정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

정보보호 거버넌스와 블록체인 거버넌스 국제표준 주요 내용과 구현 이슈

김 정 덕*

요 약

조직 또는 기술경영에 대한 주요 의사결정(Directing)과 통제활동(Controlling)을 의미하는 거버넌스에 대한 중요성이 점차 부각되면서 조직에서의 정보기술 또는 정보보호 활동에 대한 거버넌스 표준과 블록체인 또는 인공지능 등 혁신적 디지털 기술에 대한 거버넌스 표준들이 속속 발표되고 있다. 본 고에서는 ISO/IEC JTC 1 SC 27에서 작업한 정보보호 거버넌스 지침(ISO 27014, 2nd 버전, 2020.12)과 ISO/TC 307에서 작업한 블록체인 거버넌스 지침(TS 23635, 2022,02)에 대한 주요 내용과 함께 국내에서 두 가지 거버넌스 체계를 구현하기 위한 과정에서 발견할 수 있는 이슈와 이를 해결하기 위한 과제를 제시하고자 한다.

Ⅰ. 서 론

컴퓨터가 상용화되기 시작한 1950년대 이후, 기술적, 관리적 정보보호 대책 구현 노력이 있었지만, 2000년대에 진입하면서 인식하기 시작한 중요한 변화 중 하나는 이사회나 최고 경영층의 정보보호에 대한 지원과 참여가 없으면 조직내 보안관리는 성공할 수 없다는 점이다. 즉, 정보보호의 새로운 패러다임으로서 최고 경영층의 역할과 책임을 중요시 하는 “정보보호 거버넌스” 체계 구축이 요구되고 있다[1]. 더욱이 2010년 이후 인공지능, 블록체인 등 혁신적 기술의 사용이 비즈니스 모델로서 등장함에 따라 이에 대한 의사결정 권한 및 과정과 통제 활동 등 거버넌스에 대한 요구가 점증하고 있다[2].

블록체인 기술이 조직내 내재화되고 있는 기업형 블록체인 시스템/서비스가 도입됨에 따라 이에 대한 거버넌스의 필요성도 높아지고 있다. 즉 블록체인 서비스를 구현하기 위한 공동체를 이루는 구성원들이 의사결정에 참여하여 주요 사항을 집단으로 결정하는 구조와 절차를 의미한다. 거버넌스는 규칙(스마트 컨트랙트), 법(악성 행위자들에 대한 벌금), 절차(X가 일어났을 때 어떤 일이 행해질지), 또는 책임 (누가 무엇을 해야 하는가에 관한 것)과 같은 요소로 구성되어 있다. 블록체인 시스템의 구축 및 운영과정에서 생기는 여러 의사결정에 유연하게 대응할 수 없다면 블록체인 네트워크의 생존가능성(Sustainability)에 심각한 영향을 줄 수 있다.

본 고에서는 최근 발표된 정보보호 거버넌스와 블록체인 시스템 거버넌스에 대한 국제표준 내용을 기반으로 주요 개념을 소개하고 국내에서 두 가지 거버넌스 체계를 구현하기 위한 과정에서 발생할 수 있는 이슈와 이를 해결하기 위한 과제를 제시하고자 한다.

Ⅱ. 정보보호 거버넌스 지침

정보보호 거버넌스 국제표준 (ISO/IEC 27014: Governance of information security for the organization)은 정보보호 거버넌스의 개념, 원칙, 프로세스 등 전반적인 프레임워크를 제시하는 지침서이다. 2013년 국제표준으로 1차 버전이 발표되었고 이후 개정 작업을 거쳐 2020년 12월에 2차 버전이 발표되었다[3].

정보보호 거버넌스 국제표준 문서의 주요 내용은 정보보호 거버넌스 개념 소개와 더불어 거버넌스 원칙과 프로세스 그리고 최고경영층이 수행해야 할 과제를 포함하고 있다.

■ 개념: 정보보호 거버넌스와 ISMS와의 관계를 보여주면서 조직 내 기타 거버넌스 활동/표준과의 관계

* 중앙대학교 산업보안학과 (명예교수, jdkimsac@cau.ac.kr)

- 원칙과 프로세스: 정보보호 거버넌스의 6개 목표/원칙과 평가, 지시, 모니터링에 기반한 정보보호 거버넌스 프로세스
- ISMS에 대한 최고경영층의 요구사항: 최고경영층의 ISMS 구축과 운영에 관한 역할과 과제

2.1. 정보보호 거버넌스의 개념

정보보호 거버넌스 주체는 조직 내 최고 경영층 또는 주요 이해관계자이다. 최고 경영층은 외부의 주주, 고객 등 이해관계자의 요구사항을 반영하여 정보보호 활동에 대한 방향을 제시하고, 통제하는 역할을 수행한다. 다시 말해서, 정보보호 관리체계(ISMS)가 정보보호 계획수립, 실행, 검토, 개선을 위한 관리자의 활동을 위한 것이라면, 정보보호 거버넌스는 정보보호에 대한 전략 및 정책을 수립하여 나아가야 할 방향을 제시하고, 정보보호 관리체계 대한 성과를 모니터링 및 평가하는 것이다. 또한, 전사적인 정보보호 활동은 정보보호 요구사항과 비즈니스 요구사항간의 충돌, 조직 내에서 타 부서와 여러 가지 갈등이 발생할 수 있는데, 정보보호 조직의 리더인 CISO(Chief Information Security Officer)는 내/외부 이해관계자들과의 소통을 통하여 효율적이고, 효과적인 정보보호 활동이 수행될 수 있도록 노력해야 한다[4].

결국 정보보호 거버넌스의 핵심은 정보보호를 비즈니스에 어떻게 연계시킬지, 과연 정보보호가 비즈니스에 어떠한 가치를 제공할 수 있는지, 그리고 이를 위하여 최고 경영층은 무엇을 해야 하는지에 대한 해답을 찾는 것이다.

이러한 정보보호 거버넌스는 세 가지 목표(ABC)로 요약할 수 있다. 즉 책임성(Accountability), 비즈니스 연계성(Business alignment), 준거성(Compliance)이 그것이다. 책임성이라 함은 최고경영층을 위시한 모든 조직 구성원의 정보보호에 대한 역할과 책임이 명확히 규명되고, 경영층의 지시 및 통제를 수행하기 위한 적정 자원 할당이 이루어져야 함을 의미한다. 비즈니스 연계성은 정보보호가 조직의 사활을 결정짓는 전략적 이슈로서 간주되어야 하며, 따라서 전사적 위험관리 차원에서 업무활동에 기반을 둔 정보보호 체계가 구축되도록 해야 한다. 단순한 네트워크나 서버 수준에서의 정보보호 조치로는 한계가 있으며 “정보의 활용과 보호”라는 양날의 칼을 염두에 둔 균형있는 보호 조치가 실행되도록 해야 한다는 점이다. 준거성은 조직이 준수해야 할 관련 법과 규제는 물론이고 조직 내부의 정보보호 관련 정책/내규와 내부감사 활동 결과에 대한 준거 여부를 상시 모니터링하고 실행, 개선할 수 있는 체계를 구축해야 한다.

이러한 정보보호 거버넌스를 위한 ABC가 달성될 때 정보보호 솔루션 도입이나 정보보호 관리체계가 빛을 발할 것이다. 조직 내 정보보호 활동을 지휘, 통제, 평가할 수 있도록 최고경영층의 역할과 책임이 규명되고 이를 수행하기 위한 일련이 메커니즘이 지원되지 않는 한, 실무부처에서의 노력만으로는 실효를 거두기 어렵다는 점이다. 정보보호에 대한 낮은 인식수준을 제고시키고 새로운 문화로 정착시키기 위해서는 최고 경영층이 직접 챙기고 지시하며 책임지는 활동이 전제되어야 할 것이다. 이를 위해서는 정보보호 거버넌스의 실행 주체로서 역량을 갖춘 임원급의 CISO들이 더 많이 임명되어 활동해야 할 것이며, 조직 내에서 확실한 위상을 차지해야 할 것이다.

2.2. 원칙 및 프로세스

정보보호 거버넌스 원칙들은 정보보호 거버넌스 프로세스 구현 시 지켜야 할 규칙 및 활동의 기반을 제공한다. 거버넌스 주체는 이러한 원칙들이 적용되고 누군가에 의해 원칙들이 구현될 수 있도록 책임과 권한을 할당해야만 한다. 정보보호 거버넌스의 조직 적용 및 구현을 위한 6개 목표/원칙은 다음과 같다[3].

- 목표 1: 조직 전반에 걸친 정보보호를 수립한다.
- 목표 2: 위험기반 보안 의사결정방법을 채택한다.
- 목표 3: 투자 의사결정의 방향을 설정한다.
- 목표 4: 내외부 요구사항의 준수를 입증한다.
- 목표 5: 긍정적 보안문화를 조성한다.
- 목표 6: 정보보호 성과는 조직의 현재와 미래의 요구사항을 만족할 수 있도록 보장한다.

이러한 목표 달성을 위해 거버넌스 주체는 “평가(Evaluate)”, “지시(Direct)”, “모니터(Monitor)”, “의사소통(Communicate)” 등 네 가지 프로세스를 이행한다[4]. [그림 1]은 정보보호 거버넌스 프레임워크 내에서 평가, 지시, 모니터, 의사소통 프로세스의 관계를 보여

준다.

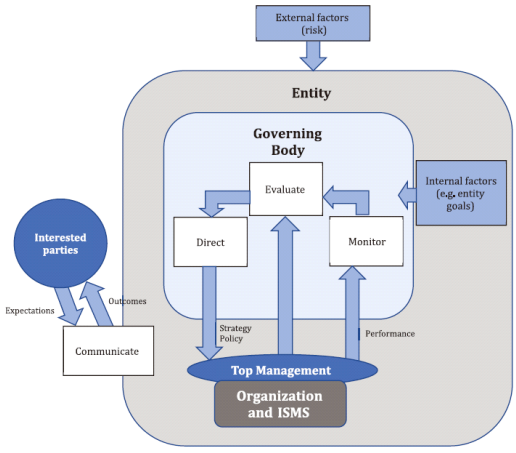
“평가”는 조직이 현재와 미래의 요구사항 및 상황을 고려하여 수립된 정보보호 활동 목표 및 전략의 성취 여부를 평가하는 거버넌스 프로세스이다. 또한, “평가”를 통해 전략 목표 성취를 위한 주요 의사결정이 이루어진다.

“지시”는 거버넌스 주체에 의해 결정된 정보보호 목표와 방향을 거버넌스 대상에게 적용하는 거버넌스 프로세스이다. 해당 방향에는 자원 투입수준과 자원 할당, 행위의 우선순위, 정책의 승인, 위험의 허용 및 위험관리 계획의 변화를 포함시킬 수 있다.

“모니터”는 거버넌스 주체가 전략적 목표의 성취 여부를 확인하는 프로세스이다.

“의사소통”은 양측의 구체적 요구에 따라 정보보호에 관한 정보를 교환하는 거버넌스 주체와 이해관계자 양방향으로 작용하는 거버넌스 프로세스 이다.

[그림 1]에서와 같이 거버넌스 주체(이사회, 최고경영층)는 ISMS와 상호작용 하에서 거버넌스 행위를 수행한다. 따라서 ISMS에 대한 최고경영층이 수행해야 할 과제는 ISMS 구축 및 인증범위를 승인하고 ISMS의 목표, 요구사항, 역할 및 자원 투입 등에 대한 의사결정을 수행하며, 위험성향(허용가능 위험수준) 및 적절한 위험처리 방안을 승인한다, 또한 의사소통 채널을 제공하여 정보공유 및 갈등 해결을 통한 전사적 보안체계 구축에 노력해야 한다.



〔그림 1〕 정보보호 거버넌스 프로세스

Ⅲ. 블록체인/분산원장기술 거버넌스 지침

3.1. 거버넌스 필요성과 개념

블록체인과 분산원장기술 거버넌스 지침(ISO TS 23635, Guidelines for Governance)에 대한 국제표준화 작업은 ISO TC 307 WG 5에서 작업하고 있다. 이 작업은 2018년부터 3년여의 노력 끝에 2022년 2월 말에 국제표준으로 발표되었다[5]. 블록체인을 활용하여 비즈니스를 수행하기 위해서는 블록체인 목표에 따라 온체인(On-chain)과 오프체인(Off-chain) 상의 의사결정권, 책임성, 보상체계와 같은 블록체인 거버넌스 요소들을 고려해야 한다. 블록체인 거버넌스가 부재한 상태로 비즈니스를 수행하면 시스템이 추구하는 목표와 전략을 효과적이고 효율적으로 달성할 수 없고, 조직의 이해관계자들의 기대 및 법규 등의 내 외부 요구사항들을 준수하기 어렵기 때문에 블록체인 서비스의 생존 가능성을 위협할 수 있다[6].

ISO TC 307에서는 블록체인 거버넌스를 중앙 또는 탈중앙화 된 의사결정권 요소를 모두 포함하는 접근방식으로, 책임성이 네트워크 내에 있고, 참여자들이 합의에 도달하도록 인센티브가 제공되어야 효과적, 효율적인 블록체인 구현이 가능하다고 정의하고 있다.

거버넌스 지침 문서에 의하면, 블록체인 거버넌스는 세 가지의 유형에 따라 다른 거버넌스 메커니즘을 구축해야 한다. Public/permissioned 시스템에서는 거버넌스 규칙이 사전에 설정되어 있기 때문에, 거버넌스 집행 주체의 선정과 거버넌스 규칙 변경 프로세스가 주요 이슈이다. 중앙 당국이나 컨소시엄이 거버넌스 집행 주체로 결정되면, 이들은 주어진 권한을 기반으로 거버넌스를 집행하며 의견 불일치 시, 포킹(forking)을 통해 의견 조율을 한다.

Public/permissionless 시스템은 전통적인 중앙집중식 시스템과 다르게, 참여자들의 공유되고 상향식 합의를 통해 거버넌스가 수행된다. 초기에는 중앙당국이나 위원회가 시스템의 목적에 따라 거버넌스 시스템을 설계하고 구축하지만, 구현단계에서는 참여자들이 투표 메커니즘과 하드/소프트 포크와 같은 민주적인 의사결정 프로세스를 통해 온체인과 오프체인 상의 거버넌스를 수행한다. 즉, Public/permissionless 시스템의 거버넌스 설계단계에서는 중앙당국에 의해 거버넌스 규칙이 설정되지만 시간이 경과함에 따라 다양한 참여자들의

상향식 의사결정을 통해 거버넌스 규칙이 변경되고 집행되어 진다.

Private/permissioned 시스템의 거버넌스는 일반적인 IT 거버넌스와 같이 전통적인 계층구조 환경의 거버넌스 체계와 유사하다. 중앙집중식 시스템이기 때문에 탈중앙화된 책임성 확보와 의사결정이 필요하지 않다. 전통적인 시스템과 차별화되지 않았기 때문에 블록체인만의 장점을 활용하기에는 부족하지만 기존 거버넌스 시스템을 블록체인 시스템에 적용함에 있어 수월하다는 장점을 가진다.

3.2. 블록체인 거버넌스 원칙과 프레임워크

거버넌스 원칙은 이해관계자가 거버넌스 활동을 수행하는데 있어 기반이 되며 항상 참조 할 수 있는 규칙(guiding rule)으로서 거버넌스 목표를 달성하고, 이 원칙에 기초하여 블록체인에서의 구조를 수립하고 활동을 구현할 수 있게 한다[7].

ISO/IEC 38500에서 기술하는 전통적인 IT 거버넌스는 단일 조직 내에서의 거버넌스 기능과 책임성을 다룬다[8]. 하지만 블록체인은 일반 IT 시스템과 달리 참여 노드들이 여러 조직이나 다양한 목적을 가진 개인들에 의해 운영되는 분산된 컴퓨팅과 탈중앙화된 시스템이다. 블록체인의 확장성으로 인해 시스템에 참여하는 조직과 신뢰의 경계가 지속적으로 확대된다. 따라서 블록체인 거버넌스는 ISO/IEC 38500에서 기술한 단일 조직 내에서의 거버넌스 접근방식과 달리 다양한 조직 및 개인을 포함해야 하며 오프체인 공동체, 오프체인 개발자, 온체인 프로토콜이라는 레이어(Layer)에서 블록체인 기술의 특성을 반영한 합의, 인센티브, 멤버십, 의사소통 등 다양한 차원(Dimension)으로 구성된 거버넌스 프레임워크를 고려해야 한다[9]

〔표 1〕 블록체인 거버넌스 원칙

제1원칙: 관련 개체(entity)의 식별자를 확인한다
제2원칙: 탈 중앙화된 의사결정을 가능하게 한다
제3원칙: 명시적 책임성을 보장한다
제4원칙: 투명성과 개방성을 지원한다
제5원칙: 블록체인 목표와 연계된 인센티브를 제공한다
제6원칙: 시스템의 성능 및 확장성을 제공한다
제7원칙: 위험 기반 의사결정과 준거성을 보장한다
제8원칙: 보안 및 프라이버시를 보장한다
제9원칙: 상호 운용성 요구사항을 고려한다
제7원칙: 위험 기반 의사결정과 준거성을 보장한다
제9원칙: 상호 운용성 요구사항을 고려한다

TS 23635에서 제시하는 블록체인 거버넌스는 의사결정권, 책임성과 인센티브, 등 3가지 차원으로 분류된다[5]. 첫째, 의사결정권은 의사결정 통제에 관한 권한(Decision control rights)과 의사결정 관리에 대한 권한(Decision management rights)으로 구별할 수 있다. 전자는 의사결정의 승인 및 모니터링에 관한 것이며, 후자는 의사결정을 제안하고 결정된 사안을 실행 및 구현하는 것이다. 이러한 의사결정권의 분배는 블록체인을 활용함에 있어 시스템의 탈중앙화 정도에 따라 결정되어야 하며 이해관계자들은 이러한 의사결정권 분배되는 방식에 따라 영향을 받는다. 또한 의사결정권은 온체인과 오프체인 상에서의 의사결정을 모두 고려하여 할당되어야 한다. 온체인 의사결정은 블록체인 운영에 필요로 한 합의나 내부규정에 관한 것으로 시스템에 내재되어 있는 사안이라면, 오프체인 의사결정은 법규준수 및 외부 이해관계자들의 기대 충족, 비 블록체인과의 상호운용성과 시스템의 유연성을 위한 사안이다.

두 번째, 책임성은 블록체인 시스템의 구축 및 사용에서 참여자의 책임 소재에 관한 내용을 의미한다. 블록체인은 신뢰하는 제 3자의 개입이 없고 각자 다른 목적을 가지고 있는 참여자들에 의해 운영된다. 이러한 참여자들이 시스템 목적을 공동으로 달성하게 하기 위해서는 역할 및 책임을 명확히 해야 하고 그에 따른 책임성을 규정해야 한다. 블록체인의 전략과 목적 달성을 위해 강력한 책임소재 규명은 필수적이고 이를 집행하는 체계가 필요하다. 자가 보상, 자가 처벌, 자가 모니터링을 피하기 위해 블록체인의 통제와 관리는 분리되어야 하며 책임성은 조직의 규정 및 법적 프레임워크를 통해 제정되어야 하고 명백하게 시행되어야 한다. 또한 블록체인의 책임성은 온체인 상에서 시스템 규칙에 따라 규정할 수 있으며 오프체인 상에서도 외부 법규로 규정할 수 있다.

세 번째, 인센티브는 블록체인의 다양한 참여자 및 이해관계자의 행동을 유도하는 핵심적인 역할을 한다. 참여자의 바람직한 행동과 인센티브의 연계는 참여자들이 자신의 행동을 자유롭게 결정할 수 있게 하며 시스

템의 목적과 자신들의 행동을 일치하도록 하게 한다. 시스템 참여자들에 대한 인센티브가 잘못 연계되면 궁극적으로 참여자 또는 이해관계자들은 장기적인 관점에서 시스템을 해치는 행동을 할 수 있으며 시스템의 지속가능한 운영을 위태롭게 할 수 있다. 시스템의 인센티브는 의사결정권자 간의 합의 달성, 분쟁 해결 및 시스템의 지속적인 관리, 설계 및 운영에 대한 결정을 유도한다. 인센티브는 금전적 인센티브와 비금전적 인센티브로 구별할 수 있다. 전자는 참여자의 행동을 금전적인 보상과 연계하는 것이며, 후자는 권한상승, 명예 등과 같은 비금전적인 보상을 참여자의 행동과 연계하는 것이다.

3.3. 블록체인 거버넌스 구현

블록체인 거버넌스 구현을 위해서는 다음과 같은 이슈들을 고려해야 한다: 1) 블록체인 생애주기와 컨텍스트별 거버넌스 활동, 2) 거버넌스 구현을 위한 주체들의 역할, 3) 거버넌스 구현 도구.

블록체인의 생애 주기는 구축, 운영, 종료의 세 가지 핵심 단계로 이루어지는데, 블록체인의 거버넌스는 모든 생애 주기 동안 책임성, 결정 권한과 인센티브를 제공해야 한다.

구축 단계에서의 거버넌스 활동에는 거버넌스의 형태, 법 및 규제와의 상호 운용 메커니즘, 블록체인 시스템 구성 형태, 분쟁 해결, 운영을 관리하기 위한 절차 및 정책, 블록체인 시스템의 종료 등이 있다. 이때 만들어진 주요한 정책들은 이후 순차적으로 형성되는 시스템들의 거버넌스 구조를 결정한다. 따라서 구축 단계에서의 거버넌스 정책은 블록체인 시스템을 어떻게 운영하고, 시스템 변경 시 어떤 식으로 합의되고 적용되는지에 대한 원칙을 포함해야 한다.

운영 단계에서의 거버넌스는 블록체인 시스템 참여자에 대한 권한 등록, 블록체인 참여에 관련된 계약 규정 등 운영 단계의 여러 주요 기능들을 감독한다.

종료 단계에서의 거버넌스는 블록체인 종료시의 상호 작용이 관련없는 오프체인 거버넌스 요인에 의해 결정될 수 있기 때문에, 거버넌스는 블록체인 종료 시 외부 환경과의 상호 작용을 명시적으로 지원해야 한다.

TS 23635에서는 블록체인의 4가지 컨텍스트(데이터, 프로토콜, 애플리케이션, 조직 등)를 규정하고 있으며, 각 컨텍스트별 거버넌스 활동을 블록체인의 생애 주기에 따라 제시하고 있다.

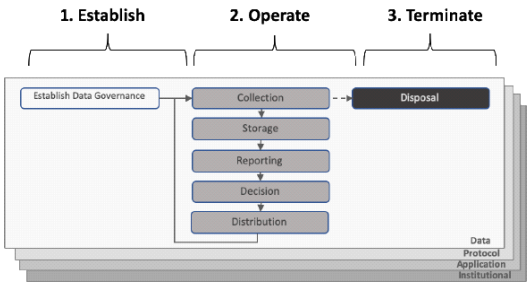
데이터 컨텍스트로는 블록체인의 구축 단계에서 데이터의 생성, 관리, 파기 방법과 종류를 포함하는 데이터 거버넌스를 정의한다. 또한 이는 기존의 다른 시스템들과 상호작용하면서 데이터 거버넌스를 결정하게 된다. 이후 거버넌스는 운영 단계에서 데이터가 어떻게 관리될 것인지에 대해 예측해야 하고, 종료 단계에서는 데이터의 폐기에 대한 정책 결정과 폐기 준수 여부를 감독해야 한다.

프로토콜 컨텍스트로는 구축 단계에서 프로토콜 거버넌스를 정의하는데, 여기에는 블록체인의 생애 주기에 걸쳐 트랜잭션을 어떻게 정의하고 관리할지에 대한 내용이 포함된다. 또한 이때 거버넌스는 프로토콜과 다른 시스템과의 상호 운용성도 결정하게 된다. 이후 운영 단계에서 프로토콜의 작동 방식과 변경에 대한 규칙을 정의해야 하며, 종료 단계에서는 종료가 결정되는 시기, 조건, 검증방식 등이 프로토콜이 기능하는 방식에 대해 예측하고, 안내해야 한다.

애플리케이션 컨텍스트로는 구축 단계에서 분산형 애플리케이션의 구현 방법, 접근 권한, 책임 등을 포함하는 애플리케이션 거버넌스를 정의하고, 운영 단계에서는 블록체인 시스템의 애플리케이션이 어떻게 상호작용하는지 그리고 지속적인 변화와 유지보수를 지원하기 위해 필요한 규칙들을 적용해야 한다. 이후 종료 단계에서는 애플리케이션이 어떻게 폐기, 파기 또는 이전될지를 안내해야 한다.

조직 컨텍스트로는 거버넌스가 생애 주기별 각 단계에서 블록체인이 기존의 조직 거버넌스와 상호 운용되는 방법을 정의한다. 이때 구축 단계에서는 블록체인 시스템의 거버넌스 메커니즘 및 구조와 기존 조직 거버넌스와의 관련성이 포함되며, 그 관계가 존재하지 않는다면 이를 분명히 제시해야 한다. 운영 단계에서는 유관기관의 시스템이 블록체인 시스템에서의 결정 권한, 책임, 인센티브를 행사하는 방법이 포함되며, 종료 단계에서는 시스템이 종료될 때 기존 시스템과 블록체인 시스템의 결정 권한, 책임, 인센티브가 상호 운용되는 방식이 포함된다. 컨텍스트별 거버넌스 의사결정 프로세스는 [그림 2]과 같다.

TS 23635에서는 블록체인 거버넌스를 위해 6가지 주체별(거버너, 감사원, 관리자, 개발자, 제공자, 사



〔그림 2〕 컨텍스트별 거버넌스 의사결정 프로세스

용자 등) 들이 수행해야 하는 역할을 책임성, 의사결정 권한, 인센티브 측면으로 구분하여 제시하고 있다. 예시로, 거버넌스 핵심 주체인 거버너(Governor)는 블록체인 시스템의 장기적인 비즈니스 모델의 구현과 지속성을 유지하는 역할을 수행한다. 이를 위해 각 주체들의 책임과 의무에 대한 정책을 설정하고, 의사결정 투표 메커니즘을 설정한다. 또한 스폰서와 자금 조달을 위한 프로세스를 마련하고 개발자 등을 위한 보상 및 인센티브 계획을 설계 및 승인한다.

블록체인 거버넌스 도구는 온체인과 오프체인 거버넌스 도구로 구성된다. 온체인 거버넌스 도구는 일반적으로 투표 메커니즘을 의미하는데, 의사 결정은 프로토콜 기반 직접 투표를 통해 이루어진다. 투표 커뮤니티는 일반적으로 블록체인 시스템 제공자, 개발자, 사용자로 구성되어 있다. 하지만 온체인 거버넌스에는 의사 결정에 대한 합의가 이루어지지 않는 경우가 발생할 수 있는데, 그 경우 포크를 통해 상황을 조정하게 된다.

오프체인 거버넌스 도구는 블록체인의 외부 메커니즘을 의미한다. 기존의 법률이나 규제 프레임워크, 표준, 부문별 행동 강령 등을 준수해야 하기 때문에, 모든 블록체인 시스템은 오프체인 거버넌스 제도의 영향을 받는다 오프체인 거버넌스 도구의 목적은 온체인에서 수행되는 트랜잭션의 의도를 유지하는 것으로, 온체인 원장과 오프체인 정보의 무결성을 유지하기 위해 불변성과 트랜잭션의 유효성 검증 등을 제공한다. 오프체인 거버넌스는 ISO 38500, ISO/IEC 27014에 명시된 원칙을 활용하며, 오프체인 거버넌스에서는 투표 외에도 여러 다양한 메커니즘을 통해 이해 관계자들의 합의를 이끌어낼 수 있다.

표준문서에서는 블록체인 거버넌스 도구의 구현을 위해 필요한 사항으로 적응성, 위험 관리, 프라이버시를 고려하고 있다. 우선 블록체인 시스템은 변화에 대해 합의하고 시행할 수 있어야 한다. 이때, ISO 9001 또는 ISO 20000과 같은 프로세스를 채택하여 변화를 관리해야 한다. Permissioned/Public 블록체인 시스템의 경우 거래 유효성을 검증하는 네트워크 내 거버너가 변화 거버넌스를 처리해야 하고, Permissioned/Private 블록체인 시스템의 경우 이해관계자들의 필요에 의해 언제든 변경될 수 있기 때문에 전용 합의 메커니즘을 필요로 하지 않는다. Permissionless/Private 블록체인 시스템에서는 온체인 거버넌스 메커니즘이 구현되어야 한다.

블록체인의 위험평가는 ISO 31000과 ISO/IEC 27005의 위험관리 프로세스를 따른다. 그러나 블록체인은 탈중앙화 시스템이기 때문에 다양한 이해관계자를 고려해야 한다. 특히 Permissionless 시스템의 경우 공식 거버넌스 메커니즘이 없기 때문에, 시스템의 생애 주기 전체에 걸쳐 이해 관계자들의 인센티브가 적절하게 유지되도록 보장하는 메커니즘을 도입하는 것이 필수적이다. Permissioned 시스템의 경우 이해관계자들을 식별할 수 있기 때문에 전통적인 거버넌스 메커니즘을 통해 인센티브를 통합할 수 있으며, 위험 평가 수행이 가능하다.

Ⅳ. 거버넌스 구현 이슈와 과제

4.1. 정보보호 거버넌스 구현 이슈와 과제

국내 대기업 및 금융그룹들은 지주사 출범을 통해 기업 거버넌스에서 요구하는 재무적인 지배구조를 확립하였고 이에 따라 IT와 정보보호 영역에서의 거버넌스 체계구축이 진행되고 있다. 금융그룹의 경우 차세대시스템 구축 프로젝트를 통해 지주회사와 계열사 간의 IT 또는 정보보호 거버넌스 체계를 일부 구축하고 있으며 최근 들어 GRC(거버넌스, 위험관리, 컴플라이언스) 프로젝트들이 점차 확산 구현되고 있다. 이러한 상황에서 국내 정보보호 거버넌스 체계가 적절히 구현되기 위해서는 다음과 같은 이슈와 과제를 해결할 필요가 있다.

첫째, 국제표준(ISO 27014)에서 권고하는 거버넌스 체계는 이사회 또는 비즈니스 최고경영층의 정보보호에 대한 리더십과 책임을 강조하고 있으며 정보보호의 비즈니스적 가치를 인정하여 최고경영층의 참여와 지원 등 전사적인 노력을 권고하고 있으나, 국내 현실에서는 정보보호 임무를 정보기술의 한 분야로 보고 있다. 조직의 실질적인 정보보호 거버넌스 역할을 수행할 수 있는

정보보호 위원회의 구성을 보더라도 정보보호 최고책임자(CISO)가 의장 역할을 하고 IT 관련 부서의 실무자급 직원이 위원회 멤버로 포함되어 있어 실질적인 거버넌스 역할을 수행하고 있지 못하다. 정보보호관리체계(ISMS)인증기준에서 요구하는 정보보호 위원회의 구성 기준은 최소한의 기준으로 간주해야 하며, 정보보호의 비즈니스 가치가 점증하는 현실을 반영하여 실질적인 거버넌스 매커니즘이 될 수 있도록 정보보호 위원회의 위상이 격상되어야 한다. 즉 정보보호에 관한 최고 의사결정기구로서 정보보호 위원회가 역할을 해야 하며 이를 통해 전사적 보안을 구축해야 한다. 또한, 현업부서의 협조를 유도할 수 있으며, 정보보호 활동으로 인한 발생 가능한 갈등 상황을 조정할 수 있도록 해야 한다. 이를 위해서는 현업과 IT부서의 상위 경영층으로 구성된 정보보호 위원회가 제대로 거버넌스 역할을 수행해야 한다. 이미 미국과 유럽 등 일부 선진 기업에서는 내부통제시스템의 일부로서 정보보호 구현에 대한 책임을 CEO와 CFO에게 지우고 있다.

둘째, 정보보호 거버넌스 구현 및 평가를 위한 제반 기준 및 지침 수립이 필요하다. 금융권에서 정보보호 거버넌스 지침이 배포되었으나, 보다 구체적인 정보보호 투자관리, 정보보호 활동의 성과평가, 정보자산에 대한 실시간 위험관리, 비즈니스와의 전략적 연계 등에 관한 지침 및 방법 개발이 요구된다. 즉 비즈니스 관점에서의 정보보호 활동을 기획하고 평가할 수 있는 지침 개발이 필요하다.

셋째, 정보보호 거버넌스를 용이하게 수행할 수 있는 제반 시스템이나 도구들이 개발될 필요가 있다. 최근 GRC (governance, risk, compliance) 시장이 점차 확대되고 있으며 이를 위한 시스템 개발이 해외에서 활발하게 진행되고 있다. 국내에서의 GRC 시장은 아직 초보단계에 있으며 앞으로 많은 연구 개발이 요구된다.

4.2. 블록체인 거버넌스 구현 이슈와 과제

최근 다수의 기업형 블록체인 서비스가 도입되어 사용 중에 있으나, 실효성 측면에서 많은 이슈를 발견할 수 있다. 다시 말해 블록체인 기술을 적용해서 시스템으로 구현하였고 서비스가 작동된다는 점에 의의를 두고 있지 이것이 실제로 원래 의도했던 목적을 달성하고 있는 가에 대해서는 아직 많은 해결되지 못한 이슈가 있다. 이러한 도입 실패 원인 중 하나가 적절한 거버넌스 체계가 구현되지 않았기 때문이다. 블록체인 설계시 경제적 관점을 무시하고 기술적 설계 우선 적용한 점이다[6].

블록체인 플랫폼은 다수의 참여자가 동등한 자격으로 참여하는 분산화된 네트워크로 구성된 경제 시스템(economic systems)으로 간주되어야 한다. 즉 공유 가치를 기반으로 자원을 공유하고 있다는 점, 탈중앙화된 지시 및 통제 활동이 요구되며 궁극적으로는 소프트웨어 솔루션이라는 점에서 새로운 형태의 거버넌스 체계가 필요하다. 다수의 참여자에 대한 정교한 인센티브 시스템 설계와 더불어 적절한 합의 메커니즘이 결여되었고, 또한 변화하는 환경에 적절히 대응할 수 있는 스마트 컨트랙트 변화관리 메커니즘이 없다면 하나의 생태계로서의 블록체인 시스템/서비스는 그 생명력을 유지하기 힘들 것이다[10].

두 번째 이유로는 잘못된 초기 비즈니스 모델을 선택하고 초기 참여 구성원 선택을 들 수 있다. 블록체인은 플랫폼의 성격을 가지고 있으며 따라서 다양한 네트워크 효과를 활용해야 하는데 네트워크 효과의 역동성에 대한 이해가 부족하여 초기 비즈니스 모델이 적절하게 개발되지 못했기 때문이다. 즉 비즈니스 모델 수립이라는 전략적 의사결정을 잘못한 결과로 인해 실효성 없는 시스템 도입이 초래될 수 있다.

Ⅴ. 결 론

과거 20년여에 걸친 국내 정보보호 확산 노력으로 인해 기술적 측면에서의 많은 업적을 이루었다는 점은 부인할 수 없다. 그러나 정보보호가 비즈니스에서 차지하는 중요성에 비추어 정보보호 거버넌스로의 패러다임 변화와 함께 실효성 있는 실천 방안 없이는 더 이상의 발전을 기대하기 어려울 것이다.

또한 블록체인 기술이 확산 단계에 진입하면서 초기의 파일롯 시스템 구현 형태의 실험단계를 지나 기업형 블록체인 서비스/시스템이 활발히 도입되고 있다. 실효성 있는 기업형 블록체인 서비스를 제공하기 위해서는 초기 설계 단계부터 블록체인 구현 및 운영에 적절한 의사결정(전략, 비즈니스 모델, 블록체인 시스템 구성 방식 등)이 실현되어야 블록체인 서비스의 생존성 및 확장성을 보장받을 수 있을 것이다.

최근 정보보호와 블록체인에 관한 거버넌스 국제표

준이 발간됨에 따라 두 거버넌스 체계 구축의 중요성이 재삼 부각되기 바라며 구축 과정에서 발생 가능한 거버넌스 관련 제반 이슈에 대한 올바른 해결이 시급한 실정이다.

참 고 문 헌

[1] Basie von Solms, “Information Security – The Fourth Wave,” Computers & Security Vol. 25, pp.165~168, 2006.

[2] R. Beck, C. Bloch, J. King, “Governance in the blockchain economy: A framework and research agenda”. *Journal of the Association for Information Systems*, 19(10), pp.1020-1034. October 2018.

[3] ISO/IEC 27014, “Information technology – Security techniques – Governance of information security for organiztions”. October 2019.

[4] ITGI, “Information Security Governance : Guidance for Boards of Directors and Executive Management,” 2002.

[5] ISO/TC 307 TS 23635, *“Blockchain and distributed ledger technologies – Guidelines for Governance”*. Feb. 2022.

[6] D. Yermack, “*Corporate governance and blockchains*”. Oxford. January 2017.

[7] Banff Executive Leadership Inc, “*Improving governance performance rules-based vs. principles-based approaches*”. February 2004.

[8] ISO/IEC 38500, “Corporate governance of information technology”. February 2015.

[9] Rowan van Pelt, Slinger Jansen, Djuri Baars & Sietse Overbeek, “*Defining Blockchain Governance: A Framework for Analysis and Comparison”*, Information Systems Management, 38:1, pp. 21-41, 2021.

[10] V. Shermin, “*Disrupting governance with blockchains and smart contracts”*. John Wiley & Sons. September 2017.

〈저 자 소 개〉

김 정 덕 (Jungduk Kim)

종신회원

1979년 2월 : 연세대학교 정치외교학과 졸업

1981년 8월 : 연세대학교 경제학과 석사

1986년 5월 : University of S. Carolina, MBA

1990년 12월 : Texas A&M University, Ph.D. in MIS

1995년 3월~2014년 8월 : 중앙대학교 정보시스템학과 교수

2014년 9월~2021년 2월: 중앙대학교 산업보안학과 교수

2018년 9월~현재 : ISO SC 27, TC 307 국제표준전문위원

<관심분야> 디지털 비즈니스 보안, 사이버보안 거버넌스 및 관리, 인간중심보안