https://doi.org/10.33778/kcsa.2024.24.3.051

# 가상자산 운영의 위험관리를 위한 내부통제 개선방안에 관한 연구

최 병 훈*, 이 진 용**, 전 삼 현***


## 요 약

블록체인 기술의 기반으로 만들어진 가상자산 사업자 및 가상자산을 운영사는 사이버위협과 내부인원을 통한 지갑탈취, 고객의 개인키 탈취, 부정 거래를 위한 가상자산 전송 서명과 같은 거래 리스크가 있다, 이러한 위협으로부터 안전하게 운영되수 있도록 ISMS-P라는 인증을 통해 보안성을 검증받고 있다. 본 연구는 가상자산 사업자 및 가상자산 운영사가 획득하고 있는 ISMS-P 인증 외 가상자산 사업자 및 운영사에 특화된 ISO TR 23576에서 제시하는 리스크를 분석하고 가상자산 사업자 점검용 ISMS-P와 ISO TR 23576의 세부 점검사항을 중심으로 중요도를 분석하고자 한다. 이를 기반으로 상위 주요 리스크에 대해 가상자산 사업자를 위한 내부 보안통제 업무 프로세스를 제안하여 실무담당자들이 효율적인 보안통제 업무를 수행하고자 한다.


# A Study on Improvement Measures for Internal Controls in Cryptocurrency

Byoung Hoon Choi*, JinYong Lee**, Sam Hyun Chun***


## ABSTRACT

Cryptocurrency service providers and virtual asset operators, built on blockchain technology, face transaction risks such as cyber threats, wallet theft by internal personnel, theft of customers' private keys, and fraudulent cryptocurrency transfer signatures. To ensure secure operations against these threats, their security is validated through the ISMS-P certification. This study to analyze the risks presented in ISO TR 23576, which is specialized for cryptocurrency service providers and operators, in addition to the ISMS-P certification they obtain. The study will focus on the detailed inspection items of ISMS-P and ISO TR 23576 for cryptocurrency service providers and assess their importance. Based on this analysis, the study proposes an internal security control process for cryptocurrency service providers to address the top-priority risks, enabling practitioners to perform security control tasks more efficiently.


**Key words : Blockchain, Cryptocurrency, Risk Management, IT Internal Controls, ISMS-P**

접수일(2024년 08월 19일), 게재확정일(2024년 09월 26일)

* 숭실대학교/IT정책경영학과 (주저자)
** 숭실대학교/IT정책경영학과 (공동저자)
*** 숭실대학교/IT정책경영학과 (교신저자)

# 1. 서 론

가상자산의 디지털 특성은 해킹과 같은 사이버 위협에 노출될 위험을 증가하고 있다. 이러한 위협으로부터 안전하게 보호하기 위해서는 적절한 보안 조치와 내부통제가 필수이다. 블록체인 기반으로 가상자산을 신규로 생성하고 발행하여 유통시키는 가상자산 운영사는 집계가 되지 않을 정도로 다양하다. 이러한 블록체인 기반으로 만들어진 비트코인이 등장한 2009년 이래로 NFT, 디지털코인, 암호토큰 등의 여러 형태로 경제적 가치를 가지는 디지털 자산으로 형성되었고 이를 활용한 경제시장은 꾸준히 증가하고 있다[1]. 시장의 증가에 따라 소비자를 보호하는 정책뿐만 아니라 가상자산의 생성, 가상자산의 거래, 가상자산의 운영 측면에서 시스템의 안정성, 사이버보안, 디지털 범위 등 가상자산과 관련된 이슈도 다양하게 증가하고 있다. 가상자산 생태계가 확산되고 있는 가운데 국내에서 내부 보안통제의 헛점을 이용한 사고가 발생한 사례가 있다. 블록체인 기업 오지스(OZYS)에서에서 발생한 사례로 1,000억 원대 규모의 가상자산 해킹 사건이 발생했으며 오지스의 정보보호 책임자가 보안장비 중 하나인 방화벽을 무력하게 만들어 사고를 일으킨 사례이다. 가상자산의 핵심 구성이 되는 블록체인은 소프트웨어(블록체인) 개발자, 암호화폐 운영자, 사용자 네트워크로 구성되며 운영된다. 다만 핵심의 일부 기술에 대해서는 외부 아웃소싱을 통해 운영이 되고 있다[2]. 소프트웨어 및 사용자 네트워크의 리스크에 대해서 다양한 솔루션을 도입·적용하여 외부로부터의 공격을 막는 것은 되지만 내부통제가 존재하지 않아 가상자산운영사의 내부자로 인한 악의적인 위해행위에 대해서 사전에 적발하기가 쉽지 않은 대표적인 사고사례이다. 이러한 사고에 대한 리스크는 개인키의 관리 및 서명리스크, 웹 해킹 및 불법적 로그인 등으로 인한 접속통제 리스크, 보안성이 낮은 H/W사용으로 인한 따른 H/W리스크 등이 대표적이다. 이 모든 리스크는 내부 관리자 및 외부 사용자의 부정행위를 통한 자산이동이며 개인 또는 조직에 대한 금전적 손실로 이어진다[3]. 이러한 리스크의 대응을 위해 국내 가상자산 사업자의 경우 법적으로 ISMS-P 획득하게 하여 보안성을 검증하고 있다. 해외 가상자산 사업자 및 가상자산 운영사의 경우 국제적 보안 표준인 CCSS 또는 ISO TR 23576을 기반으로 보안성을 검증하고 있다[4]. 본 논문에서는 가상자산 사업자 및 가상자산 운영사의 국내 보안인증제도인 ISMS-P와 글로벌 표준 보안 인증제도인 ISO TR 23576의 항목별 중요도를 비교 및 분석하고 개선될 인증항목의 우선순위를 도출한 후 세부 통제업무 프로세스의 도출 및 제안하고자 한다. 도출된 개선사항의 통제업무 프로세스를 통해 가상자산 사업자 및 가상자산 운영사에 대한 내부통제를 강화하고 신뢰성 및 안전성을 확보하여 가상자산의 안전한 환경 활성화에 기여하고자 한다.

# 2. 내부 보안통제에 관련 사례연구

## 2.1 금융 기관의 내부 보안통제 현황

금융기관의 경우 ISMS-P 및 전자금융 감독 규정으로 정보보안사고 및 내부 보안통제를 실시하고 있다. 그러나 정보보안 및 내부 통제사고가 끊이지 않는 이유는 내부통제 시스템은 구축되어 있으나 시스템 자체가 작동되지 않았거나 내부통제 시스템의 운영에 있어서 형식적인 운영이 사고의 원인이다[5]. 내부통제 시스템이 형식적으로 운영되는 이유는 경영진의 내부통제에 대한 형식적 운영 및 선진화된 내부통제 시스템 미비, IT금융에 대한 내부통제 시스템 이해도 미흡, 세부 통제항목에 대한 의지 부족이다[6]. 또한 내부통제 조직의 문제로 주요 내부통제 조직의 독립성 미흡, 통제활동 관련 직무분리 미흡, 내부통제 책임의 차원의 문제점, 전 직원의 통제문화 미형성이다[7].

## 2.2 가상자산 서비스 제공업체(VASP)의 내부 보안 통제 현황

우리나라 가상자산의 대표적인 5대 거래소인 코인원, 빗썸、업비트、고팍스、코빗에서는 임직원들 대상으로 가상자산 거래 제한 및 감독 규정을 규정하고 내부보안통제 및 모니터링을 하여 리스크에 대한 예방을 하고 있다. 일부 소규모의 가상자산 거래소는 임직원이 자사 거래소 계정으로 가상자산을 매매할 수 없다는 규정 외에 임직원 일탈을 차단할 수 있는

특별한 장치가 없다. 가상자산 거래소의 운영자는 내부 정보를 활용해 불공정거래를 쉽게 할 수 있으며 부정적 행위 가능성에 노출이 되어 있다[8]. 가상자산에 대한 운영이 용이한 가상자산의 운영사는 내부 임직원들의 일탈을 방지하기 위한 업무 프로세서의 독립성 및 무결성을 기반으로 하는 지시통제 및 예방통제의 강화 조치로 사고를 예방하고 있다[9]. 가상자산 사업자 및 가상자산 운영사는 공통적으로 국내법적 필수 인증인 ISMS-P를 획득하고 있으며 해외 각종 정보보호 인증인 ISO 정보보안 관리체계 및 개인정보보호 관리체계, 클라우드 보안에 대한 체계를 운영하여 사고에 대한 예방 활동을 하고 있다.

<표 1> 가상자산 거래소별 인증현황

| 거래소명 | 보안인증 현황 |
|---|---|
| 업비트 | 정보보호 관리 체계(ISMS-P)<br>ISO 27001, ISO 27017<br>ISO 27018, ISO 27701<br>ISO 22301 |
| 빗썸 | 정보보호 관리 체계(ISMS-P)<br>ISO 27001, ISO 27701<br>ISO 27017, ISO 27018 |
| 코인원 | 정보보호 관리 체계(ISMS-P)<br>ISO 27001 |
| 코빗 | 정보보호 관리 체계(ISMS-P)<br>ISO 27001, ISO 27701<br>ISO 27017, ISO 27018 |
| 고팍스 | 정보보호 관리 체계(ISMS-P)<br>ISO 27001, ISO 27017<br>ISO 27018 |

## 3. 정보보호 보안통제 비교

5대 가상자산 사업자들이 법적 인증사항인 ISMS-P를 제외하면 ISO 27001을 공통으로 획득하고 있다. ISMS-P의 경우 가상자산 사업자에 특화된 항목이 있으나 ISO 27001의 경우 정보보안 경영 국제표준으로 조직의 비즈니스에 필요한 품질경영, IT 서비스경영, 사이버보안, 사업연속성경영, 위험관리등 정보보안의 포괄적인 내용으로 가상자산사업자 및 가상자산 운영사에 특화된 내용을 담고 있지는 않다. 각 인증제도에서 중점적으로 확인하는 도메인을 도출하기 위하여 각 인증기준에서 제시하는 전체 인증항목에서의 도메인별 인증항목 비율을 확인 하였다[10].

### 3.1 ISMS-P 보안 통제의 정의

ISMS-P는 각 조직에서 정보보호 관리체계를 위한 일련의 조치와 활동이 인증기준에 적합함에 대해 한국인터넷진흥원 또는 인증기관이 점검하고 증명하는 제도이다. ISMS-P의 경우 관리체계 수립 및 운영 영역과 보호대책 요구사항 영역, 개인정보 처리단계별 요구사항 영역으로 세 가지로 구성되어 있다. 관리체계 수립 및 운영 영역은 4개 분야 16개의 인증기준으로 구성되어 있으며 가상자산사업자 대상 주요 확인사항 11개를 포함하여 총 27개의 확인 사항으로 이루어져 있다. 보호대책 요구사항 영역의 경우 12개 분야 64개 인증기준으로 구성되어 있으며 가상자산사업자 대상 주요 확인사항 45개를 포함하여 총 109개의 확인 사항으로 이루어져 있다. 개인정보 처리단계별 요구사항영역의 경우 21개의 기준으로 구성되어 있다.

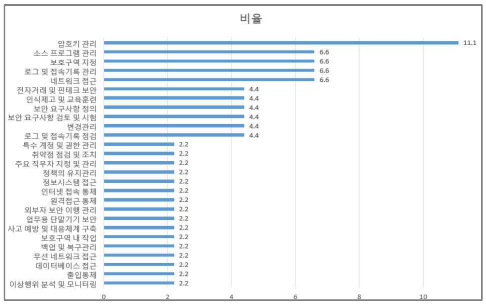
### 3.2 ISO TR 23576 보안 통제의 정의

ISO TR 23576의 경우 ISO 27001의 표준 및 연구를 기반이며 가상자산 관리자에 대한 주요 내용으로 구성되어 있다. 세부적으로 가상 자산 관리자의 모범사례, 고객의 자산을 보호하기 위한 설계, 구현하는 보안 위험 및 위협의 조치로 작성되어 있다. 가상자산 사업자 및 가상자산 운영사의 위협에 대해 제시하는 가상자산관리자의 보안통제 사항은 크게 5가지로 구성되어 있다. 가상자산 수탁 서비스 모델의 기본, 보안관리 목표, 보안 통제, 위험 관리, 기술 관리로 되어 있다. 이중 보안관리 목표는 ISMS-P의 관리체계 수립 및 운영과 유사하며 보안 통제, 위험 관리, 기술 관리 영역은 보호대책 요구사항과 유사하다. 보안통제(security control)는 14개의 도메인으로 구성되어 총 177개의 점검항목으로 구분되어 진다. 또한 가상자산 사업자 및 가상자산 운영사의 보안 위협에 대해 정의하고 이에 대한 보안 통제사항을 서명리스크, 개인 키 리스크, 전송리스크, 로그인 및 웹 해킹 리스크, 자산 분실 리스크, 디바이스 공급 리스크로 정의하였다.

### 3.3 ISMS-P와 ISO TR 23576 통제비교

가상자산 관련 인증제도 및 표준의 경우 국낸 ISMS-P와 글로벌 표준인 ISO TR 23576에서의 바라보

는 시각이 각각 다르다. 이에 인증제도 및 보안표준별 중점적으로 확인하는 도메인을 도출하기 위하여 전체 인증항목 및 글로벌 표준에서 제시하는 도메인별 인증항목 비율을 확인하여 중요도를 측정하였다. 그중 가상자산 사업자들이 공통으로 획득하고 있는 가상자산 사업자용 ISMS-P의 45개의 점검 상세내용에 대한 도메인별 인증항목 중요도를 (그림 1)과 같이 확인하였다.




(그림 1) ISMS 인증 도메인별 중요도

가상자산사업자를 위해 점검항목 중에서 인증항목 비율이 가장 높은 도메인은 암호키 관리(11%), 네트워크 접근통제 (6.6%), 로그 및 접속관리 및 보호구역 지정, 소스 프로그램관리가 각각 (6.6%)씩으로 중요도가 평가되었다. 그 외 인식 및 복구관리, 주요 직무자 지정 및 관리, 특수계정관리의 경우 2.2%씩 비율이 되어 중요도가 낮은 것을 확인하였다. 또한 가상자산 사업자 및 가상자산 운영사의 관리자에 대한 ISO TR 23576의 보안통제는 14개의 도메인과 177개의 점검항목에 대한 도메인별 인증항목 비율을 (그림 2)와 같이 확인하였다.

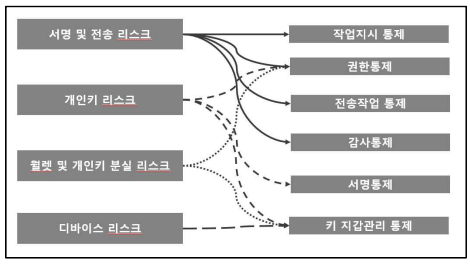

(그림 2) ISO TR 23576 도메인별 중요도

가상자산사업자를 위해 비율이 가장 높은 도메인은 서명 키에 대한 보안 통제 (12.4%), 접근통제 (8.5%), 통신 및 네트워크 보안 (7.9%), 정보사고 관리 및 인적 보안 (각각 7.3%) 등으로 중요도가 평가되었다. 그외 ISMS-P에서 제시하지 않았던 정보보안 조직 (5.6%), 공급망관리 (6.2%)로 나타났으며 물리적 환경보안 (4.5%)로 중요도가 낮은 것을 확인하였다. ISMS-P와 ISO TR 23576의 비교한 결과 공통으로 암호키 및 서명, 네트워크 및 접근통제 또는 접근제어에 대한 중요도는 매우 높게 나타났다. 또한 공통으로 중요도가 낮은 도메인은 백업 및 복구관리, 정책 등의 유지관리, 비즈니스 연속성 관리 등으로 나타났다. ISMS-P의 경우 직무자의 직무 분리 및 역할 정의, 보안 사고관리 및 인적 보안 도메인의 중요도가 낮지만 ISO TR 23576에서는 직무 분리 및 역할, 사고관리 및 인적 보안의 도메인에 대해서 중요도가 높게 나타난 것이 확인되어 ISO TR 23576과 ISMS-P 간의 차이가 있음을 확인하였다.

## 4. 정보보호 보안통제 제안모델

### 4.1 가상자산 사업자의 운영자를 위한 보안통제 모델

ISMS-P와 ISO TR 23576에서의 공통으로 중요도가 높은 도메인인 키 관리 및 서명, 직무 및 인적 보안에 대한 리스크를 선정하였다. 가상자산 운영자의 독립성과 무결성을 기반으로 악의적인 부정적 행동이나 원치 않은 실수로 인한 부정의 발생할 수 있는 리스크를 예방하고 있다. 이에 대해 가상자산 관리자 또는 작업자의 리스크에 대한 통제행위에 대해 권한 통제, 키(지갑) 관리통제, 키 (지갑) 백업 통제, 작업지시 통제, 전송작업 통제, 서명 통제, 감사 통제로 정의하였고 각 리스크별 통제행위에 대해서 (그림 3)과 같이 정의하였다.




(그림 3) 리스크별 제안모델의 관계도

해당 리스크에 대한 가상자산 사업자 및 가상자산 운영사에서 운영해야 하는 통제항목별 세부 통제업무 프로세스를 도출하였다.

#### 4.1.1 작업자별 권한통제

가상자산에 대한 권한은 가상자산 관리자, 가상자산 담당자, 출입 관리자, 금고 관리자, 키 권한자, 가상자산 감사자로 구분하여 각 역할에 대해 독립성을 유지할 수 있도록 한다. 가상자산 관리자는 전반적인 가상자산 시스템 보안 관리에 대한 책임을 진다. 출입 관리자는 가상자산의 작업 및 가상자산 키를 보관하는 장소의 출입 통제를 책임진다. 또한 가상자산의 작업 및 가상자산 키를 보관하는 장소의 물리적 관리의 역할을 수행한다 금고 관리자는 가상자산 키를 보관하고 있는 금고 관리를 책임진다. 키 권한자는 자상자산 전송 시 반드시 필요한 역할로 가상자산의 개인키에 접근 가능한 권한자로서 보유된 키에 대한 접근을 통제 및 서명한다. 키 관리자는 지갑의 성격에 멀티시그방식(2of3 또는 3of5) 또는 MPC 방식으로 서명한다. 가상자산 담당자는 가상자산 전송 업무 수행에 따른 노트북 및 디바이스 관리하고 가상자산 전송 및 작업 업무 수행한다. 가상자산 감사자는 가상자산 전송결과에 따른 업무 감사한다. 위와 같은 조직담당자의 권한을 분리함으로써 작업의 독립성을 확보하고 내부자의 부정적 행위를 차단할 수 있다.

#### 4.1.2 개인 키 (지갑) 통제

실물자산과는 전혀 다른 특성이 있는 가상자산은 안전하고 신중하게 다루어야 한다. 하지만 지갑의 개인 키를 아는 사람이라면 누구나 쉽게 해당 가상자산을 탈취할 수 있는 단점을 가지고 있다. 작업에 사용되는 지갑의 안전성을 확보하기 위해 Private Key가 노출되지 않도록 하고, ISO/IEC 15408 EAL4, FIPS 140-2 level 3 등국제 표준 인증을 취득한 Secure USB 사용한다. Key 생성 절차는 명확한 업무분장을 가지며, Key 생성시 필요한 권한은 상호 감시·감독하에 적절한 담당자만 제한적으로 보유한다. 업무의 독립성을 위해 출입 담당자 최소 2인 이상으로 분리, 작업 담당자는 키 개발 관련 이해당사자가 아닌 독립적 인원, 정확한 절차 이행을 위한 감시 감독관 배치하여 부정의 발생할 수 있는 부분을 통제한다. 담당자는 이러한 Key 생성 정책에 따라 Key가 생성하는지를 주기적으로 검토하고 전결권자의 승인을 얻어 개인키의 노출 및 지갑 정보의 외부 노출을 통한 차단하여 가상자산의 탈취를 차단할 수 있다.

#### 4.1.3 개인 키 (지갑) 백업 통제

Key 백업은 적절한 최소 인원 및 안전한 장소(별도의 작업룸)에서 수행한다. 해당 작업은 작업완료 보고서에 기재 뒤 전결권자의 검토 및 승인을 얻는다. Key 백업이 발생할 시 이는 보관 중인 백업 Key의 현황을 파악하기 위해 백업 Key 관리 대장에 작성된다. 백업 관리 대장은 계정명, 주소, 백업 Serial Number, 저장 위치, 백업 일자 등 기재하고 주기적으로 검토되어 전결권자의 승인을 얻는다. 보안 USB의 분실, 파손 및 생성자의 유고 등 기타 불가피한 사정으로 인하여 해당 생성자의 백업 Shamir share file 및 Keystore file과 Passphrase의 열람이 필요한 경우, 열람 사유를 기재한 품의서를 작성하여 전결권자의 승인을 얻는다. 백업 Shamir share file, Keystore file 및 Passphrase의 복제가 필요한 경우, 복제 사유를 기재한 품의서를 작성하여 전결권자의 승인을 얻는다. 중요한 지갑을 안전하고 투명하게 관리하기 위해서는 Multy Sig형태의 서명권자를 지정하고 서명 시 관리된 지갑의 키에 대해서 서명하도록 명확히 구분하여 키의 분실 또는 키의 손상에 대해 안전한 복구가 가능하게 하였다.

#### 4.1.4 작업지시 통제

작업지시 통제는 작업의 수행 전 작업자의 권한분리, 예정작업의 구체적인 수행 내용 등을 작성하여 품의를 수행함으로 해당 작업에 대한 타당성을 나타낸다. 해당 내용은 감사 통제 시 수행작업의 기초가 되는 역할을 가진다. 작업지시는 해당 지갑 사용함에 있어 사용 목적, 작업일시, 작업장소, 사용 지갑 주소, 키 권한자, 작업자, 키 보관관리자 , 키 사용 감사자 등을 구분하여 전결권자의 승인을 얻는다. 지갑, 키 생성/변경, 가상자산 전송작업, Contract 배포 등 관련

작업품의서, 작업절차서, 결과에 대한 품의를 진행한다. 이때 작업절차서는 지갑, 키 생성/변경, 가상자산 전송작업에 대한 작업의 세부 내용으로 작업수행자와 명령어까지 세부 사항을 적어 작업에 대한 타당성 및 관련 근거를 마련하였다.

#### 4.1.5 전송작업 통제

전송작업통제는 사전에 작성된 작업 절차서를 기반으로 정채진 장소, 시간 작업자 외 출입, 가상자산 전송 및 Contract 배포 등의 주요 작업 시 통제구역으로 지정된 별도의 격리된 공간(작업룸)에서 작업을 실시한다. 전송작업은 가상자산 발행, 외부와의 Transaction, Transaction 소액 전송 테스트, Transaction 작업 승인, Transaction 관리, 지갑 내 잔고 모니터링도 구분된다. Transaction발생에 대한 내부 품의 상에 거래 상대방에 대한 Due Diligence 절차를 포함하여 Transaction 상대방에 대한 적격성을 확인한다. 다만 예외적으로 허용되는 긴급 건을 제외하고는 반드시 계약 전에 내부 품의 절차를 준수하여 승인 완료 후, 계약을 진행한다. Transaction 소액 전송 테스트의 경우 Transaction 수행 전, 소액 전송 테스트를 수행한다. 해당 절차는 Transaction 절차서에 기재되어 검토되고 전송 결과 품의서에 첨부되어 상위권 자의 승인을 얻는다. 아는 작업 중 부정한 작업에 대해 발생할 수 있는 리스크에 대해서 탐지하고 관리함으로써 작업자의 부정행위를 차단할 수 있다,

#### 4.1.6 서명 통제

금액 또는 전손 지갑의 성격 등에 대한 서명 인원 또는 서명자의 지위 등에 대한 사전에 정의한다. 서명을 하기 위한 블록체인 시스템 접속 시 지정된 단말에서 지정된 담당자만이 접속할 수 있도록 통제한다. 서명용 월렛 또는 보안 USB에 접속할 수 있는 권한자는 최소화하여 관리한다. 작업 및 서명은 사전에 정의된 절차 및 방법을 통해서만 사용(전송 등)될 수 있도록 통제한다. 보안성이 높은 서명을 통해 외부에서의 대리 서명 등의 리스크를 차단할 수 있다.

#### 4.1.7 감사 통제

전송 후 Transaction Hash를 통한 작업 과정 및 결과에 대해 검토한다. 최초 작업 지시서 및 작업절차에 대한 대조와 Contract 배포 등 관련 작업 관련 품의서 및 작업계획서, 작업 결과서를 토대로 거래 시 비정상적인 행위탐지 정책(예:디지털 자산 간의 교환 횟수、 디지털 자산 단일 거래 수량 등) 에 위반사항에 감사하도록 통제한다. 이상이 발생 시 작업절차서 및 작업일지 등을 확인 후 요청자 또는 작업자, 서명자들에 대한 감사를 실시하여 모든 작업 통제절차의 무결성을 확보하여 외부감사에 대응하기 용이하다.

## 5. 결론 및 제언

가상자산 사업자 및 가상자산 운영사의 경우 내부 보안통제가 있음에도 불구하고 사고가 증가하고 있다. 가상자산 사업자 및 가상자산 운영사는 보안 사고를 방지하기 공통적으로 ISMS-P, ISO 27001을 통해 보안통제를 하고 있다, 그러나 ISMS-P와 ISO 27001의 경우 정보보안의 포괄적인 내용으로 가상자산사업자 및 가상자산 운영사에 특화된 내용이 부족하다. 또한 가상자산 운영에 대한 세부적인 프로세스에 관한 사례들이 없어 가상자산 사업자 및 가상자산 운영사의 담당자는 어려움을 겪을 수밖에 없다. 이와 같은 문제를 개선하기 위해서 가상자산에 특화된 ISO TR 23576과 ISMS-P의 항목의 중요도를 파악하고 높은 중요도에 따른 리스크에 대해 실무적 측면에서 활동할 수 있는 통제 프로세스에 대해 권한통제, 키(지갑) 관리통제, 키 (지갑) 백업통제, 작업지시 통제, 전송작업 통제, 서명통제, 감사통제과 같은 통제별 세부 프로세스를 제안하였다. 이를 통해 가상자산 사업자 및 가상자산 운영사의 리스크에 대해서 실무담당자들이 통제업무를 효율적으로 활용할 수 있도록 기여 하였다. 추후 가상자산사업자 및 가상자산 운영담당자의 견해 및 의견 등이 반영되어 있는 통제 프로세스 설계가 필요하다. 또한 ISO TR 23576의 통제 뿐만 아니라 내부 회계감사 기준 및 CCSS등과 같은 국제 표준통제에 대한 비교분석을 통해 가상자산 사업자 및 가상자산 운영사에서 가지고 있는 리스크에 대한 통제사항 및 프로세스를 제시하고자 한다. 해당 프로세스를 통해 경제적 효율성 및 추가적인 리스크의 우선순위의

신뢰성을 보완하여 가상자산 거래의 안전성 및 신뢰성을 확보한다면 전 세계 금융시장에 긍정적인 영향을 줄 것으로 기대해 본다.

## 참고문헌


[1] Cryptocurrency Market Capitalizations, https://coinmarketcap.com/charts/.

[2] D.S Choi, “A case study of blockchain-based fintech innovation in Latin ”, Jouranl of Information and Security, Vol 21, No. 5, pp121-128, 2021, DOI:https://doi.org/10.33778/kcsa.2021.21.5.121.

[3] B. H Choi, jylee, nhkoh, shchun, “ A study on QR code-based backup methods to strengthen the security of Cold wallet Purse”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 23, No. 6, pp.21-26, 2023, DOI:https://doi.org/10.7236/JIIBC.2023.23.6.21

[4] Y. H. KIM "A Study on the Improvement of ISMS(Information Security Management System) Control Items Considering the Environment of Virtual Asset Service Provider", Konkuk University, 2023.

[5] Sean J. Coughlin and Angela A. Turiano, "Cryptocurrency Compliance and Regulatory Considerations", Journal of Financial Planning, 2023.

[6] Y. B. Lee, “A Study on Roles and Effects of Financial Institutions′ Internal Control System”, The Graduate School of Public Administration Yonsei University, 2008.

[7] Suhag, pandya.murugan, "Cryptocurrency: Adoption efforts and security challenges in different countries", HOLISTICA - Journal of Business and Public Administration, Vol. 10, Issue 2, pp. 167-186, 2019, DOI:10.2478/hjbpa-2019-0024.

[8] H. J. Song, "A Study on the Tooling of Money Laundering Using Cryptocurrency", Journal of the Society of Disaster Information, Vol. 17, No. 3, pp. 600-607, 2021, DOI:https://doi.org/10.15683/kosdi.2021.9.30.600.

[9] I. I. Shin and I. K. Yoon, “A Case Study on the Internal Control System to Secure IPE Reliability”, Korean Accounting Journal, 31(5) 253-281, 2022, DOI:https://doi.org/10.24056/KAJ.2022.07.006.

[10] E. J. Kim and J. H. Koo and U. M. Kim “Improvement of ISMS Certification Components for Virtual Asset Services: Focusing on CCSS Certification Comparison”, KIPS Transactions on Computer and Communication Systems, Vol 11, No. 8, pp.249-258, 2022, DOI:https://doi.org/10.3745/KTCCS.2022.11.8.249.


## 〔저자소개〕


최 병 훈(Byoung-hhon Choi)
숭실대학교 산업정보시스템 공학(석사)
현재 숭실대학교 IT정책경영학과 박사과정
관심분야 : 제로 트러스트, 정보보안, 블록체인, E-Commerce

이 진 용(JinYong Lee)
연세대학교 컴퓨터과학과(석사)
현재 숭실대학교 IT정책경영학과 박사과정
관심분야 : 제로 트러스트, 블록체인, 정보보호 및 개인정보보호 IT 및 정보보호 법률·정책

전 삼 현(Sam-Hyun Chun)
숭실대학교 법학과(석사)
프랑크푸르트대학교 법학과(박사)
현재 숭실대학교 법학과, IT정책경영학과 교수
관심분야 : 블록체인, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책