NFT 서비스 제공자 보안 수준 점검 항목 중요도 분석을 통한 보안 위협 대응

[1*] 임동성

Response to Security Threats through Importance Analysis of NFT Service Provider Security Level Check Items

[1*]Dong Sung Im

요 약

블록체인과 함께 NFT(Non-Fungible Token) 수요가 확대됨에 따라 사이버상의 보안 위협도 증가하고 있다. 따라서 본 연구는 NFT 보안 강화를 목적으로 NFT 특징, 보안 위협, 컴플라이언스 등 NFT 보안 관련 현황 분석을 통해서 보안 점검 항목을 도출하였고 이를 바탕으로 AHP 모형에 적용, 상대적 중요도를 확인하였다. 실증 분석 결과 관리체계 수립 및 운영, 암호화, 위험관리 등으로 중요도 우선 순위가 나타났다. 본 연구의 의의는 NFT 관련 보안 수준 점검 항목을 도출하고 모형을 실증함으로써 NFT 보안 사고 감소 및 관련 회사들의 보안 관리 수준을 보다 더 향상시킬 수 있다. 그리고 NFT 점검 항목의 상대적인 중요도를 고려하여 보안 점검을 수행한다면 조기에 보안 수준을 식별할 수 있을 것이다.

Abstract

Demand for NFT is expanding along with Blockchain. And cyber security threats are also increasing. Therefore, this study derives security level inspection items by analyzing status related to NFT security such as NFT features, security threats, and compliance for the purpose of strengthening NFT security. Based on this, the relative importance was confirmed by applying it to the AHP model. As a result of the empirical analysis, the priority order of importance was found in the order of Security management system establishment and operation, encryption, and risk management, etc. The significance of this study is to reduce NFT security incidents and improve the NFT security management level of related companies by deriving NFT-related security level check items and demonstrating the research model. And If you perform considering relative importance of the NFT check items, the security level can be identified early.

Keywords: *NFT, Security, Information Security Management System, Block Chain, AHP*

[1*]*오산대학교 컴퓨터정보계열 컴퓨터보안전공 교수(seaids@osan.ac.kr)*

Received: Sept. 28, 2023, Revised: Oct. 30, 2023, Accepted: Oct. 30, 2023

I. 서론

블록체인 기술을 활용하는 가상화폐와 더불어 NFT 는 오프라인상의 대면 거래를 DX(Digital Transformation)로 가속화시키고 있다. 블록체인 서비스 시장조사 분석업체인 DappRadar 조사에 따르면, NFT 시장 규모는 2020 년 9 천 4 백만 달러에 불과했던 NFT 거래금액이 2021 년 249 억 달러까지 치솟으면서 약 260 배 폭발적으로 성장했다[1]. 최근 미국 실리콘밸리은행, FTX 파산 등의 금융시장 악화로 2022 년 NFT 성장이 잠시 주춤하고 있었다[2]. 그러나 현재 NFT 잠재성에 기업들의 투자와 인프라 구축이 재개되고 있고, 마켓앤마켓((MarketsandMarkets) 기관에서 발표한 NFT 시장 전망 보고서를 보면 2027 년까지 연간 35%의 성장률을 기록할 것으로 예상하고 있어 향후 NFT 시장의 긍정적 변화가 기대된다[3]. 이처럼 기업 재투자와 시장 규모 확대로, 디지털 자산의 권리 증명서인 NFT 는 스마트폰처럼 게임, 수집품, 미술품, 엔터테인먼트 등 여러 분야의 생태계를 빠르게 변혁시킬 것이다.

그러나 NFT 의 시장 규모 확대와 다양한 분야로의 진출은 사이버 공격이 가능한 접점 확대로 이어져, 결국 NFT 의 보안 위협도 증가하고 있다. 가장 많이 알려진 NFT 보안 위협 사례 경우로 2022 년 4 월 발생한 지루한 원숭이 요트 클럽(BAYC) 디스코드에서 발생한 해킹이며, 총 11 개의 BAYC NFT 가 도난당해 피해 규모는 대략 166 만 달러였다[4]. 해당 사건은 프로젝트가 사용하는 디스코드 서버를 해킹, 사용자들에게 낚시성 해킹 주소를 클릭하도록 유도하여 피해자의 지갑내 NFT 와 가상화폐를 탈취한 불법 공격이었다. 그리고 같은 해 2 월 세계 1 위 NFT 플랫폼 사업자인 오픈씨(OpenSea)에 해커가 피싱 이메일 공격을 수행하여, 20 억원 상당의 NFT 탈취 등 다양한 보안 사고 사례들이 지속적으로 보고되고 있다[5]. 따라서 디지털 자산의 성격을 띠고 있는 NFT 의 경우, 이용자의 자산에 직접적인 피해를 줄 수 있기 때문에 체계적 보안 대응체계가 필요할 것으로 판단된다. 그리고 가상자산 이용자보호법은 2023 년 7 월 공포, 2024 년 7 월 시행될 예정인데 해당 법률에서는 이용자 보호와 시세조종, 미공개 거래 행위 등 불공정 거래 행위 방지에 중점을 두고 있다. 이처럼 컴플라이언스 측면에서도 사이버 공격에 대해 안전 장치를 요구하고 있다. 그러나 기존 연구들은 기술적 보안 트랜드 중심의 연구로, NFT 디지털 자산을 위협하는 해킹 공격 대응의 취약성이 나타나고 있다. 따라서 물리적 · 기술적 · 관리적 보안 점검 항목과 컴플라이언스를 연계한 통합적 연구가 필요하다. 그리고 조직은 시간, 비용 등의 자원이 유한하기 때문에 보안 점검 항목의 중요도를 고려하여 우선 점검한다면, 비용과 시간을 절감할 수 있으며 또한 보안 수준을 빠르게 식별할 수도 있다.

따라서 본 연구는 NFT 보안 위협, 국내외 법률, 보안 컴플라이언스 등을 분석하여 NFT 관련 통합적 보안 수준 점검 항목을 도출하였다. 또한 점검 항목간 상대적 중요도를 실증하였는데 본 연구 결과를 기반으로 자원과 시간이 부족한 조직의 경우, 상대적 상위 랭킹 항목을 선별적으로 이용한다면, 보안 수준을 조기에 식별할 수 있을 것이다.

본 논문은 2 장에서 관련 이론인 NFT 특징, 보안 위협, 관련 법률, 국내 컴플라이언스인 보안 관리 체계, 선행 연구 등에 대하여 기술한다. 3 장에서는 NFT 서비스 제공자 보안 수준 점검 항목 도출과 모형 및 연구 방법을 제시한다. 그리고 4 장에서는 AHP 분석 기법을 이용, 상대적인 중요도를 실증 분석하고 마지막 장에서 결론을 제시한다.

II. 관련 이론 및 연구

2.1 NFT

NFT(Non-Fungible Token)관련 정의를 살펴보면 위키 백과사전에서는 '블록체인에 저장된 데이터 단위로, 고유하면서 상호 교환할 수 없는 토큰'이라고 정의하고 있으며, 네이버지식백과에서는 '대체 불가능한 토큰'이라 정의하고 있다. 즉 신뢰할 수 있는 블록체인 기술을 활용하여 디지털 자산의 소유주를 증명하는 가상의 토큰으로 디지털 콘텐츠에 대한 권리 증명서라고 할 수 있다[6].

그리고 NFT 는 블럭체인, 스마트 컨트랙트, 메타데이터, 미디어 콘텐츠로 나누어 설명할 수 있다. 블록체인 부문은 NFT 서비스 사업자의 외부에 존재하고, 블록간 해쉬 알고리즘 연계

기술을 이용하여 토큰의 위·변조가 불가능하게 하는 신뢰성 있는 트랜잭션을 제공한다. 스마트 컨트랙트는 ERC721 또는 ERC1155 등의 표준을 따름으로써 대체 불가능한 토큰을 구현하고 거래간 상호운용성을 확보하여 손쉽은 거래가 가능하다. Solidity 언어로 소유권 확인, 양도, 로열티 처리 등 실제 거래 계약 조항을 작성한다. 또한 콘텐츠의 정보가 포함된 메타데이터 주소를 포함한다. 그리고 스마트 컨트랙트로 자율성, 투명성, 비용 절감, 접근성을 확보할 수 있다. 기존 거래에서는 보증 기관을 통한 복잡한 거래 절차가 필요했으나 스마트 컨트랙트는 자율적 기반하에 중립적이며 자동화가 가능하다. 투명성은 블록체인 특성상 스마트 컨트랙트 내용을 누구나 확인할 수 있으며, 성사된 계약은 모든 노드로 복제된다. 비용 절감은 중개 비용이 제거되어 비용 효과적이며, 접근성은 언제 어디서나 이용할 수 있다는 것이다. 메타데이터 부문은 우리가 알고 있는 속성 정보처럼 정보를 효율적으로 찾고, 이용하기 위해 콘텐츠의 정보와 콘텐츠가 포함된 주소를 저장하고 있다. 미디어 콘텐츠는 NFT 의 실제 디지털 자산이 저장되는 공간으로 용량이 상대적으로 클 수 있다. 그리고 높은 수수료와 제한된 블록 데이터 크기 사용 등의 블록체인 특성으로, 용량이 큰 미디어 콘텐츠와 메타데이터는 일반적으로 블록체인 외부 별도 서버에 저장하여 비용과 효율성을 확보한다.

2.2 NFT 보안 위협

NFT 보안 위협을 서비스 플랫폼 측면과 이용자 측면으로 구분하여 확인할 수 있다. NFT 의 서비스 플랫폼은 NFT 서비스 제공자의 내부 서비스 플랫폼과 블록체인 연계의 외부 플랫폼으로 구성되어 있어 먼저 두 부분 중심으로 보안 위협을 살펴보고자 한다.

내부 서비스 플랫폼은 원본 디지털 자산을 저장하는 시스템, 거래를 관리하는 마켓 플레이스 웹 포탈 등으로 구성되는데 저장소의 경우 시스템 취약점을 악용하여 관리자 계정 탈취, 악성 코드 또는 랜섬웨어 공격을 할 경우 이용자의 지갑에 있는 NFT 와 가상화폐를 탈취할 수 있다. 그리고 마켓 플레이스 웹 사이트의 보안 취약점을 악용하여 구매 또는 판매 가격을 조작, NFT 의 불법적인 재판매 가능성의 위협이 발생할 수 있다. 블록체인 연계의 외부 플랫폼에서는 ERC-721 기반 소스 코드에서의 취약점들이 노출되고 있다. 최근에 NFT 를 추적하고 전송하는 기능을 담당하는 ‘setApprovalForAll’의 소스 코드 취약점을 악용하여, NFT 를 탈취하는 보안 사고가 발생했다[7]. 이러한 중요 소스 코드가 유출될 경우, 해커는 NFT 마켓 플레이스의 지갑 내 NFT 와 가상 자산 등을 쉽게 탈취할 수 있다. 향후 NFT 발행·관리 기술의 발전 및 타 ICT 와의 연계로 소스 코드의 보안 위협이 증가하여, 버그 공격 및 Zeroday attack 등 다양한 사이버 공격이 예상된다. 스마트 컨트랙트 운영 및 동작관련 외부 정보의 요청·검증을 수행하는 블록체인 오라클은 서비스 사업자가 시스템 혹은 API 로 구성·운영하여 관리자 계정에 대한 위협이 존재한다. 해커가 관리자 계정을 해킹하거나, 인증 및 권한관리가 취약하여 내부 관리자가 본인의 권한을 악용하는 경우 정보의 위·변조, 허위 정보 업로드 등 불법 행위가 가능하여 거래의 안전성 및 신뢰성을 훼손할 수 있다. 그리고 오라클은 블록체인 내부가 아닌 외부 인프라 시스템, API 등으로 구성하여 기존 ICT 보안 취약점을 내재하고 있다[8].

NFT 서비스 이용자 측면에서는 해커가 문자, 이메일, Discord 등을 매개로 하는 피싱, 스미싱 공격 등으로 이용자의 NFT 와 가상자산을 탈취할 수 있다. 예를 들어 위조 사이트 링크를 이용자에게 전송하고 해당 사이트에서 복구 문자를 입력하도록 유도하여 전자 지갑을 획득한다. 또한 해커가 허위 플랫폼 또는 해커 지갑으로 연결, 정상적인 거래가 발생한 것처럼 위장하여 메시지를 전송한 후 해커는 이용자에게 개인키 서명을 유도하여 이용자의 자산을 불법 탈취할 수 있다.

2.3 국내외 법률

NFT 는 최신 기술의 특성과 상업적·법적·규제관점에서 다양한 고려사항을 내재하고 있어, 아직까지 많은 나라에서 NFT 의 법적인 해석이 명확하게 이루어지지 않고 있으며 그에 대한 검토가 계속적으로 이루어지고 있다. 한국의 경우도 NFT 가 24 년 7 월 19 일 시행 예정인 가상자산 이용자 보호 등에 관한 법률(가상자산 이용자보호법)상의 가상자산에 해당되는지가 관건이다. 동법은 가상자산을 ‘경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표’로 정의하고, 다만 ‘화폐·재화·용역 등으로 교환될 수 없는 전자적 증표

또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것'등 일부 제외되는 범위를 열거하고 있는데, NFT 가 이런 제외 범위에 해당되는지 여부에 대해 결정되지 않고 있다.

NFT 는 기본적으로 교환 가능하지 않고 유일한 수집물로 볼 수 있으나 스마트계약에 의하여 특정한 조건이 부가될 수 있고 NFT 기반 담보대출, 자산관리 · 평가, 펀드 조성 등 DeFi 와 연결된 다양한 활용 사례가 발생하고 있어, NFT 별로 가상자산으로 평가될 가능성이 있다. 따라서 NFT 가 가상 자산으로 결정되지 않았고 사안별 가상 자산의 가능성이 존재하여 가상자산에 관한 법률을 분석하려고 한다.

가상자산관련 법률은 21 년 특정금융법으로 최초 시행되었으나 테라-루나 사태와 미국의 FTX 거래소 파산 등 시장 전반과 이용자 보호에 커다란 영향을 미치는 사건들이 다수 발생하여 법 체계 마련이 시급하였다. 이에 국회에서는 가상자산 이용자 보호의 시급성을 고려, 기존에 국회위원들이 발의한 19 건을 가상자산 보호자이용법으로 통합하여 입법화하였다. 해당 법안은 디지털자산기본법 제정을 위한 2 단계 입법 중 1 단계로 이용자 보호를 위해 가상자산을 제도권안으로 들어오게 했다는 데 의의가 있으며, 24 년 7 월 시행 예정이다. 법안을 좀더 살펴보면 이용자 보호와 시세조종, 미공개 거래 행위 등 불공정 거래 행위 방지에 중점을 두고 있다. 제 7 조의 3 항에 가상자산 사업자는 일정 비율 이상의 가상자산을 인터넷과 분리하여 안전하게 보관하도록 하고 있으며, 4 항에는 이용자의 가상자산을 보안기준을 충족하는 기관에 위탁하여 보관할 수 있도록 하고 있다. 그리고 제 8 조에 '가상자산사업자는 해킹 · 전산장애 등 대통령령으로 정하는 사고에 따른 책임을 이행하기 위하여 금융위원회가 정하여 고시하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.'로 하여 보안 침해사고시 이용자를 보호하도록 하고 있다. 또한 제 9 조에 가상자산 거래기록을 거래관계 종료 후 15 년간 보존할 의무를 신설하여 이용자 자산 보호를 강화하였다. 향후 디지털자산기본법 2 단계 혹은 시행령 등에서 좀더 구체화된 보안 관련 내용들은 추가될 것으로 보인다.

해외의 경우 미국에서는 2022 년 6 월 7 일 책임 있는 금융 혁신법안(Responsible Financial Innovation Act) 발의를 통해 디지털자산에 대한 포괄적인 규제 체제의 틀을 마련하였다[9]. 그리고 유럽연합에서도 6 월 30 일 디지털자산을 그 특성에 따라 유형별로 분류하고 각 유형별 규제를 정한 암호자산규제법안(MiCA)이 마련, 2023 년 6 월 9 일 관보에 게재되어 향후 시행 예정인데 이처럼 주요 국가들은 디지털자산 규제 체계를 본격적으로 구축하고 있는 실정이다.

2.4 Compliance

국내에서는 NFT 보호를 위한 특정화된 관리체계는 없으나, 가상자산관련 정보보호 관리체계를 운영 중에 있다. 해당 관리체계는 ISMS-P 로 기존 관리 체계에 멀티시그, 월렛 등의 가상 자산의 특성을 반영하여 보안 위협에 대응하고 있다. NFT 도 가상 자산과의 연관성 및 보안 위협 대응 측면에서 ISMS-P 를 연구하는 것이 필요하다. ISMS-P 는 기업 · 기관이 각종 위협으로부터 정보자산과 개인정보를 안전하게 보호하기 위해 수행하는 종합적인 정보보호 관리 프레임워크로서 관리체계 수립 및 운영, 보호대책 요구 사항, 개인정보 처리 단계별 요구 사항으로 구분할 수 있다. 특히 가상 자산과 NFT 에 적용할 수 있는 ISMS-P 는 개인정보보호 부문보다는 정보보호 부문에 관리체계 수립 및 운영, 보호대책 요구 사항에 중점을 두고 있다.

좀더 살펴보면 관리체계 수립 및 운영 영역은 정보보호 관리체계를 지속적으로 기획하고 운영하도록 관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선으로 구성되어 있다. 보호대책 요구 사항 영역에서는 관리체계 수립 및 운영 과정에서 수행한 위험평가 결과와 조직의 서비스 및 정보시스템 특성 등을 반영하여 체계적으로 보호 대책을 수립 · 이행하도록 정책, 조직, 교육, 인증 및 권한관리, 개발, 접근 통제, 보안관리, 재해 복구 등 64 개의 점검 항목으로 구성되어 있다. 그리고 가상자산관련 인증 및 월렛 개인키 보안 강화를 위해 멀티시그 등의 MFA 추가 인증 수단 적용 여부, 월렛에서 사용되는 키와 패스프레이즈는 물리적으로 안전한 장소에 소산하여 보관하고 있는지를 점검하고 있다. 또한 디지털 자산과 개인키 등을 보관하고 있는 월렛 인프라에 대한 접근 통제 및 로그 모니터링, 월렛 룸에 대한 CCTV 및 출입통제장치 등의 물리적 접근 통제 수행 여부를 판단하고, 가상 자산 인프라의 중요성을 고려하여 업무망과 인터넷망 안전 분리 여부를 중요하게 다룬다.

2.5 계층 분석 기법

1970 년대 초 Thomas L Satty 교수가 개발한 AHP(Analytic Hierarchy Process) 기법은 효과적인 의사결정을 하기 위해 의사결정 모든 과정을 단순화하고 최종적인 의사결정을 할 수 있게 하는 모형이다[10]. 해당 기법은 쌍대비교를 이용하여, 평가자가 일관성 있게 판단하도록 도와주는 것을 특징으로 하고 있으며, 상대적 중요도를 계량화 · 판별하여 많이 이용하고 있다. AHP 는 최상위 계층에 평가할 목표를 설정하고 그 하위에는 평가 목표에 영향을 주는 항목들을 구성한다. 그리고 해당 항목들은 여러 단계로 나누고, 다시 하부 세부 평가 항목으로 계층화할 수 있다. 좀더 살펴보면 다수의 속성들을 계층 배열하고 그 상태에서 설문 결과 데이터를 기입, 쌍대비교를 수행한다. 쌍대비교 값에서 각각의 계층별 의사 결정관련 상대적 중요도를 추정하고, 유효성 여부 판단을 위해 일관성 비율(Consistency Ratio)을 구한다. 일관성 비율이 10% 이내로 나오는 경우, 판단에 있어 일관성이 있는 것으로 간주한다.

2.6 관련 연구

Song et al.연구[7]는스마트 컨트랙트, 메타데이터, 미디어 데이터로 NFT 구성을 분류하고 동작 원리를 기술하였다. 그리고 ERC-721 기반 소스 코드 취약점 공격, 블록체인 네트워크와 외부 데이터를 연결하는 블록체인 오라클 공격, 해커가 문자 및 이메일 등을 매개로 하는 사회공학적 공격 기법으로 이용자의 NFT 와 가상자산을 탈취 등의 NFT 주요 공격 기법들을 설명하였다. 또한 발급된 NFT 가 가리키는 미디어 데이터 주소가 공격자에 의해 변조될 수 있는 위협을 제시하고 이에 해시 알고리즘을 사용하여 파일 위변조를 탐지하는 방안을 제언하였다. Jung et al.연구[11]는 NFT 마켓플레이스 정의 및 현황을 살펴보았고, 거래에 직접적인 영향을 미치는 위협 요소인 인적 자산, 플랫폼 서비스, 정보자산을 식별하였다. 그리고 지갑 개인키 정보 탈취를 위한 사용자 사칭, 마켓플레이스 사이트 CSRF 를 통한 권한 상승, 취약한 접근 통제로 인한 NFT 원본 데이터 저장소 정보 유출 등의 보안 위협 요인을 도출하였다. Lee et al.연구[12]는 NFT 시장에 대한 이용자 수요가 증가함에 따라 국내 NFT 마켓플레이스의 역할과 책임의 중요성에 초점을 맞추어, NFT 시장의 보안 이슈 해결 목적으로 정보보호 거버넌스 요구사항을 도출하였는데 특히 NFT 마켓플레이스 담당자의 역할과 책임, 위험 기반 관리 등을 제언하였다.

그러나 대부분의 관련 연구에서는 NFT 특징 및 보안 위협 동향에만 치우져 있고, NFT 보안 수준 점검 항목 및 상대적 우선 순위를 분석하려는 연구가 부족한 것으로 판단된다.

III. 연구모형

3.1 NFT 점검 항목 도출

앞에서 연구했던 이론적 고찰과 함께, 국내외 법률과 Compliance 등에서 NFT 보안과 관련 있는 점검 항목들을 분석하여 아래 ‘그림 1’과 같이 도출한다.

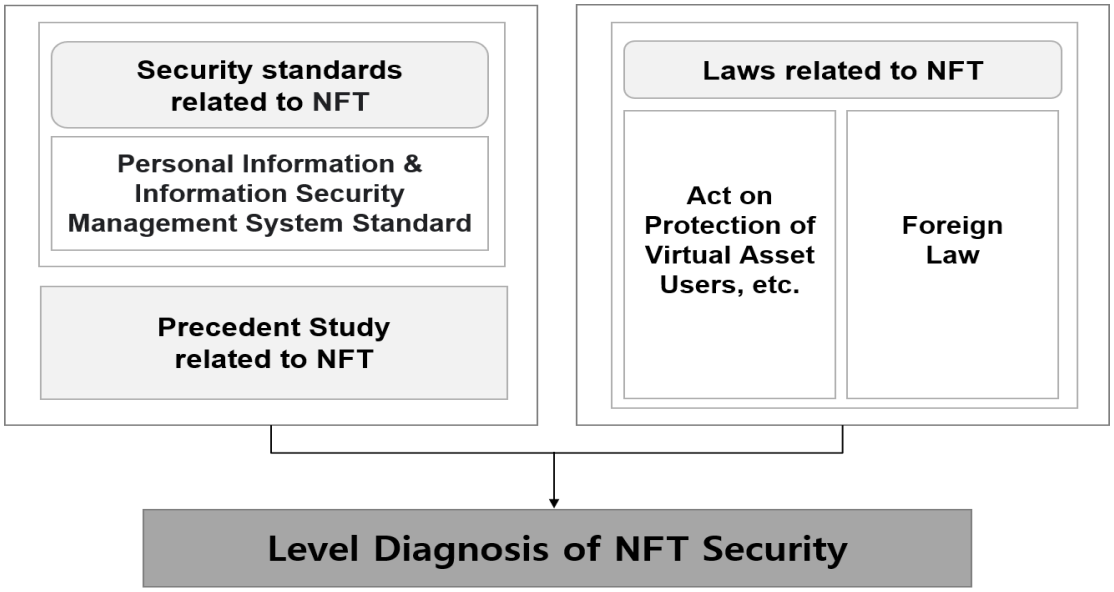

Figure 1. Derivation of Checklist of NFT
그림 1. NFT 보안 점검 항목 도출 도식도

그리고 도출된 NFT 보안 수준 점검 항목들은 본 모형의 계층화 요소로 이용한다. 좀더 살펴보면 멀티시그 등의 MFA 인증이 안되어 있어 공격자가 인증을 우회하거나 NFT 서비스 사업자의 시스템 관리자 권한 관리 미흡으로 인한 정보 유출 등의 보안 위협으로 NFT 이용자의 디지털 자산이 불법 탈취될 수 있다. 이에 불법 인증 우회와 중요 시스템 관리자 권한 탈취 등을 탐지 · 대응할 수 있는 인증 및 권한 관리가 필요하다. 따라서 보안관리 체계인 ISMS-P 의 2.5 키관리 시스템, 월렛 서버 등의 NFT 정보 인프라에 접속할 수 있는 관리자의 계정과 권한 관리를 수행하는지와 정보시스템 접근시 안전한 인증절차와 인증방식을 적용했는지를 점검하는 사용자 인증 항목을 인증 및 권한 관리 점검 항목으로 도출하였다. 도출된 해당 항목을 Jung et al.연구에서 제안한 NFT 거래관련 보안 위협 Spoofing Identify 의 T1, T2 등과 매핑하여 기술적 부문의 NFT 인증 및 권한 관리 점검 항목으로 최종 확정하였다. 다음 '표 1' 은 관련 법률, 보안 컴플라이언스와 기존 관련 연구들로부터 도출된 NFT 보안 관리 수준 점검 항목들이다.

Table 1. Checklist derived by this study for NFT security
표 1. NFT 보안 점검 연구를 통해 도출된 점검 항목

Item	Checklists	Description
Administrative Diagnosis	Establishment and operation of a security management system	Plan and implement an overall security management system related to NFT
	Establishment of a dedicated organization	Forming and operating a dedicated organization for NFT platform security
	Risk Management of NFT Platform	Identify NFT platform assets and evaluate risks to establish risk scenario measures
	Security management system inspection and improvement	Check whether the security management system is operating effectively and reflect improvements
Technical Diagnosis	Authentication and authority Management	User authentication and access rights management to NFT platform
	Access Control	Access control such as user access control to the NFT platform, safe network access, and network separation
	Encryption	Encryption during data storage and transmission for NFT service
	Development Security	Establish and implement development security policy
	Security operation management	Manage IPS, DDoS, etc. for safe NFT service, and manage security operations such as SW update PMS, vaccine, etc.
	Logging and security monitoring	NFT platform security log storage and monitoring
Physical Diagnosis	Physical access control	Physical access control to major physical facilities such as computer facilities and offices
	Wallet physical access control	Block illegal access to wallet-related physical facilities

3.2 연구 모델

도출된 NFT 보안 점검 항목을 기반으로 항목간 상대적 중요도 평가를 위한 연구 모델은 '그림 2'와 같다. 제 1 계층은 연구 모델 목표, 제 2 계층은 하위 평가 기준을 NFT 보안 수준 점검 항목 3 개 영역으로 구성하고 물리적, 기술적, 관리적 점검으로 구분하였다.

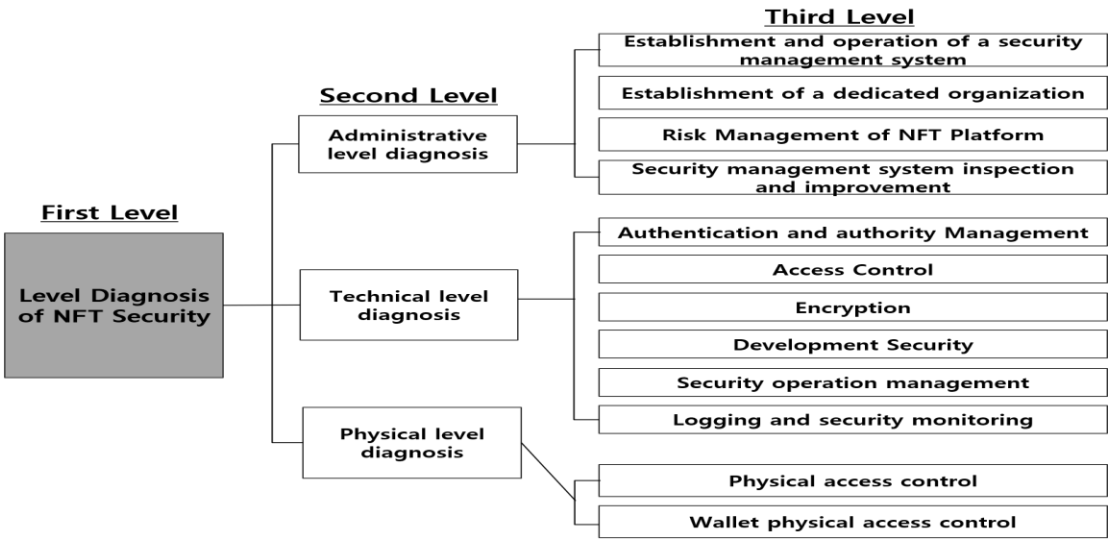

Figure 2. Hierarchy Model
그림 2. 계층 모델

제 3 계층에서는 12 개의 하위 항목으로 구성하고 관리적 보안 점검 하위 항목은 NFT 보안 관리 체계 수립 및 운영, 전담 조직 구성, 위험관리, 보안 관리 체계 점검 및 개선이며 기술적 보안 점검 하위 항목은 접근 통제, 인증 및 권한관리, 암호화, 개발보안, 보안 운영관리 등이다. 마지막으로 물리적 수준 항목은 주요 물리 시설 접근 통제, 월렛 물리적 접근 통제이다.

3.3 연구 방법

3.3.1 방법 및 표본 특성

본 연구관련 AHP 설문 조사는 2023 년 6 월 12 일부터 7 월 12 일까지 실시하였고 설문 방법은 설문의 객관성과 정확도를 목적으로 유선으로 먼저 각 항목에 대해 설명하고, 이메일 또는 직접 방문을 통해 작성했다. 설문지의 평가 항목은 3 개의 상위 점검 항목과 3 계층의 12 개 하위 점검 항목으로 구성하여 동일 계층간 쌍대비교 하였다. 또한 평가 수치 척도는 AHP 설문에서 많이 사용하는 9 점 척도를 이용하였고, 가중치 분배는 비교 대상의 가중치들을 모두 더하면 1 이 되는 모드를 이용하였다. 즉 두 개의 점검 항목을 서로 비교하는데 어떤 항목이 상대적으로 중요한지를 9 점 척도 내에서 점수를 부여하여 구성했다. 또한 대상자는 5 년 이상의 정보보호 경력 및 CISSP, CISA, ISMS-P 등 공인 정보보호 자격증을 가진 회사의 보안 전문가로 선정하였다. 따라서 정보보호 전문가 22 명으로부터 상대적 중요도를 산출, 일관성 비율이 0.1 이상인 1 부를 제외하고 유효한 21 부를 분석에 이용하였다. 표본의 인구 통계학적 특징을 살펴보면 응답 연령은 40-49 세가 57.1%로 가장 비중이 높았으며, 학력은 석사 42.9%, 박사 9.5%로 전체의 52%이상을 차지하였다. 또한 보안 경력은 11-19 년 47.6%, 다음으로는 20 년 이상이 28.6% 등의 순으로 나타났다. 다음으로는 6-10 년 사이가 14.3%, 3-5 년 사이가 9.5% 등의 순으로 확인되었다.

3.3.2 AHP 절차

본 연구에서는 상대적 중요도 분석을 단계적으로 수행하였는데 1 단계는 NFT 보안 수준 점검을 계층화하였다. 2 단계로서 전문가 22 명에게 AHP 관련 설문 조사를 진행하고, 해당

설문은 2 개의 항목을 쌍대비교 하여 어떤 점검 항목이 상대적으로 중요한지를 평가하는 것이다. 3 단계는 유효성 검증으로 일관성 비율을 확인한후 쌍대비교 행렬 값을 이용하여 점검 항목 계층별 상대적인 중요도를 계산하였다. 마지막으로 각 계층의 상대적 중요도 값을 곱하여 나온 수치로 우선 순위를 도출하였다.

IV. 실증 결과

NFT 보안 수준 점검 영역 및 하위 세부 점검 항목관련 상대적 중요도 분석 결과는 '표 2'와 같다.

Table 2. The priority analysis of importance among checklists
표 2. 점검 항목간 상대적 중요도 분석

Higher Standard		Lower Standard			Final Relative importance	Priorities
Classification	Relative importance of higher Standard	Checklists Item	Relative importance of Lower Standards	Priorities of Lower Standard		
Administrative Diagnosis	0.5880	Establishment and operation of a security management system	0.6480	1	0.3810	1
		Establishment of a dedicated organization	0.0260	4	0.0153	11
		Risk Management of NFT Platform	0.2500	2	0.1470	3
		Security management system inspection and improvement	0.0760	3	0.0447	6
Technical Diagnosis	0.3530	Authentication and authority Management	0.2530	2	0.0893	4
		Access Control	0.1340	3	0.0473	5
		Encryption	0.4320	1	0.1525	2
		Development Security	0.0850	4	0.0300	8
		Security operation management	0.0640	5	0.0226	9
		Logging and security monitoring	0.0320	6	0.0113	12
Physical Diagnosis	0.0590	Physical access control	0.3330	2	0.0196	10
		Wallet physical access control	0.6670	1	0.0394	7

이를 통해 상부 영역인 제 2 계층의 각 영역별 가중치 및 순위를 파악하고, 하부 영역 제 3 계층의 세부 보안 점검 항목별 가중치 결과값들을 확인할 수 있다. 그리고 제 2 계층과 3 계층을 종합하여 하위 점검 항목별 전체 가중치에 대한 상대적인 우선 순위를 파악할 수 있다. 상세 결과를 좀더 살펴보면, 상부 영역 간의 쌍대 비교 수치는 관리, 기술, 물리 수준 점검의 중요도 결과가 58.8%, 35.3%, 5.9%로 나타났다. 따라서 2 계층에서 관리적 보안 점검이 가장 중요한 것으로 확인할 수 있었다. 이러한 결과는 체계적인 보안관리 체계 기반 마련, 자원 할당, 안정적 보호대책 운영 등을 포함하는 NFT 관련 보안 관리체계 수립 · 운영과 주요 자산 식별, 위험평가, 정보 보호 대책 수립 등을 수행하는 위험 관리인 관리적 보안 부문이 베이스라인으로 구조화되어야 NFT 보안을 확보할 수 있기 때문이다. 또한 관리적 보안 부문의 베이스라인이 취약한 보안관리 체계상에서 기술적 보안 수준 점검은 효과적일 수 없다.

하부 영역을 살펴보면 NFT 관리적 보안 점검 측면의 하부 영역관련 우선 순위 분석 결과, 보안 관리 체계 수립 및 운영이 64.8%로 가장 높고 위험관리 25%, 보안 관리 체계 점검 및 개선 7.6%, 전담 조직 구성 2.6% 순으로 나타났다. 특히 보안 관리체계 수립 및 운영이 가장 높게 나타난 것은 보안 관리체계 기반 마련, 보안 관리체계 운영 등이 NFT 보호를 위해 라이프사이클 측면에서 보안 관리 체계를 전반적으로 안전하게 확립하는 것이기 때문이다. 기술적 점검 측면의 하부 영역 우선 순위 분석 결과, 암호화가 43.2%로 가장 높은 수치를 보이며 인증 및 권한관리 25.3%, 접근 통제 13.4%, 개발 보안 8.5%, 보안 운영관리 6.4% 등으로 나타났다. 그중 상대적으로 암호화가 중요하다고 판단되는 이유는 가상 자산의 핵심인 개인키 탈취의 위협에 월렛 개인키 관리 등의 암호화를 통해 가장 효과적으로 수행해야 한다는 것이며, 기능 측면에서는 중요 데이터 송수신 · 저장시 암호화 적용으로 공격자가 정보 식별을 할 수 없기

때문이다. 물리적 점검 측면의 하부 영역 우선 순위 분석 결과, 물리적 통제 33.3%, 월렛 물리적 접근 통제는 66.7% 순으로 나타났다. 즉 상대적으로 월렛 물리적 접근 통제 부문이 중요하게 나타난 것은 고객의 자산인 월렛을 운영 · 보관하고 있는 월렛 물리시설 보호가 설비, 정보시스템 등의 기타 시설 물리적 접근 통제보다 더 중요하다고 판단했기 때문이다.

상부와 하부 영역의 상대적 가중치를 통해서 최종 우선순위를 살펴보면 NFT 관리적 보안 수준 점검 영역의 보안 관리 체계 수립 및 운영이 38.1%로 1 순위, 기술적 점검의 암호화가 15.2%로 2 순위, 관리적 수준 점검 영역의 위험관리가 14.7%로 3 순위 등의 순서로 나타났다. 따라서 보안 수준을 조기에 식별하고 위협에 대응하고자 하는 회사에서 상대적 우선 순위를 활용하면, 효과적으로 NFT 보안 수준 점검 활동을 수행할 수 있을 것이다. 아래 '표 3'에서는 기존 연구와 비교하여, 본 모형의 우수성을 평가하였다.

Table 3. The Comparison precedent Studies with Proposed Model
표 3. 기존 연구와의 비교를 통한 평가

Evaluation items		Precedent Studies	Proposed Model
Compliance	Security Standard System	Not referenced	Personal Information & Information Security Management System Standard Compliance analysis
	Law	Not referenced	Analysis of various laws, including foreign laws
Research method		fragmentary Studies for focusing on technological security trend	Integrated Study that combines physical, technical, and administrative security item
Checklists and their relative importance		Few Precedent Study	Derivation of check item for the first time through security threat technology analysis and compliance Identification of relative Importance ranking by AHP

선행 연구는 기술적 보안 트랜드 중심의 단편적 연구로 NFT 보안 위협만 분석하여, 통합적으로 NFT 보안 수준을 점검하는데 어려움들이 존재했으나 본 연구에서는 관련 법률, 가상자산사업자 ISMS-P 등의 컴플라이언스를 분석하고 이를 물리적보안 · 기술적보안 · 관리적 보안 항목으로 결합한 통합적 연구로, NFT 보안 위협에 대응할 수 있다. 또한 점검 항목간 상대적인 중요도를 AHP 기법으로 파악 · 제공하여 NFT 보안 수준 점검을 위한 시간과 자원이 부족한 경우에 상대적으로 중요한 항목들을 우선 점검한다면, NFT 보안 관리 수준을 보다 빠르게 식별할 수 있다.

V. 결론

NFT 의 시장 확대와 다양한 분야와의 연계로 해킹 공격 경로가 다양해지고 있어, 결국 NFT 의 보안 위협도 증가하고 있다. 따라서 이용자의 가상자산을 활용하는 NFT 보안 강화를 위해 본 연구는 NFT 특징, 보안 위협, 국내외 관련 법률, 컴플라이언스 등 NFT 보안 관련 현황 분석을 통해서 점검 항목을 도출하였다. 이를 기반으로 AHP 기법에 적용하여 상대적 중요도를 확인하였다. 결과를 요약하면 점검 항목 중요도 평가관련 상부 영역 중에서 NFT 관리적 보안 수준 점검 영역이 가장 중요한 것으로 확인되었다. 이러한 결과는 체계적인 보안관리 체계 기반 마련, 자원 할당, 안정적 보호대책 운영 등을 포함하는 NFT 관련 보안 관리체계 수립 · 운영과 자산식별, 위험평가, 정보 보호 대책 수립 등을 수행하는 위험 관리 등의 관리적 보안 점검 항목들이 베이스라인으로 체계적으로 잡혀 있어야, 그것을 기반으로 물리적 보안 · 기술적 보안 점검을 안정적으로 수행할 수 있기 때문이다. 또한 하부 영역에서 암호화, 위험관리 등이 상위 랭크되었는데 그중 암호화를 중요하게 판단한 이유는 가상 자산의 핵심인 개인키 탈취의 위협에 월렛 개인키 관리 등의 암호화를 통해 가장 효과적으로 수행해야 한다는 것이며, 중요 데이터 송수신 · 저장시 암호화 적용으로 공격자가 데이터를 탈취하더라도 정보 식별이 불가능하다는 것이다.

본 연구의 의의는 NFT 보안 수준 점검관련 선행 연구가 거의 존재하지 않는 상황에서 컴플라이언스 분석을 토대로 물리적 · 기술적 · 관리적 보안 수준 점검 항목을 도출하고 제안 모형을 실증함으로써 금융 자산을 침해할 수 있는 사이버 공격에 통합적으로 대응할 수 있다는

것이다. 그리고 조직들이 시간과 자원 부족 및 짧은 시간 안에 보안 수준을 식별해야 하는 경우, 해당 연구 결과의 상대적 중요도 항목중에서 상위 랭킹 항목들을 활용하여 보안 점검을 수행한다면, 전체 점검 항목 대비 시간 · 비용 절감 효과와 보안 수준들에 대한 조기 식별이 가능할 것이다.

마지막으로 본 연구는 AHP 로 검증했지만 다소 일반화하는데 한계가 있어, 추가적인 사례 연구가 더욱 필요할 것이다.

VI. 참고문헌

[1] Maeil Business Newspaper, "Last year, NFT transaction volume exceeded 30 trillion won.", https://www.mk.co.kr/economy/view.php?sc=50000001&year=2022&no=43422
[2] Chosunilbo, "NFT market takes a hit due to FTX bankruptcy.", https://biz.chosun.com/stock/finance/2022/12/06/536WXBQFN5DF3HQUUEAKIHWBZI/
[3] ITworld, https://www.itworld.co.kr/numbers/82002/249538
[4] Korea JoongAng Daily, "Can NFTs be hacked too?", https://www.joongang.co.kr/article/25102934#home
[5] Money Today, "2 billion stolen in 3 hours", https://news.mt.co.kr/mtview.php?no=2022022113592917335
[6] H. K. Kim, “A Study on Legal Issues in NFT Content Transactions,” Sungkyunkwan Law Review, Vol. 33, No. 3, pp. 394-395, Sep. 2021.
[7] H. J. Song, S. H. Jeong, and K. B. Kim, “Utilizing Hash Algorithms for NFT Data File Integrity Checks,” Journal of Digital Contents Society, Vol. 24, No. 7, pp. 1531-1532, Jul. 2023.
[8] KISA, “Metaverse and NFT, Cybersecurity Threat Outlook and Analysis”, https://www.kisa.or.kr/20301/form?postSeq=12&lang_type=KO
[9] Lee&Ko, “Current issues and laws in digital finance”, https://www.leeko.com/upload/news/newsLetter/900/20221018104428442.pdf
[10] Satty T. L., “Axiomatic foundation of the Analytic Hierarchy Process,” Management Sci., Vol. 32, No. 7, 1986, pp. 841-850.
[11] S. H. Jung, C. M. Lee, “A Study on the Analysis of Security Threats of NFT Transaction in Korea,” Korean Journal of Industrial Security, Vol. 12, No. 1, pp. 302-307, Dec. 2022.
[12] D. Y. Lee, Y. J. Kim, and J. W. Yoon, “A Study Information Security Governance requirement of domestic NFT marketplace,” Journal of Information Technology Service, Vol. 24, No. 7, pp. 634-636, Nov. 2021.

저자소개

임동성 (*Dong Sung Im*)

2011 년 4 월~2021 년 AhnLab 보안컨설턴트
2022 년 3 월~현재 오산대학교 컴퓨터정보계열 컴퓨터보안전공 교수

관심분야 : Cyber Security, Block Chain, Cloud, ISMS