KIPS Trans. Comp. and Comm. Sys.
Vol.11, No.8 pp.249~258
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2022.11.8.249

Improvement of ISMS Certification Components for Virtual Asset Services: Focusing on CCSS Certification Comparison

Kim Eun Ji† · Koo Ja Hwan†† · Kim Ung Mo†††

ABSTRACT

Since the advent of Bitcoin, various virtual assets have been actively traded through virtual asset services of virtual asset exchanges. Recently, security accidents have frequently occurred in virtual asset exchanges, so the government is obligated to obtain information security management system (ISMS) certification to strengthen information protection of virtual asset exchanges, and 56 additional specialized items have been established. In this paper, we compared the domain importance of ISMS and CryptoCurrency Security Standard (CCSS) which is a set of requirements for all information systems that make use of cryptocurrencies, and analyzed the results after mapping them to gain insight into the characteristics of each certification system. Improvements for 4 items of High Level were derived by classifying the priorities for improvement items into 3 stages: High, Medium, and Low. These results can provide priority for virtual asset and information system security, support method and systematic decision-making on improvement of certified items, and contribute to vitalization of virtual asset transactions by enhancing the reliability and safety of virtual asset services.

Keywords : Virtual Asset, Virtual Asset Exchange, Virtual Asset Service, ISMS, CCSS

안전한 가상자산 서비스를 위한 ISMS 인증항목 개선에 관한 연구: CCSS 인증제도 비교를 중심으로

김 은 지† · 구 자 환†† · 김 응 모†††

요 약

비트코인이 등장한 이후, 다양한 가상자산이 가상자산 거래소의 가상자산 서비스를 통해 활발하게 거래되고 있다. 최근 가상자산거래소에 대한 보안사고가 자주 발생하고 있어 정부는 가상자산 거래소의 정보보호 강화를 위해 Information Security Management System (ISMS) 인증 획득을 의무화하고 있으며, 이를 위한 56개 특화항목을 추가로 제정하였다. 본 논문에서는 ISMS와 암호화폐를 이용하는 모든 정보시스템에 대한 요구사항을 담고있는 CryptoCurrency Security Standard (CCSS)의 도메인 중요도를 비교하고 상호매핑을 한 후 그 결과를 분석하여 각 인증제도의 특성을 통찰하였으며, 도출된 개선항목의 중요도 평가를 통해 개선항목에 대한 우선순위를 High, Medium, Low 등 3단계로 분류하여 High Level 4가지 항목에 대한 개선사항들을 도출하였다. 이러한 결과는 가상자산 및 정보시스템 보안에 대한 우선순위를 제공하고 인증항목 개선에 대한 방법 및 체계적인 의사결정을 지원할 수 있을 뿐만 아니라 가상자산서비스에 대한 신뢰성 및 안전성을 제고하여 가상자산 거래 활성화에 기여할 수 있을 것으로 보인다.

키워드 : 가상자산, 가상자산 거래소, 가상자산 서비스, ISMS, CCSS

1. 서 론

비트코인이 도입된 이후[1], 가상자산은 물리적 공간의 제약 없이 다양한 방식의 거래가 가능하다는 점에서 기존 화폐를 대체 및 보완하는 지급 결제 수단으로서 활용되고 있다. 가상자산은 거래정보를 담은 장부를 블록체인 네트워크에 연결된 여러 참여자가 공동으로 기록 및 대조하여 거래 과정에서의 신뢰성과 투명성을 보장하고 블록체인의 분산처리와 암호화 기술을 통해 보안성을 확보한다는 특징이 있다. 가상자산의 핵심 기술이 되는 블록체인은 체인의 유기적 관계를 통해 신뢰성을 보장하고 중앙서버 없이 P2P 분산 서버를 통해 구동되기 때문에 안정성을 보장하며 해시 알고리즘을 통한 보안성을 보장한다. 블록체인의 강력한 보안성에도 불구하고 가상자산을 보관하는 월렛 보안 취약성, 프라이빗 키 유출, 가상자산 서비스 플랫폼 취약성 등과 같이 여러 가지 보안 취약성으로 인해 가상자산 도난 사례가 발생되었다[2].

가상자산은 월렛 소유주에 대한 익명성, 거래내용에 대한

† 준 회 원 : 성균관대학교 정보보안학과 석사과정
†† 정 회 원 : 성균관대학교 소프트웨어융합대학 초빙교수
††† 종신회원 : 성균관대학교 소프트웨어융합대학 교수
Manuscript Received : April 5, 2022
Accepted : April 22, 2022
* Corresponding Author : Koo Ja Hwan(jhkoo@skku.edu)

암호화 등으로 도난 또는 분실되는 경우 범인을 잡기가 어렵기 때문에 해킹의 표적이 되고 있다. 2012년부터 최소 46개의 암호화폐 거래소가 해킹당했으며, 약 27억 1천만 달러의 누적 금액이 도난당했다[3]. 한국의 경우 최근 5년간 가상자산거래소에서 발생한 해킹 사건은 9건이며, 경제적 피해 규모는 1,266억원(1억 달러) 이상이다[4]. 보고되지 않은 가상자산해킹과 다른 나라의 가상자산해킹을 종합하면 피해 규모는 훨씬 상회할 것으로 추정된다. 이에 해킹이 가상자산에 미치는 영향, 가상자산의 취약성 및 보안성을 강화하기 위한 연구가 진행되고 있다[5-8].

가상자산의 규제와 관련해서는 가상자산의 불분명한 법적 지위로 인하여 규제 기관, 가상자산정책, 기존 자산과의 관계, 이용자 보호, 자금 세탁 방지 등에 대하여 각국이 상이한 태도를 보이고 있다[9]. 가상자산을 수용하고 있는 각국의 정책 방향 및 규제는 다소 차이가 있으나 대체로 가상자산의 안전한 거래 보장을 위한 거래소 등록 및 거래의 투명성을 높이기 위한 가상자산 관련 과세 기준 제시 등에는 유사한 방향을 제시하고 있다.

안전한 가상자산 서비스를 위해 정보보호 인증제도를 취득하여 보안 현황을 확인하고 개선함으로써 보안성을 검증할 수 있다. 국제적으로 인증 가능한 제도는 암호화폐 보안표준인 CCSS가 있다. 한국에서는 가상자산거래소에 대한 ISMS 인증서 획득을 의무화하고, 가상자산거래소 인증 심사를 위한 56개 특화 체크리스트를 추가로 제정하여 보안성을 검증하고 있다.

본 논문에서는 국내 인증제도인 ISMS와 국외 암호화폐 보안표준인 CCSS의 항목에 대한 비교분석을 통해서 가상자산 서비스에 대한 ISMS의 현황을 상세히 파악한 후 도출된 비교 연구 결과를 토대로 중요도 평가를 수행하여 추가 또는 개선해야 할 ISMS 인증항목의 우선순위를 도출한 후 개선안을 제안한다. 개선한 항목을 통해 가상자산 거래소에 대한 신뢰성 및 안전성을 제고하여 가상자산 거래 활성화에 기여하기를 기대한다. 본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 관련 연구를 살펴보고, 3장에서는 ISMS와 CCSS 분석 및 비교한 후 4장에서 개선안을 도출하고 5장에서 결론을 내리고 본 논문의 끝을 맺는다.

2. 관련 연구

2.1 가상자산 서비스

1) 가상자산 서비스 보안위협

K. Grobys[5]는 해킹 이후 가상자산의 변동성이 증가하며 가상자산 시장의 불확실성에 영향을 미친다고 제언한다. 또한 대형 거래소에 비해 보안 기준이 미흡한 소규모 거래소에서 해킹 발생 가능성이 높으며 여러 가상자산을 거래하는 거래소가 해킹당할 경우 변동성에 대한 파급 가능성이 있다고 제언하며 가상자산 시장의 활성화를 위하여 보안성을 강화해야 한다는 것을 시사한다.

R. Zhang외[10]는 블록체인의 보안 및 개인정보보호 속성 및 보안 방안을 기술하고 있으며 N. Amiet[11]는 이더리움을 중심으로 스마트 계약과 관련된 취약점이 악용될 수 있는 방식 및 공격을 방지하기 위한 기술을 설명하며 철저한 코드 검토 또는 보안 감사를 수행할 것을 제안하고 A. Mense외[12]는 스마트 계약(Smart Contract)의 취약점 식별 및 감지 시 사용가능한 코드 분석 도구를 비교하며 이는 안전한 서비스 구현을 위해 취약성을 개선해야 한다는 것을 시사한다.

정용식 외[2]는 가상자산 거래 시 발생할 수 있는 보안 위협을 서비스 구현 과정 및 운영자 관리 과정 측면에서 분류하고 해결방안을 제시하고 L. Konig 외[6]는 블록체인 시스템의 취약성과 관련 있는 요소를 4개 도메인으로 구조화한 24가지 위험에 관해 설명하며 조직의 보안 측면 제어가 중요한 구성요소라고 제언한다. Y. Maleh[7]는 2011년 이후 블록체인 네트워크에서 발생한 사건의 위협 및 취약성 분류 결과를 제시하며 액세스 제어의 구현을 위해서는 향상된 암호화 기술, 맬웨어 및 기타 능동적인 위협 처리가 필요하다고 제언하며 J. H. Lee[8]는 블록체인 시스템의 보안성이 블록체인 기술에서 상속된 보안 기능에 의존하고 있으며 사고 대응 및 보안 개선방안이 충분하지 않다고 제언한다. 이는 보안 위협에 대한 가상자산 거래소의 대응 강화가 필요하다는 것을 시사한다.

H. Poston[13]는 Open Web Application Security Project(OWASP) 프레임워크를 블록체인에 매핑하여 블록체인 시스템의 잠재적 취약점을 식별하고, M. Al. Ketbi 외[14]는 기존의 프레임워크 기반의 블록체인 기술을 위한 정보보안 프레임워크를 제안한다. JJ. Bucko 외[15]는 가상자산의 신뢰에 미치는 요소를 식별한 후 가상자산 관련한 표준을 제정해야 한다고 제언한다. G. Bello외[16]는 트랜잭션 지원 블록체인 플랫폼에 대한 Payment Application Data Security Standard(PA-DSS) 적용 가능성을 비교한 결과 두 플랫폼 모두 PA-DSS 표준에 적합하지 않으며 블록체인 지불 시스템에서 데이터 보안을 보장하기 위해서는 새로운 표준을 개발해야 한다는 것을 제언한다. T. Hardjono 외[17]는 연구에서는 Internet Service Provider(ISP) 모델에 대응하는 Contract Service Provider(CSP) 모델에 대해 제안하며 V. Tumas 외[18]는 Virtual Asset Service Provider(VASP)에 대한 신뢰를 제공하고 규정 준수 부담을 줄이기 위해 혼합된 중앙 집중식 및 분산 접근 방식을 활용하여 Financial Action Task Force(FATF)의 권장사항을 준수할 수 있는 시스템을 제안한다. 해당 연구는 공통으로 가상자산 관련 보안 표준 제정이 필요하다는 것을 시사한다.

T. Hardjono외[19]는 VASP가 격리된 데이터에 직접 액세스하지 않고도 이러한 엔터티로부터 정보를 얻을 수 있는 개방형 알고리즘 접근방식을 제안하며 T. Hardjono외[20]는 VASP 및 가상 자산 전송 시 적용되는 공개키 인증서의 기존 표준을 검토하고 T. Hardjono[21]와 T. Hardjono[22]

는 개인 지갑의 최종 사용자가 개인키를 제어해야 한다고 제언하며 이를 위한 시스템 구현을 제안한다. G. Soana[23]는 탈중개화 기술을 보존하기 위하여 개인 중심의 금융 범죄 통제에서 거래 중심의 접근 방식으로 전환할 것을 제안한다.

위 논문들을 보면 가상자산의 안정성 및 보안 수준을 높이기 위하여 다양한 보안 위협 요소와 기술적 대응 방안에 대해 연구했다. 하지만 가상자산서비스 관련 조직의 정보보호 관리체계 측면에서의 정보보호 방안에 대한 연구는 매우 미흡하다. 이에 본 논문에서는 가상자산서비스에 대한 정보보호 방안을 CCSS 인증제도와의 비교를 통한 ISMS 인증항목 개선을 통해 도출한다.

2) 국내외 가상자산 서비스 운영 및 규제현황

2010년 세계 최초 가상자산거래소인 비트코인마켓닷컴(bitcoinmarket.com)을 통해 첫 번째 거래가 이루어진 이후 BTC China(중국), MT.Gox(일본), bitcoin.de(독일) 등 여러 거래소가 잇달아 등장하였으며 미국은 2011년 코인베이스가 개장하였고 한국은 2013년 코빗을 시작으로 2014년 빗썸, 코인원이 등장하였다.

현재 비트코인을 포함하여 7,000여 종의 가상자산이 발행되었으며, 다양한 가상자산을 교환할 수 있는 12,000여 개의 가상자산 거래소가 등장하였고 이들의 시가총액은 2022년 3월 현재, 2조 달러를 상회하고 있다[24]. 가상자산 중 가장 인기 있는 가상자산은 비트코인이며 시장 지배력이 43%에 달하고 시가총액은 1조 2천억 달러에 달한다. 다음으로 인기 있는 가상자산은 이더리움이며 시장 지배력 19%, 시가총액 5천억 달러이고 뒤를 이어 Binance Coin, Cardano, Solana가 각각 시장 지배력 3.6%, 2.5%, 2.4%이고 시가총액의 합이 2천 5백억에 달한다[25].

대규모의 거래소는 해킹에 대한 대형 표적이 되고 있어 2014년 전 세계 비트코인(BTC) 거래의 70% 이상을 차지한 마운트곡스(Mt.Gox)가 거래 가변성(transaction malleability)을 이용한 공격을 통해 4억 달러 이상의 피해로 파산하였고[26] 2018년 Coincheck가 인적오류로 인해 5억 달러 이상의 손해를 입었으며 2020년 KuCoin이 개인 키 유출을 통해 2억 8천만 달러의 손해를 입었다[27]. 2022년 3월 현재 거래소 순위 1위는 Binance로 일 거래량 150억 달러며 2위는 Coinbase로 일 거래량 38억 달러고 이후 FTX, Kraken, Kucoin가 뒤를 잇는다[28].

주요국의 가상통화에 대한 규제는 크게 가상통화거래소 등 가상통화업자에 대한 규제, 자금 세탁 및 테러 자금 조달 방지를 위한 규제, 조세회피를 방지하기 위한 규제로 크게 구분할 수 있다. 미국 뉴욕주는 BitLicense 가상자산 규정을 통해, 일본은 관련법을 제정하여 가상통화업자를 직접적으로 규율하고 있으며 중국은 가상통화의 유통과 거래를 전면적으로 금지하고 있다. 영국은 가상통화를 교환의 매개체로써 인정하고 가상통화와 관련된 과세를 완화하여 우호적인 환경을 조성한다[29]. 그러나 미국의 BitLicense 외에 해킹사고에 대비한 정보보안에 대한 규제는 미흡하며 BitLicense 또한 세부 평가 기준이 없어 실효성이 부족한 상황이다.

2.2 ISMS 인증제도

1) ISMS 개요

한국 정부는 2001년 정보통신사업자를 대상으로 정보보호 관리체계를 구축·운영하는데 활용할 수 있도록 국제표준 정보보안 경영시스템인 ISO27001을 기반으로 국내 실정을 반영하여 한국 내 기업 및 기관 등 조직에서 주요 정보자산을 보호하기 위해 수립, 관리, 운영하는 정보보호 관리체계가 인증기준에 적합한지 심사하여 인증을 부여하는 제도인 Information Security Management System (ISMS)를 도입하였다[30].

2013년부터 이동통신사, 인터넷서비스사업자 등 정보통신서비스 사업자 중에서 전년도 매출액 100억 원 이상 또는 전년도 말 기준 3개월간의 일일 평균 이용자 수가 100만 명 이상인 곳이 ISMS 인증제도 의무인증 대상자로 지정되면서 ISMS 인증제도가 확산되었다. 2016년 ISMS 심사 의무대상이 의료·교육 분야로 확대되면서 연간 매출액 또는 세입이 1,500억 이상인 상급 종합병원, 고등교육법상 재학생 수 1만 명 이상인 학교가 ISMS 인증 의무대상에 포함되었고, 2021년 가상자산 투자자와 거래대금이 크게 증가함에 따라 가상자산을 매도·매수·교환 및 이를 중개하는 행위, 이전 행위, 보관·관리 행위 등을 하는 가상자산 사업자가 ISMS 인증 의무대상에 포함되었다[31].

2) ISMS 인증항목

한국인터넷진흥원은 2001년 ISMS 제정 이후 2013년 개정안을 고시하였다. Personal Information Management System(PIMS, 개인정보보호 관리체계) 인증제도는 2010년 ISMS 인증제도와 별도로 개인정보보호 관리체계 인증을 위해 제정되었다. 2018년 PIMS 인증제도를 폐지하고 개인정보보호와 정보보호관리체계를 통합하여 ISMS-P(정보보호 및 개인정보보호) 인증제도를 제정하였다. (구) ISMS와 PIMS 인증제도의 유사 항목을 통합하여 Table 1과 같이 ISMS 80개 항목을 제정하였으며, 개인정보 특화 22개 항목을 추가하여 ISMS-P 인증 기준 총 102개 항목으로 제정하였다. 인증 대상자는 ISMS 또는 ISMS-P 인증 중 하나를 선택할 수 있다.

또한 한국인터넷진흥원은 가상자산 거래소 인증 시 적용할 관리체계 수립 및 운영 항목 11개, 보호대책 요구사항 45개 총 56개의 확인사항을 추가하였다. 가상자산 거래소는 ISMS 인증 시 80개 항목에 대한 234개 주요 확인사항에 가상자산 거래소 특화 확인사항 56개를 추가하여 총 290개 확인사항으로 점검하여야 한다[32].

본 논문에서는 가상자산거래소의 보안성을 강화하기 위하여 선택적 항목인 개인정보보호를 제외하고 ISMS-P 중 ISMS에 속하는 290개의 확인사항을 포함하는 80개의 인증항목을 연구범위로 설정한다.

Table 1. ISMS-P Certification Components

Certification		Part	Domain(Number of Components)
ISMS-P	ISMS	1. Establishment and Operation of Management System (16)	1.1 Establishment of Management System Foundation(6) 1.2 Risk Management(4) 1.3 Management System Operation(3) 1.4 Management System Inspection and Improvement(3)
		2. Protection Requirements (64)	2.1 Policy, Organization, and Asset Management(3) 2.2 Human Security(6) 2.3 Outsider Security(4) 2.4 Physical Security(7) 2.5 Authentication and Rights Management(6) 2.6 Access Control(7) 2.7 Encryption Enforcement(2) 2.8 Information System Introduction and Development Security(6) 2.9 System and Service Operation Management(7) 2.10 System and Service Security Management(9) 2.11 Accident Prevention and Response(5) 2.12 Disaster Recovery(2)
	-	3. Requirements for each Stage of Personal Information Processing (22)	3.1 Protection Measures when Collecting Personal Information(7) 3.2 Protection Measures for Retention and Use of Personal Information(5) 3.3 Protection Measures when Providing Personal Information(3) 3.4 Protection Measures when Personal Information is Destroyed(4) 3.5 Protection of Data Subject Rights(3)

2.3 CCSS 인증제도

1) CCSS 개요

CCSS 인증제도는 CryptoCurrency Certification Consortium(C4)에서 2015년 제정한 암호 화폐를 사용하는 모든 정보 시스템을 보호하는 데 도움이 되는 보안 표준이다[33]. C4는 Certified Bitcoin Professional(CBP) 자격증과 CCSS 인증제도를 게시 및 심사하는 비영리 조직이다. CCSS의 추진 배경은 거래소, 웹 애플리케이션 및 암호자산 저장 솔루션을 포함한 정보 시스템에 대한 요구사항 및 방법론을 표준화함으로써 ISO27001과 같은 기존의 정보보호 표준을 보완하도록 설계되었다.

가상자산거래소는 보안 원칙 준수를 입증하고 안전한 서비스를 제공하기 위하여 인증을 취득하고 있으나 의무는 지지 않는다. C4는 표준 정보 보안 관행을 강화할 목적으로 2015년 2월 표준을 공개하여 별도의 조건 없이 사용할 수 있게 함으로써 기관별로 수행하던 보안 활동이 표준화되면서 비용, 시간 등의 절감이 가능하게 되었다. 또한 인증제도 및 항목에 대한 의견을 수렴하여 지속적으로 업데이트 및 개선하고 있다.

2) CCSS 인증항목

CCSS 인증 도메인은 암호화 자산 관리(Cryptographic Asset Management)와 운영(Operations) 크게 두 부분으로 나뉜다. 암호화 자산 관리는 정보시스템의 키/지갑 생성, 저장, 사용, 삭제에 대한 6가지 분야로 구성되며 운영은 감사, 지급준비금과 같이 데이터 및 정보시스템의 기밀성과 무결성을 위한 4가지 분야로 구성된다. 정보시스템은 서비스를 제공하기 위해 작용하는 환경으로 하드웨어 및 소프트웨어, 인력, 정책 및 절차를 모두 포함한다.

각 항목은 3가지 레벨로 구성되어 있으며 레벨1은 상대적으로 가장 보안성이 낮고 레벨3은 보안성이 높고 포괄적이다. 레벨 1을 달성하기 위해서는 전체 37개의 항목 중 레벨1에 해당하는 23개의 항목을 필수적으로 충족해야 한다. 레벨2의 경우 30개, 레벨3의 경우 37개 필수 충족항목이 있으며 레벨별 기준이 차등한 때도 있다. 예를 들어 '1.3.6 Backup Key is Encrypted'의 경우 백업키가 강력한 암호화되는 경우 레벨3을 충족하고 레벨1과 레벨2의 경우 해당 내용이 없어 CCSS 인증을 위한 필수적인 항목은 아니게 된다. 또한 '2.1.1 Security Audit'은 비트코인 보안에 대해 잘 알고 있는 개발자가 시스템 설계 및 개발을 수행하였을 때 레벨1이고 제3자가 보안감사를 완료하였을 때 레벨2이며 외부 보안감사를 최소 연 1회 수행하는 경우 레벨3을 충족한다. 인증심사 결과 각 항목 최솟값의 평균을 통해 정보시스템의 전체 레벨이 결정된다.

2015년 최초 릴리즈 당시 10개 분야 34개 항목으로 구성되었으나, 2021년 7월 10개 분야 37개 항목으로 변경되었다. 모든 트랜잭션에 고유 지갑/주소 생성하는 '1.2.1 Unique Wallet per Transaction'과 키/시드 백업이 EMP (Electro- Magnetic Pulse)에 내성이 있도록 요구하는 '1.3.7 Backup Key is Protected from EMP' 2개 항목이 삭제되었다. 또한 엔트로피 풀을 확인하는 '1.1.4 Entropy Pool'과 지갑 생성, 키 저장 및 사용 관련 절차 수립에 관한 '1.2.6 Documented Wallet Creation Policy', '1.3.7 Documented Key Storage Policy', '1.4.9 Documented Key Storage Policy'과 모든 승인/취소가 안전한 통신채널을 통해 수행되도록 하는 '1.6.2 Requests made VIA Authenticated Communication

Channel' 총 5개 항목이 추가되었다.

본 논문에서는 CCSS의 보안 요구사항을 반영하기 위해 최신 항목 레벨3을 기준으로 연구범위를 설정한다.

3. ISMS와 CCSS 비교 분석

3.1 ISMS와 CCSS 도메인 중요도 비교

ISMS와 CCSS에서 중점적으로 확인하는 도메인에 따라 인증항목이 많이 분포되어 있다고 판단할 수 있다. 인증제도마다 바라보는 시각이 다르기 때문이다. 인증제도별 중점적으로 확인하는 도메인을 도출하기 위하여 전체 인증항목에서의 도메인별 인증항목 비율을 확인하였다.

Fig. 1A를 보면 가상자산사업자를 위해 추가된 특화항목 중에서 인증항목 비율이 가장 높은 도메인은 접근통제(14%), 시스템 및 서비스 운영관리(14%) 항목이며 다음으로 비율이 높은 도메인으로 정보시스템 도입 및 개발 보안(13%)으로 나타났다. 가장 낮은 비율의 도메인은 관리체계 운영(0%), 재해복구(0%)로 나타났다. ISMS는 가상자산사업자 인증 시 시스템의 접근제어에 대한 보안과 백업 및 복구 등 시스템 및 서비스 가용성과 데이터의 무결성을 중점적으로 확인한다는 것을 알 수 있다.

Fig. 1B를 보면 CCSS 도메인 중 인증항목 수가 가장 많은 도메인은 키 사용법(24%) 항목이며 다음으로 키 저장소(19%), 지갑 생성(16%) 항목의 비율이 높은 것으로 나타났다. 가장 낮은 비율의 도메인은 보안감사/침투(3%) 및 예약증명(3%) 항목으로 나타났다. CCSS 인증제도에서 키/시드 및 지갑의 기밀성과 무결성을 가장 중점적으로 확인한다는 것을 알 수 있다.

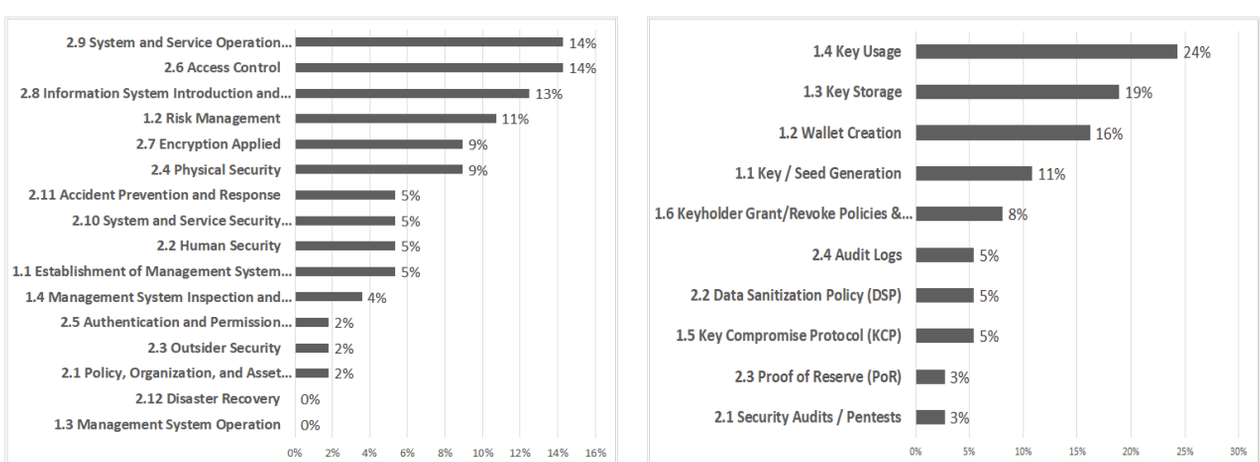
각 인증제도의 항목 비율을 확인한 결과 ISMS는 가상자산사업자의 정보통신서비스 시스템 접근제어에 대해 상세하게 확인하여 내외부에서 발생할 수 있는 권한 없는 사용자의 접근 시도 및 공격을 차단하는 것과 백업 및 로그 정책을 수립 및 검토하여 시스템 운영상태를 최적화하고 시스템 오남용을 방지하는 것에 중점을 두고 있다. 한편, CCSS 인증제도는 암호자산을 위한 보안인증이기 때문에 키/시드/지갑의 생성 및 사용과 저장 시 발생할 수 있는 보안 문제에 중점을 두고 있다는 것을 확인할 수 있다.

3.2 ISMS와 CCSS 인증항목 상호매핑

ISMS 인증항목 80개를 기준으로 CCSS Level 3 35개 인증항목과 점검 내용 및 방법이 유사한 항목을 매핑하여 도메인별로 비율을 도출하였으며 Sankey Diagram을 통해 각 도메인에 연결된 선 두께를 통해 상대적인 양의 비례 결과를 표기한 결과 Fig. 2와 같다. ISMS 인증 24개 항목이 CCSS 27개 항목에 각각 일대일 또는 다중매핑되었다.

CCSS 인증항목에 매핑되는 ISMS의 24개 항목 중 19개 항목은 1:1 매핑되며 5개 항목은 CCSS 인증항목에 다중매핑된다. 가장 많이 다중매핑되는 항목은 '2.7.2 암호키 관리'로 CCSS 인증항목 11개에 매핑되며 다음으로 '2.9.4 로그 및 접속기록 관리'가 4개, '1.1.5 정책 수립'과 ''2.7.1 암호정책 적용'이 각각 3개 '2.9.7 정보자산의 재사용 및 폐기'가 2개로 다중매핑된다. CCSS는 정보시스템 및 정보관리체계의 전반적인 부분보다 암호키 및 데이터의 무결성과 관련한 기능적 요구사항에 대해서 중점적으로 확인하는 것을 알 수 있다.

ISMS에 매핑되는 CCSS 27개 항목 중 17개 항목이 1:1 매핑되며 10개 항목이 다중매핑된다. 다중매핑되는 항목으로는 '1.6.1 Grant/Revoke Procedures/Checklist'와 '2.1.1 Security Audit' 항목이 ISMS 항목 4개에 각각 다중매핑되며, '2.4.1 Application Audit Logs'가 3개 '1.4.9 Documented key storage policy'을 포함한 7개 항목이 각각 2개씩 다중매핑된다. ISMS 인증제도는 정보시스템의 도입 및 데이터 생성, 권한 부여, 사용, 파기에 이르는 전체적인 부분에서의 정보보안을 위한 절차에 대해 중점적으로 확인하



(A) (B)

Fig. 1. Components Ratio by Domain; (A) Virtual Asset Business Checklist Ratio by ISMS, (B) Components Ratio by CCSS

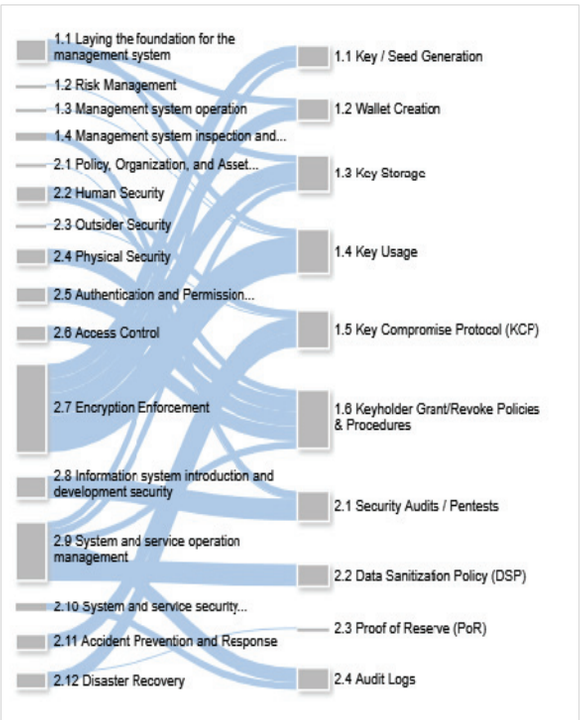


Fig. 2. Results of ISMS and CCSS Components Mapping

며 가상자산에 특화된 지급준비금 확인 및 키/시드 생성에 대한 기술적 요구사항에 대한 부분이 다수 미적용 되었음을 확인할 수 있다.

3.3 ISMS와 CCSS 인증항목 차이

ISMS와 CCSS의 인증항목을 상호매핑하여 다중매핑되는 항목에 대한 가중치를 부여하지 않고 각 인증제도의 도메인별 매핑율을 통해 유사도를 도출한 결과 Fig. 3과 같다. 관리적, 기술적, 물리적으로 다방면의 정보보호 관리체계를 점검하는 ISMS의 경우 암호화 적용 및 복구와 관련한 기술적 항목의 매핑율이 높고 관리체계 수립 및 운영에 관련한 항목이 매핑율이 낮은 것을 볼 수 있다. 암호화 프로세스의 기술적 요소를 중점적으로 점검하는 CCSS의 경우 데이터 복구 및 감사와 관련한 항목의 매핑율이 높고 지급준비금과 키/지갑 생성 및 사용에 관련한 항목의 매핑율이 낮은 것을 볼 수 있다.

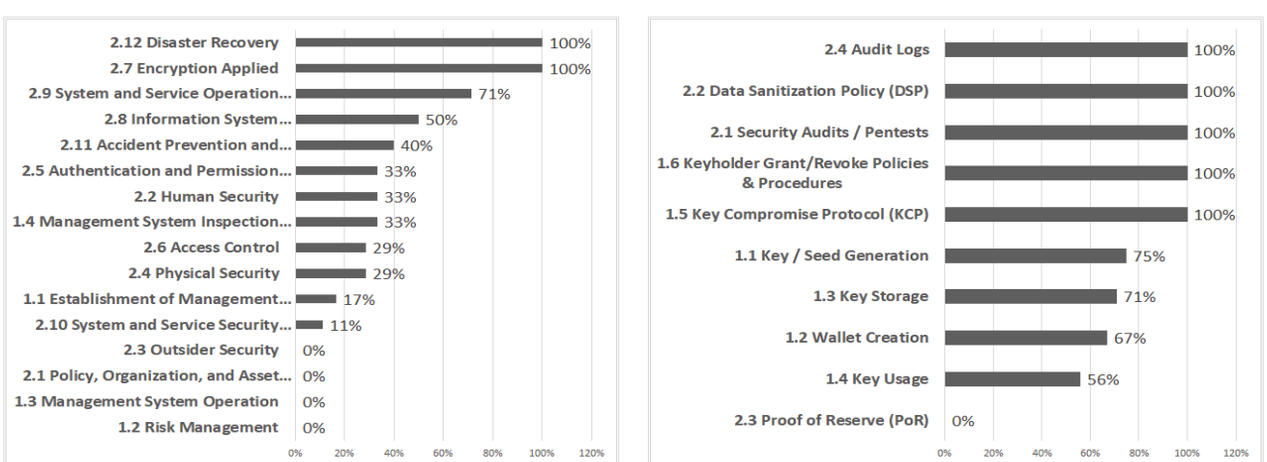
도메인별 매핑율이 가장 높은 도메인은 '2.7 암호화 적용(100%)'과 '2.12 재해복구(100%) 이고 다음으로 '2.9 시스템 및 서비스 운영관리(71%)'이다. '1.2 위험 관리'를 포함한 4개의 도메인이 매핑율 0%로 가장 낮은 매핑율을 보이며 정보보호 관리체계 전반적인 부분이 CCSS에 반영되어 있지 않았다.

CCSS 도메인별 매핑율이 가장 높은 도메인은 '1.5 Key Compromise Protocol (KCP)' 를 포함하여 키 및 데이터의 안전한 삭제 및 복구, 로그 및 감사를 통한 데이터 무결성과 관련한 도메인 총 5개로 100% 매핑율을 보이며, 매핑율이 가장 낮은 도메인은 '2.3 Proof of Reserve (PoR)'이다.

4. ISMS 인증항목 개선안

4.1 ISMS 개선항목 도출

ISMS에 미적용된 CCSS 항목의 적용 우선순위를 도출하기 위하여 중요도를 산정하였다. 중요도 산정 방식은 Al Ketbi, M외(2021) 블록체인 프레임워크 위험평가 방식과 유사하게[14] ISO 31000:2018 위험관리를 기반으로 위험 분석 및 위험평가 방식을 사용하되[34] 중요도 평가 요소를 정보보안 부분에서 중요시되고 있는 영향도 및 위험도와 CCSS에서 중요시되는 가중치로 구성하고 각 요소의 합으로 중요도 등급을 부여하였다. 영향도는 위협의 강도가 업무에 미치는 영향의 정도로써 취약점을 이용한 위협의 강도가 개인 프라이버시나 조직의 사업 진행에 치명적인 피해를 줄 수 있는 수준에 따른 것이다. 위험도는 취약점을 이용한 잠재위험이 실현될 가능성의 정도이며 CCSS 가중치는 CCSS 내 각 항목의 중요성으로 Level 1과 같이 CCSS 인증을 위한 필수적 항



(A) (B)

Fig. 3. Mapping Rate by Domain: (A) Mapping Rate by ISMS Domain, (B) Mapping Rate by CCSS DomainISMS

목일 경우 High(H), CCSS 인증을 위한 선택적 항목이며 Level 2, 3에 해당하는 경우 각각 Medium(M)과 Low(L)를 부여하였다. Table 2와 같이 평가 정도에 따라 각 요소별 1~3점을 부여하며, 각 요소의 합으로 구한 최종 중요도 값의 범위에 따른 중요도 등급을 부여한다.

CCSS 37개 항목 중 ISMS 항목에 기적용된 항목을 제외한 미매핑된 10개 항목에 대한 중요도 평가 결과는 Table 3과 같다. 4개 항목이 중요도 평가 결과 High, 4개 항목이 Medium, 2개 항목이 Low로 도출되었다. 보안 요구사항 평가 점수가 가장 높은 항목은 '1.1.1 Operator-created Key/Seed'로 키/시드의 경우 특정 관리자만 접근해야 하며 다른 행위자를 통해 발급되어 변조될 경우 조직의 사업 진행에 치명적 피해를 미칠 수 있으므로 9점이다. 다음으로 점수가 높은 항목은 8점으로 '1.4.3 Operator reference checks', '1.4.4 Operator ID checks' 및 '2.3.1 Proof of Reserve Audits'이다. 앞선 두 항목의 경우 키/시드 홀더에 대한 내부자 평판 조회 및 신원 검증 미수행 시 악의적인 권한자를 통한 자금 손실의 위험이 있으며 마지막 항목의 경우 지급준비금에 대한 감사를 수행하지 않아 자금에 액세스할 수 있음을 증명할 수 없는 경우 자금 무결성을 보증할 수 없다. 세 항목 모두 잠재위험의 실현 가능성이 높으며 조직의 사업 진행에 상당한 피해를 줄수 있다.

중요도 Medium인 4가지 항목 중 점수가 가장 높은 '1.2.3 Deterministic wallets'은 비결정적 지갑 방식 사용 시 지갑 손실에 대한 복구 불가능에 대한 대안으로 결정론적 발생으로 지갑을 생성하도록 요구하고 있으며 지갑 무결성을 보증한다. '1.4.6 Spends are verified before signing' 또한 7점으로 키 사용 전 자금의 목적지 및 금액 확인을 통해 자금 무결성을 보증한다. 두 항목 모두 자갑 및 자금 무결성에 관한 잠재위험의 실현 가능성이 높으며 실현되는 경우 조직의 사업 진행에 상당한 피해를 줄수 있다. 각각 5점인 '1.3.5 Backup key has tamperevident seal' 및 '1.3.6 Backup key is encrypted'는 백업키의 무결성과 기밀성을 보증한다. 백업키 관련 취약점을 이용한 잠재위험의 실현가능성이 있으며 백업키가 변조되는 경우 영향이 내부적이고 제한적이나 유출되는 경우 조직의 사업 진행에 상당항 필해를 줄 수 있다.

마지막으로 중요도 Low인 '1.2.5 Organizational distribution of keys'는 별도 법인에 키를 저장함으로써 법적 위험이 자금을 방해할 수 없도록 지갑 가용성을 보증하며 '1.4.5 Operator background checks'은 개인을 포함한 키 및 시드 홀더에 대한 신원확인을 통해 악의적인 권한자로부터 자금 무결성을 보증한다. 두 항목 모두 위협의 강도가 조직의 사업 진행에 상당한 피해를 줄 수 있으나 실현 가능성

Table 2. Component Materiality Rating Factors and Ratings

Classification	Influence	L(1)			M(2)			H(3)		
	Risk	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
CCSS weights	L(1)	3	4	5	4	5	6	5	6	7
	M(2)	4	5	6	5	6	7	6	7	8
	H(3)	5	6	7	6	7	8	7	8	9

Importance Class	Score
High	8~9
Medium	5~7
Low	3~4

Table 3. Importance Evaluation Result of Nonapplied Components

Component	Influence	Risk	CCSS weights	Importance Class
1.1.1 Operator-created Key/Seed	H	H	H	H
1.2.3 Deterministic wallets	M	H	M	M
1.2.5 Organizational distribution of keys	M	L	L	L
1.3.5 Backup key has tamper-evident seal	L	M	M	M
1.3.6 Backup key is encrypted	M	M	L	M
1.4.3 Operator reference checks	M	H	H	H
1.4.4 Operator ID checks	M	H	H	H
1.4.5 Operator background checks	M	L	L	L
1.4.6 Spends are verified before signing	M	H	M	M
2.3.1 Proof of Reserve Audits	M	H	H	H

Table 4. ISMS Improvement Components

Domain	Component	Checklist (new)	CCSS Component
2.2. Human Security	2.2.1 Designation and Management of Key Personnel	In the case of key/seed operators related to virtual assets, are you checking references for identity verification, such as whether you have not been fired from your previous employment for reasons that may pose a risk to the organization?	1.4.3
2.7 Encryption applied	2.7.1 Password Policy Application	For secure Keys/seeds generation, is it generated by the key/seed operator itself, not by another actor, when generating Keys/Seeds?	1.1.1
2.10 System and Service Security Management	2.10.4 Electronic Transactions and Fintech Security	In order to prevent loss of funds through malicious authorities, are key and seed holders identified based on their real name through I-PIN authentication and mobile phone authentication?	1.4.4
2.10 System and Service Security Management	2.10.4 Electronic Transactions and Fintech Security	Are Proof of Reserves for all funds held by the information system signed by an independent party certifying the accuracy of the audit?	2.3.1

이 미흡하다. 본 논문에서는 중요도가 High인 4가지 항목을 우선으로 개선안을 도출한다.

4.2 ISMS 인증항목 개선안

CCSS 인증항목 중 중요도가 H등급에 해당하는 ISMS 미적용 항목을 기준으로 ISMS 인증항목 개선사항을 도출한 결과 Table 4와 같다.

개선안에서는 가상자산과 관련한 데이터 기밀성과 가상자산 자금에 대한 통제를 위한 주요 확인사항을 추가하여 기존 확인사항을 통해 확인할 수 없었던 부분을 보완하였다. 가상자산과 관련한 데이터의 기밀성 보장을 위해 확인할 사항으로 주요 권한자에 대한 신원 검증과 안전한 키/시드 생성을 위한 연산자 자체 생성 보장하여 보안성 입증에 도움을 줄 수 있도록 하였다. 또한 지급준비금에 대한 감사를 수행하고 결과에 대한 독립당사자의 서명을 통해 감사의 정확성을 증명하고 있는지를 확인하여 가상자산 자금에 대한 통제 및 자금에 대한 무결성을 보증할 수 있도록 하였다.

5. 결 론

최근 비트코인을 포함한 가상자산에 대한 인식이 확산되면서 가상자산 이용 및 투자가 활발해지고 있으며 가상자산거래소에 대한 보안사고 또한 빈번하게 발생하고 있다. 주요국은 기존 제도와 정책 목표에 따라 가상자산 관련 시장에 다양하게 접근하고 있으나 정보보안에 대한 규제는 미흡하며 실질적인 실효성이 부족하다. 한국에서는 가상자산사업자에 대한 ISMS 인증 의무화 및 가상자산사업자를 위한 특화 확인사항을 추가로 제정하였으나 가상자산 보안에 대한 신뢰성을 보장하기엔 부족함이 있다.

본 논문에서는 ISMS와 CCSS 인증항목을 정성적으로 비교분석한 후 중요도 평가를 수행하여 적용 우선순위를 도출하였으며 우선순위가 높은 4가지 항목을 ISMS 인증항목 개선안으로 제안하였다. 비교분석 결과 ISMS는 정보보호관리체계 전반에 대한 절차를 중점적으로 확인하며 CCSS의 경우 키/시드/지갑 생성 및 사용, 저장에 대한 기술적 요구사항을 중점적으로 확인하는 것을 알 수 있었으며 특성이 다른 두 인증제도의 비교를 통해 ISMS의 개선방향을 확인할 수 있었다. 또한 ISMS에 미적용된 CCSS 인증 10가지 항목의 평가기준을 계층화하고 계층에 따른 중요도 분석을 통해 우선 적용할 항목 4가지를 도출하였으며 결과적으로 ISMS 항목의 추가 확인사항을 제안하였다. 개선안을 통해 가상자산과 관련한 데이터의 기밀성과 자금 무결성을 추가로 보장할 수 있도록 하였다.

본 연구는 정성적 비교분석만으로 개선 사항에 대해 도출하였지만 향후 연구에서는 이해당사자 또는 전문가들의 견해가 반영될 수 있는 의사 결정 방법론 등을 통한 다차원적인 분석이 필요하다. 또한 구현 가능성 및 경제적 효율성 등 추가적인 우선순위 판단 지표를 통한 결과의 신뢰성을 보완할 수 있을 것이다. 마지막으로 가상자산의 정보보안을 보장할 수 있는 다른 인증제도에 관한 추가적인 연구가 필요하다.

4차 산업혁명의 시대에 있어서 가상화폐는 국내 금융 산업에 적지 않은 영향을 주고 있으며 경제적인 가치가 인정되고 있는 상황에서 데이터 및 자금의 무결성, 서비스의 가용성 등을 정보보안의 세밀한 규제를 통해 보증하여 가상자산 거래의 안전성 및 신뢰성을 확보한다면 전 세계 금융시장에 긍정적인 영향을 줄 것으로 기대해본다.

References

[1] S. Nakamoto, “A peer-to-peer electronic cash system,” *Decentralized Business Review*, pp.21260, 2008.

[2] Y. S. Chung and J. S. Cha, "The security risk and countermeasures of blockchain based virtual currency trading," *The Journal of Korea Institute of Information, Electronics, and Communication Technology,* Vol.11, No.1, pp.100-106, 2018.

[3] Hedgewithcrypto, Cryptocurrency Exchange Hacks (Updated 2022 List) [Internet], https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/.

[4] Strategy and Finance Committee, "Analysis of government audit issues," *National Policy Committee,* Vol.4, 2020.

[5] K. Grobys, "When the blockchain does not block: On hackings and uncertainty in the cryptocurrency market," *Quantitative Finance,* Vol.21, Iss.8, pp.1267-1279, 2021.

[6] L. König, S. Unger, P. Kieseberg, and S. Tjoa, "The risks of the blockchain a review on current vulnerabilities and attacks," *Journal of Internet Services and Information Security*, Vol.10, Iss.3, pp.110-127, 2020.

[7] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, "Blockchain for cybersecurity and privacy: Architectures, challenges, and applications," Eds., *CRC Press,* 2020.

[8] J. H. Lee, "Systematic approach to analyzing security and vulnerabilities of blockchain systems," *Massachusetts Institute of Technology,* Diss, 2019.

[9] B. Y. Kim, "Positions and responses of major countries on cryptocurrency," in *Capital Market Focus*, Korea Capital Market Institute, Vol.25, 2017.

[10] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR),* Vol.52, Iss.3, pp.1-34, 2019.

[11] N. Amiet, "Blockchain vulnerabilities in practice," *Digital Threats: Research and Practice,* Vol.2, Iss.2, pp.1-7, 2021.

[12] A. Mense and M. Flatscher, "Security vulnerabilities in ethereum smart contracts," *Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services*, pp.375-380, 2018.

[13] H. Poston, "Mapping the OWASP top ten to blockchain," *Procedia Computer Science*, Vol.177, pp.613-617, 2020.

[14] M. Al. Ketbi, K. Shuaib, E. Barka, and M. Gergely, "Establishing a security control framework for blockchain technology," *Interdisciplinary Journal of Information, Knowledge, and Management,* Vol.16, pp.307, 2021.

[15] J. Bucko, D. Palová, and M. Vejacka, "Security and trust in cryptocurrencies," *Central European Conference in Finance and Economics*, pp.14-24, 2015.

[16] G. Bello and A. J. Perez, "Adapting financial technology standards to blockchain platforms," *Proceedings of the 2019 ACM Southeast Conference*, pp.109-116, 2019.

[17] T. Hardjono, A. Lipton, and A. Pentland, "A contract service provider model for virtual assets," *The Journal of FinTech,* Vol.1, No.2, Iss.2150004, 2022.

[18] V. Tumas, R. Norvill, D. Magoni, and R. State, "VaVite: Verifiable information exchange for virtual asset service providers," *2020 Principles, Systems and Applications of IP Telecommunications (IPTComm),* pp.1-8, 2020.

[19] T. Hardjono, A. Lipton, and A. Pentland, "Privacy-preserving claims exchange networks for virtual asset service providers," *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp.1-8, 2020.

[20] T. Hardjono, A. Lipton, and A. Pentland, "Toward a public-key management framework for virtual assets and virtual asset service providers," *The Journal of FinTech,* Vol.1, No.1, Iss.2050001, 2021.

[21] T. Hardjono, "Future directions for regulated private wallets and VASP trust infrastructures," *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* pp.1-3, 2021.

[22] T. Hardjono, "Attestation infrastructures for private wallets," *arXiv preprint arXiv:2102.12473*, 2021.

[23] G. Soana, "Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?," *Economic Notes*, Vol.51, No.1, 2022.

[24] CoinMarketCap, All Cryptocurrencies [Internet], https://coinmarketcap.com/all/views/all/.

[25] CoinMarketCap, Bitcoin [Internet], https://coinmarketcap.com/currencies/bitcoin/.

[26] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and MtGox," In *European Symposium on Research in Computer Security*, Springer, Cham, pp.313-326, 2014.

[27] Y. Tsuchiya and N. Hiramoto, "How cryptocurrency is laundered: Case study of Coincheck hacking incident," *Forensic Science International: Reports,* Vol.4, Iss.100241, 2021.

[28] CoinMarketCap, Top Cryptocurrency Spot Exchanges [Internet], https://coinmarketcap.com/rankings/exchanges/

[29] I. S. Choi, "A study on the regulation of risks associated with the use of virtual currencies," Ph.D. dissertation, Yonsei University Law School, Seoul, Republic of Korea, 2019.

[30] Korea Internet & Security Agency, Introduction of the certification system [Internet], https://isms.kisa.or.kr/main/isms/intro/.

[31] Korea Ministry of Government Legislation, Act on Promotion of Information and Communications Network Utilization and Information Protection, [Internet], https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%

ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0/(20211209,18201,20210608)/%EC%A0%9C47%EC%A1%B0.

[32] Korea Internet & Security Agency, Announcement of detailed inspection items for ISMS for virtual asset business [Internet], https://isms.kisa.or.kr/main/ispims/notice/?boardId=bbs_0000000000000014&mode=view&cntId=12.

[33] CryptoCurrencyCertificationConsortium, Crpto Currency Security Standard [Internet], https://cryptoconsortium.github.io/CCSS/.

[34] ISO, ISO 31000:2018(en) Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

김 은 지

https://orcid.org/0000-0001-8203-3110
e-mail : eunjikim@g.skku.edu
2018년 경일대학교 컴퓨터공학과(학사)
2020년 ~ 현 재 성균관대학교 정보보안학과 석사과정
관심분야 : 정보보호, 시스템 보안, 침해사고 대응

구 자 환

https://orcid.org/0000-0002-2844-3183
e-mail : jhkoo@skku.edu
1995년 성균관대학교 정보공학과(학사)
1997년 성균관대학교 전기전자컴퓨터공학과 (석사)
1999년 ~ 2002년 LG CNS 연구원
2006년 성균관대학교 전기전자컴퓨터공학과(박사)
2007년 ~ 2010년 미국 위스콘신대학교 컴퓨터과학과 박사후 연구원
현 재 성균관대학교 소프트웨어융합대학 초빙교수
관심분야 : Data Communication, Computer Network, Big Data, Machine Learning, Data Security

김 응 모

https://orcid.org/0000-0001-5464-6358
e-mail : ukim@skku.edu
1981년 성균관대학교 수학과(학사)
1986년 미국 Old Dominion 대학교 컴퓨터과학과(석사)
1990년 미국 Northwestern 대학교 컴퓨터과학과(박사)
1990년 ~ 현 재 성균관대학교 소프트웨어융합대학 교수
관심분야 : Database, Data Mining, Big Data, Data Security