 80개 통제항목을 ISMS-P는 21개 domain의 102개 통제항목으로 구성되어 있으며 주요 평가 분야는 Table 3과 같다[6].

Table 3. ISMS, ISMS-P Certification Standard Items

Certification realm	Certification Criteria	Number of items	Whether to apply	
			ISMS	ISMS-P
Establishment and operation of management system	5 Domains	16	O	O
Protective measures requirements	12 Domains	64	O	O
Requirments for each stage of personal information processing	5 Domains	22	X	O
Sum	21 Domains	102	80	102

2.3.2 클라우드컴퓨팅서비스 보안인증제(CSAP)

CSAP 인증제도는 클라우드서비스 제공자가 제공하는 서비스에 대해 CSAP 인증기준에 적합하게 운영되고 있음을 인증기관이 증명하는 제도로서 정보시스템의 인프라를 제공하는 서비스인 IaaS, 인프라 외에 각종 응용프로그램을 제공하는 서비스인 SaaS, 클라우드 관련 서비스를 개발하는 환경(플랫폼)을 제공하는 서비스인 PaaS, 가상 PC 제공을 위한 서비스인 DaaS 등 네 가지 유형이 있다. CSAP 인증은 서비스의 종류에 따라 IaaS는 117개의 요구사항, SaaS 표준과 PaaS는 78개 요구사항, SaaS 간편은 30개 요구사항, DaaS는 110개 요구사항으로 구성되어 있으며 주요 평가 분야는 Table 4와 같다[7].

Table 4. CSAP Certification Standard Items

Certification realm	Certification Criteria (Domains)	Number of control items			
		IaaS	SaaS standard	SaaS simple	DaaS
1.Information Protection Policy and organization	2	5	5	2	5
2.Human Security	3	12	5	2	8
3.Asset Management	3	10	3	-	10
4.Service Supply Chain Management	2	4	3	-	4
5.Incident Management	3	7	7	2	7
6.Service Continuity Management	2	7	6	2	7
7.Compliance	2	4	3	1	4
8.Physical Security	2	12	-	-	12
9.Virtualization Security	2	10	6	1	7
10.Access Conrtrol	3	10	10	5	10
11.Network Security	1	6	5	2	6
12.Data protection and Encryption	3	10	8	4	10
13.System development and introduction security	4	12	10	2	12
14.Public sector additional security requirements	1	8	7	7	8
Sum	33	117	78	30	110

2.4 메타버스 환경에서의 정보보호 및 개인정보보호 문제점

2.4.1 정보보호 관점에서의 문제점

ISMS-P, CSAP 등 기존의 보호모델에서는 메타버스 환경 내에서 이용자 간 주고받는 중요정보 및 개인정보에 대한 저장 및 암호화 여부를 점검할 수 있는 기준을 제시하지 못하고 있다.

2.4.2 개인정보보호 관점에서의 문제점

국내 메타버스 서비스는 아직 태동 단계로 메타버스 환경에서 정보보안 사고가 일어난 사례를 발견되지 않고 있으나, 해외에서는 메타버스 서비스를 사칭하는 피싱 사이트에 접속하도록 하여 이용자의 개인정보를 탈취하는 사례가 발견되고 있다[8]. 이에 따라 메타버스 환경에서 수집, 이용, 저장, 전송, 파기 등 개인정보의 생명주기에 따른 보안의 이슈가 존재하게 된다. 하지만 ISMS-P 인증기준 중 개인정보보호 점검기준들은 ISMS 인증 의무대상 기관의 인증심사 시에는 점검하지 않는 문제가 발생하고 있으며, CSAP 인증기준 중 개인정보보호 점검기준은 공공 클라우드 환경을 이용하는 공공 클라우드 서비스 제공자들을 대상으로만 적용되기 때문에 일반 기업들은 ISMS-P, CSAP 인증을 통해 개인정보보호 점검기준에 따라 개인정보의 생명주기에 따른 개인정보보호 여부를 점검할 수 있는 기준을 제시하지 못하는 문제가 발생하고 있다.

2.4.3 공공업무 보호 관점에서의 문제점

공공부문에서 메타버스 환경을 구축하는 경우 준수해야 할 공공기관 보안요구사항을 준수하여 메타버스 서비스를 구현하는지 여부를 고려할 필요가 있으나 ISMS-P 인증기준에는 공공업무 보호 관점의 점검기준이 존재하

지 않으며, CSAP 인증기준은 공공 클라우드 서비스를 제공하는 기관에 대해서만 공공기관 보안요구사항의 준수 여부를 점검하는 문제가 있다.

2.5 메타버스 환경에 대한 정보보호 및 개인정보보호 점검기준의 필요성

기존에 제시되고 있는 정보보호 및 개인정보보호 보호모델에서는 새로운 형태의 서비스가 제공되는 메타버스 환경에서의 정보보호 및 개인정보보호 관련 보호모델이 정립되어 있지 않은 문제점이 발생하고 있다. 메타버스 환경을 이용한 서비스에서 발생할 수 있는 암호화 이슈 등 정보보호에 대한 보호모델이 기존 보호모델에 추가될 필요성이 있다. 또한, 메타버스 콘텐츠에서의 미성년자 보호 이슈(폭력물, 음란물 등), 메타버스 서비스 이용자의 개인정보 유·노출, 등 개인정보의 처리 과정에서 발생할 수 있는 개인정보의 생명주기 관련 이슈 이슈 등 개인정보보호에 대한 보호모델에 추가되어야 할 것이다. 마지막으로 공공부문 업무 수행에 따른 법적 요구사항 준수와 공공기관 보안요구사항에 대한 보호모델도 고려되어야 할 것이다.

3. 메타버스 환경에서의 정보보호 및 개인정보보호 점검기준 수립방안

3.1 메타버스 환경에서의 정보보호 및 개인정보보호 점검기준의 문제점 해결방안

3.1.1 정보보호 관점에서의 보호모델

기존 정보보호 및 개인정보보호 점검기준에서는 메타버스 환경에서 이용자 간 주고받는 중요정보 및 개인정보의 저장 및 암호화에 대한 점검기준이 포함되어 있지 않는 문제가 있다. 이에 대한 문제해결을 위해 메타버스 환경에서 이용자 간 서비스 이용 중 생성되는 중요정보 및 개인정보의 저장 및 암호화 기준이 포함되어야 한다. 메타버스 환경에서의 정보보호 점검기준의 예시는 Table 5와 같다.

Table 5. Information Security Protection Model

Category	Requirement
Cryptographic Control	Encryption of important and personal information circulated between users
	Encryption when storing important and personal information circulated between users

Table 5에서는 이용자 간에 유통되는 중요정보 및 개인정보에 대한 전송구간 암호화와 저장 시 암호화에 대한 점검기준을 제시하고 있다.

3.1.2 개인정보보호 관점에서의 보호모델

ISMS-P 인증에서는 ISMS 인증만을 받을 경우 개인정보보호 점검 기준을 적용하지 않고 있으며, CSAP 인증에서는 민간 클라우드 서비스 제공자에게는 개인정보보호 점검 기준을 적용하지 않는 문제가 있다. 이에 대한 문제해결을 위해 메타버스 환경에서 개인정보의 생명주기에 따른 동의 및 처리내역을 확인하고 미성년자를 대상으로 폭력물이나 음란물을 서비스 하고 있는지를 점검하는 기준이 포함되어야 한다. 메타버스 환경에서의 개인정보보호 점검기준의 예시는 Table 6과 같다.

Table 6. Personal Information Security Protection Model

Category	Requirement
Protection measures when collecting personal information	Consent to collection and use of personal information during service use
	Resident registration number processing
	Sensitive information processing
	Consent to collection of personal information from children under the age of 14
Protection measures when providing personal information	Consent to provide personal information to third parties while using the service
Protection of minors	Measures to protect minors against violent and obscene materials

Table 6에서는 개인정보 수집 시 보호조치로 개인정보 수집 및 이용 동의, 주민등록번호 처리, 민감정보의 처리, 만14세 미만 아동의 개인정보 수집 동의 점검기준을 제시하고, 개인정보 제공 시 보호조치로 개인정보 제3자 제공 동의 점검기준을 제시하며, 미성년자의 보호를 위한 보호조치로 폭력물, 음란물 등으로부터 미성년자를 보호하기 위한 점검기준을 제시하고 있다.

3.1.3 공공업무 보호 관점에서의 보호모델

공공 메타버스 환경에서 요구하는 공공기관의 보안요구사항에 대한 점검기준이 별도로 존재하지 않는 문제가 있다. 이에 대한 문제해결을 위해 공공부문에서 메타버스 환경을 구축하는 경우 준수해야 할 공공기관 보안요구사항을 계약서에 반영하고 CC인증을 취득한 솔루션을

이용하여 메타버스 서비스를 구현하는지 여부를 고려할 필요가 있다. 또한, 클라우드 환경에서 공공부문 메타버스 서비스를 구축하는 경우 CSAP 인증 취득 여부를 확인할 필요성이 존재한다. 메타버스 환경에서 공공업무 보호 점검기준의 예시는 Table 7과 같다.

Table 7. Public Information Protection Model

Category	Requirement
Security service level agreement	Define the security requirements of public institutions and reflect them in the contract
Safety of introduced computing equipment	Whether to use CC certified products
Availability of public cloud services	Whether to acquire CSAP when using public cloud services
physical location of data	The physical location of data is limited to domestic

Table 7에서는 공공업무 보호를 위해 보안 서비스 수준 계약의 보호조치로 공공기관의 보안요구사항 정의 및 계약서 반영 점검기준을 제시하였고, 도입된 전산장비의 안전성을 위한 보호조치로 CC인증 제품 사용 여부 점검기준을 제시하였으며, 공공 클라우드 서비스의 가용성에 대한 보호조치로 공공 클라우드 서비스 이용 시 CSAP 취득 여부를 확인하는 점검기준을 제시하였고 데이터의 물리적 위치에 대한 보호조치로 데이터의 물리적 위치가 국내로 제한되는지 여부를 확인하는 점검기준을 제시하고 있다.

4. 사례연구 및 비교분석

‘2.관련연구’에서 국내/외 정보보호 및 개인정보보호 점검기준을 분석하여 메타버스 환경을 고려한 메타버스 점검기준이 필요하다고 판단하였으며 이에 따라 메타버스 환경에서 점검 시 추가해야 할 정보보호 및 개인정보보호 보호모델을 제시하였다. 본 장에서는 메타버스를 이용하는 서비스를 기존의 점검기준과 메타버스 점검기준에 따라 점검하였을 경우 기존 점검기준에 정립되어 있지 않은 보호모델을 메타버스 점검기준을 통해 개선할 수 있다는 것을 확인하였다.

4.1 공공 메타버스 서비스에서의 정보보호 및 개인정보보호 점검기준 개선 사례

4.1.1 정보보호 관점에서의 보호모델

ISMS-P, CSAP 등 기존의 점검기준에서는 전송 및 저장 시 암호화 요건만을 점검하도록 하고 서비스 내에서 이용자 간 주고받는 중요정보 및 개인정보의 저장 및 암호화를 고려하지 않고 있으나, 메타버스 점검기준에서는 이용자 간 서비스 이용 중 생성되는 중요정보 및 개인정보에 대한 저장 및 암호화 여부를 점검하는 기준을 마련하고 있다. 기존 점검기준에서 요구하는 암호화 점검기준과 메타버스 점검기준의 차이는 Table 8과 같다[6,7].

Table 8. Comparison of ISMS-P, CSAP, and Metaverse certification standards from the point of view of information protection

Required certification criteria	ISMS-P	CSAP	Metaverse Certification Criteria
Encryption of important and personal information circulated between users	X	X	O
Encryption when storing important and personal information circulated between users	X	X	O

메타버스 서비스에서 채용을 위한 이력서 등 개인정보가 포함된 문서의 전달, 회의를 위한 화면공유 중 회사의 중요정보의 노출, 될 경우 메타버스 인증기준을 통해 이용자 간 처리되는 중요정보 및 개인정보의 저장 및 암호화 처리 여부를 점검하는 것이 가능하게 된다.

4.1.2 개인정보보호 관점에서의 보호모델

ISMS-P 인증기준에서는 ISMS-P 인증심사 시에만 개인정보의 생명주기에 따른 개인정보보호 점검을 수행하고 CSAP 인증기준에서는 공공기관에 서비스하는 IaaS, SaaS 서비스 중 개인정보가 포함된 경우에만 개인정보보호 점검을 수행하고 있으나 메타버스 점검기준에서는 메타버스 서비스 내에서 발생하는 개인정보의 생명주기에 따른 동의 및 처리내역을 점검하고 미성년자를 보호할 수 있는 점검기준을 마련하고 있다. 기존 점검기준에서 요구하는 개인정보보호 점검기준과 메타버스 점검기준의 차이는 Table 9와 같다[6,7].

민간기관이 ISMS 인증기준에 따라 메타버스 서비스에 대한 인증 시 개인정보의 생명주기에 따른 개인정보보호 인증기준을 적용하지 않는 것과 달리 메타버스 인증기준에서는 메타버스 서비스 이용 중 고유식별정보,

민감정보 등 개인정보와 기기정보(IP, MAC, 카메라/마이크 통제 권한 등)에 대한 개인정보 생명주기에 따라 수집·이용·제공·저장·파기 시 개인정보를 법적 요구사항에 따라 처리하고 있는지 여부를 점검하도록 하고 있으며, 메타버스 서비스에서 제공하는 서비스의 내용이 폭력물이나 음란물일 경우 미성년자에 대한 보호대책이 있는지 여부를 점검하는 기준을 마련하고 있다.

Table 9. Comparison of ISMS-P, CSAP and Metaverse authentication standards from the perspective of personal information protection

Required certification criteria	ISMS-P	CSAP	Metaverse Certification Criteria
Consent to use of personal information	△	△	O
Resident registration number processing	△	△	O
Sensitive information processing	△	△	O
Consent to collection of personal information from children under the age of 14	△	X	O
Protection of minors	X	X	O

4.1.3 공공업무 보호 관점에서의 보호모델

ISMS-P 인증기준에서는 공공기관의 보안요구사항에 대한 점검 기준을 별도로 제공하지 않고 있으며, CSAP 인증기준에서는 공공기관의 보안요구사항에 대한 점검 기준을 제시하고 있다, 하지만 CSAP 인증은 공공 클라우드 서비스를 이용하는 서비스 제공자만을 대상으로 인증을 수행하고 있어 공공 메타버스 서비스 제공자가 공공 클라우드 서비스를 이용하지 않는 경우 공공기관의 보안요구사항에 대한 점검을 수행할 수 없다. 메타버스 점검기준에서는 공공메타버스 서비스 이용 중 생성되는 중요정보 및 개인정보에 대한 공공기관 보안요구사항에 대한 점검기준으로 CC인증 받은 제품 사용 여부, 공공 클라우드 서비스의 경우 CSAP 인증 획득 여부와 중요정보와 개인정보가 국외이전 되는 지 여부를 점검하는 기준을 마련하고 있다. ISMS-P, CSAP 점검기준에서 요구하는 공공기관 보안요구사항 점검기준과 메타버스 점검기준의 차이는 Table 10과 같다[6,7].

민간기관이 공공 메타버스 서비스를 제공하고자 하는 경우 ISMS-P 인증기준에서는 공공 메타버스 서비스를 구축하기 위해 사용하는 정보시스템의 안전성 여부나 데이터의 국외이전 여부를 점검하는 점검 기준을 별도로 제공하고 있지 않으며, CSAP 인증기준에서는 공공 클라우드 서비스를 이용하는 경우에만 점검 기준을 제공하고 있는 것과 달리 메타버스 인증기준에서는 공공 메타버스 서비스를 구축하기 위해 사용하는 정보시스템이 CC인증을 취득한 솔루션을 사용하고 있는지 여부를 확인하고, 클라우드 서비스를 이용하여 공공 메타버스 서비스를 제공하는 경우 CSAP 인증을 받은 공공 클라우드 환경을 통해 서비스를 제공하고 있는지 여부를 확인하는 점검기준을 마련하고 있다. 또한, 공공 메타버스 서비스 이용 중 발생하는 중요정보 및 개인정보가 국외로 이전되는지 여부를 확인하여 공공 데이터의 국외이전 여부를 점검하는 기준을 마련하고 있다.

Table 10. Comparison of ISMS-P, CSAP and Metaverse authentication standards from the perspective of public security requirements

Required certification criteria	ISMS-P	CSAP	Metaverse Certification Criteria
Definition of security requirements for public institutions	X	△	O
Whether to use CC certified products	X	△	O
CSAP certification or not	X	△	O
The physical location of data is limited to domestic	X	△	O

5. 결론

기존의 보호모델에서는 메타버스 환경에서의 정보보호, 개인정보보호, 공공업무 보호 관련 보호모델이 정립되지 않고 있어 메타버스 서비스에 대한 정보보호, 개인정보보호, 공공업무 보호 관련 점검을 수행할 수 없는 문제가 있다. 이러한 문제점에 대한 해결방안으로 본 논문에서는 세 가지 해결 방안을 제시하였다. 첫째, 메타버스 환경에서 이용자 간 주고받는 중요정보 및 개인정보에 대한 저장 및 암호화 기준을 제시하였다. 둘째, 메타버스 환경에서 개인정보의 생명주기에 따른 동의 및 처리내역을 확인하고 미성년자를 대상으로 폭력물이나 음란물을 서비스 하고 있는지를 점검하는 기준이 포함하였다. 마지막으로 공공부문 메타버스 서비스에서 공공기관 보안요구사항을 반영할 수 있는 점검기준을 제시하는 등 세 가지 개선방안을 제시하였다.

본 논문에서 제시한 메타버스 환경에서의 정보보호,

개인정보보호, 공공업무 보호 관련 점검기준은 메타버스 서비스를 제공하는 기관에 대한 보호모델을 제시할 수 있을 것으로 기대한다.

References

[1] ISO Association. Introducing ISO27001[Internet]. ISO.org, c2022, [cited March 19, 2022], https://www.iso.org/isoiec-27001-information-security.html (Accessed March 19, 2022)

[2] NAVER. Naver Encyclopedia of Knowledge[Internet]. NAVER, c2022[cited March 19, 2022], https://terms.naver.com/entry.naver?docId=3432094&cid=58437&categoryId=58437 (Accessed March 19, 2022)

[3] ISO Association. Introducing ISO27701[Internet]. ISO.org, c2022, [cited March 19, 2022], https://www.iso.org/standard/71670.html (Accessed March 19, 2022)

[4] J. Y. KIM, *A Study on Improvement of ISO/IEC 27701 Based ISMS-P Certification Standar*, Master's thesis, Department of Information Security Graduate School of Information Science Soongsil Universi, pp.83-115, 2020.

[5] Wikipedia. ISO/IEC 27701[Internet]. Wikipedia, c2021 [cited April 26, 2021], https://en.wikipedia.org/wiki/ISO/IEC_27701 (Accessed March 19, 2022)

[6] KISA, ISMS-P Certification System Guide, Technical Report, KISA, Korea, pp.13, pp.18.

[7] KISA, ISMS-P Cloud Security Certification Guide, Technical Report, KISA, Korea, pp.6-7, pp.13, pp.17-18.

[8] Financial metaverse service 'security blind spot' [Internet], Electronic newspaper, c2021 [cited 2021 Nov. 19], https://www.etnews.com/20211119000147 (accessed Nov. 19, 2021)

홍 성 욱(Sung Wook Hong) [정회원]

- 2018년 2월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2019년 3월 ~ 현재 : 숭실대학교 대학원 금융기술융합학과 박사과정

〈관심분야〉
정보보안, 개인정보보호, ISMS-P, 클라우드, 금융IT

박 재 표(Jae-Pyo Park) [종신회원]

- 1998년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

〈관심분야〉
보안평가 인증, 네트워크 보안, 디지털포렌식, FinTech