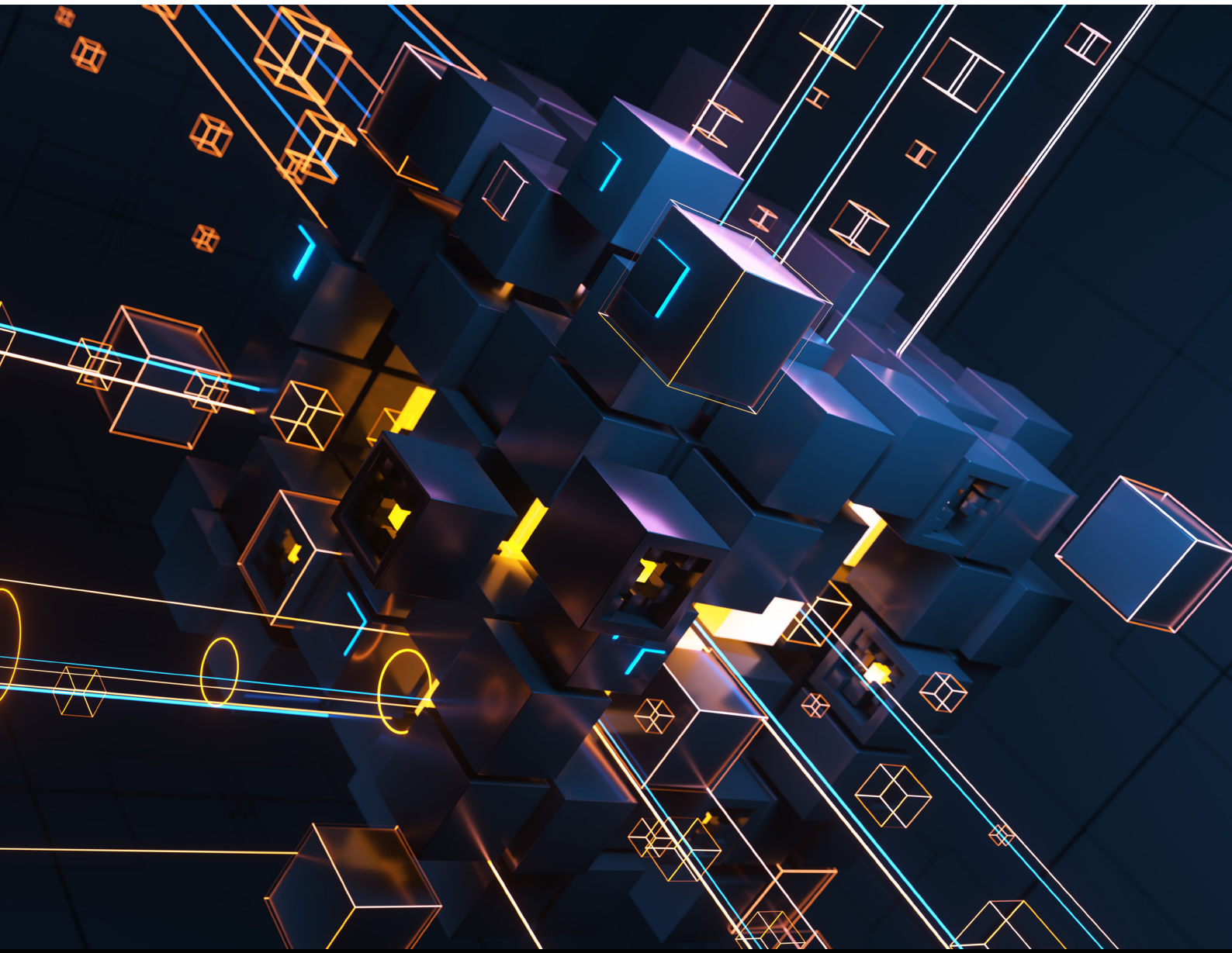
IDG
STRATEGIC
MARKETING SERVICES

IBM

IDG Summary

외부 해킹도, 내부자 위협도 '원천 봉쇄' '토큰화 시대' 디지털 자산 인프라의 조건

현실의 자산을 블록체인 네트워크 속 토큰으로 바꿔 자산에 대한 권리를 디지털화하고 이를 이용해 거래할 수 있도록 하는 것을 토큰화(tokenization)라고 한다. 일단 토큰화가 이루어지면 마치 온라인 쇼핑몰에서 물건을 구매하듯 간편하게 자산을 사고팔 수 있다. 주식이나 부동산, 광산 채굴권, 미술 경매품 등 잠재적 토큰화 시장은 전 세계적으로 1,200조 달러에 달한다. 그렇다면 이 막대한 디지털 자산을 안전하게 보관하는 시스템을 어떻게 구축해야 할까. 핵심 요건은 바로 보안이다. 성능과 확장성이 아무리 좋아도 토큰을 해킹당하면 의미가 없기 때문이다. 오늘날 점점 더 큰 위협으로 부상하는 '특권자 제어'를 비롯해 디지털 자산 인프라의 필수 보안 조건을 살펴보자.



외부 해킹도, 내부자 위협도 '원천 봉쇄' '토큰화 시대' 디지털 자산 인프라의 조건

이명철 | 한국IBM 시스템 사업부 상무

토큰화(tokenization). 다소 낯설게 들리지만 개념 자체는 간단하다. 현실의 자산을 블록체인 네트워크 속 토큰으로 바꿔 자산에 대한 권리를 디지털화하고 이를 이용해 거래할 수 있도록 하는 것을 의미한다. 일단 토큰화가 이루어지면 마치 온라인 쇼핑몰에서 물건을 구매하듯 간편하게 자산을 사고팔 수 있다. 주식이나 채권, 부동산 거래, 광산 채굴권은 물론 심지어 미술 경매품도 모두 토큰으로 만들어 거래할 수 있다. 국제결제은행(BIS)에 따르면, 잠재적 토큰화 시장은 전 세계적으로 1,200조 달러에 달한다. 미래 성장 가능성을 짐작할 수 있는 대목이다.

'1,200조 달러' 디지털 토큰화의 거대 잠재력

디지털 토큰은 여러 가지 장점이 있다. 일단 국경이나 시간의 제약이 적다. 우리나라에 있는 사람이 미국에 있는 사람에게 24시간 언제든 클릭 몇 번으로 토큰을 보낼 수 있다. 소유권을 매우 세분화해 배분할 수 있는 것도 특징이다. 비트코인의 경우 1비트코인의 소유주가 수백만 명이 되기도 한다. 또한 주식 시장 외에 세컨더리 마켓이 활성화돼 있고 거래 비용도 저렴하다.

반면 토큰은 정부 규제에 큰 영향을 받는다. 예를 들어 지난 2018년 1월 우리 정부는 가상화폐 시장 과열을 막기 위해 거래 실명제를 도입했다. 당시에는 반발도 많았지만 결과적으로 이후 2년간 전 세계 가상화폐 시장이 안정세를 유지하는 데 공헌을 했다.

토큰 시장이 규제에 취약하다는 것은 바꿔 말해 정부의 제도적 지원에 따라 크게 성장할 수도 있음을 의미한다. 실제로 최근 미국 와이오밍주가 비트코인을 자산으로 인정하고 누구나 합법적으로 거래할 수 있도록 허용했다. 독일의 솔라리스 뱅크는 법의 보호를 받는 블록체인 서비스를 시작했고, 미국의 피델리티 디지털 에셋은 파생 상품, 투자 상품 등 복합적인 서비스까지 제공한다. 지금은 주로 미국이나 유럽을 중심으로 토큰을 제도적으로 뒷받침하고 있지만, 우리나라도 곧 뒤따를 것으로 전망된다.

디지털 토큰의 종류는 크게 4가지다. 가장 널리 알려진 것이 비트코인 같은 암호화폐다. 금융거래를 보호하고 이중 결제를 막는 디지털 통화다. 그러나 암호화폐는 가격의 변동이 크기 때문에 안정적인 토큰이 필요했고, 그 대안으로 등장한 것이 스테이블 코인이다. 정부 통화기관이 발행, 관리, 보증해 유로나 달

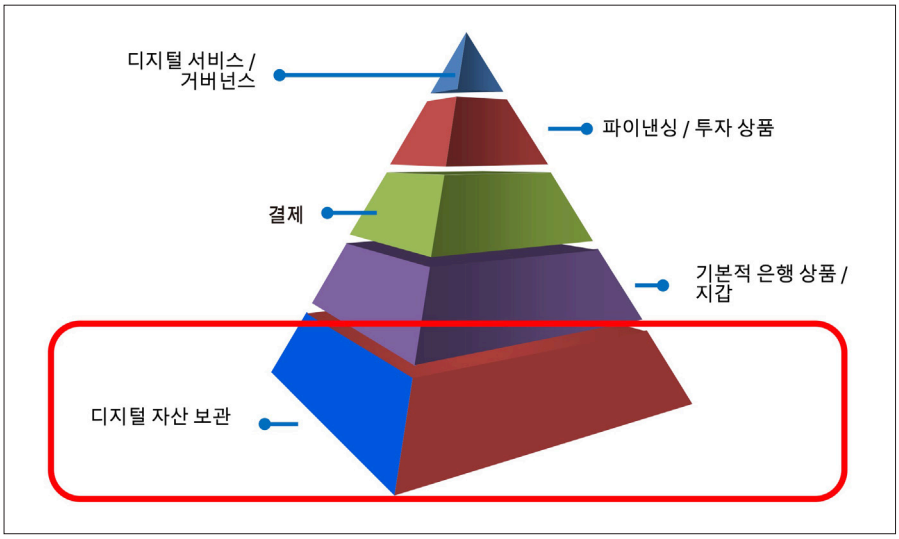
러 등 법정 통화로 바꿀 수 있는 디지털 자산이다. 증권형 토큰도 있다. 특정 프로젝트를 1/n로 나눠 토큰화한 후 지분 혹은 권리를 나눠 갖는다. 마지막은 자연자산 토큰이다. 광산 채굴권, 석유 시추권, 미술품 같은 것을 토큰화해 거래할 수 있도록 지원한다.

디지털 자산 서비스도 빠르게 확산 중

현재 디지털 토큰 시장에는 다양한 기업이 활동하고 있다. 유명 자산거래 플랫폼인 비트맥스(Bitmex), 오는 7월부터 비트코인 선물 거래를 시작하는 백트(Bakkt)를 비롯해 대형 아시아은행 DBS가 있다. 블록체인 기반의 보험사, 송금 기업도 이름을 올렸다. 새로운 기업도 속속 시장에 뛰어들고 있다. 디지털 자산 관리 전문기업 시그넘(Sygnum), OTC(Over The Counter market) 거래에 특화된 서클(Circle) 등이 대표적이다. 앞으로 이 시장의 성장 가능성을 고려하면 더 많은 기업이 계속 출사표를 던질 것으로 전망된다.

이들 기업의 여러 디지털 자산 관련 서비스는 크게 4가지로 분류할 수 있다. 먼저 디지털 자산 생성과 보관 서비스다. 투자 상품에 대한 정보나 서비스를 제공하고 자산을 보관한다. 대표적인 기업이 코인베이스(Coinbase), BTC팩츄얼(BTCPactual) 등이다. 두 번째는 신용 거래다. 주로 파이낸싱 기법을 이용해 ETF(Exchange-Traded Funds) 등을 발행하며, 주요 기업은 메이커(Maker), 텐엑스(TenX) 등이 있다.

최근 들어 미국과 유럽 등을 중심으로 주목받고 있는 디지털 자산 설계 서비스도 있다. 보통 비트코인이나 이더리움 등 디지털 자산의 주소와 비밀번호는 가족은 물론 유산 상속자에게도 미리 알려주지 않는다. 유출되면 타인이 임의로 가져갈 수 있기 때문이다. 문제는 소유자가 갑자기 사망하는 경우인데, 이처럼 숨어 있는 자산을 찾아주는 서비스가 자산 설계에 포함된다. 트라이던트 트러스트(Trident Trust), 레저(Ledger) 등이 이런 서비스를 제공한다. 마지막은 디지털



다양한 디지털 자산 금융 서비스가 있지만 모든 서비스의 기반은 디지털 자산 보관이다.

서비스와 거버넌스다. IBM이 북미에서 남미까지 송금 서비스를 제공하는 것이 대표적이다. 메서리(Messari) 같은 기업도 비슷한 서비스를 제공한다.

이처럼 많은 기업이 디지털 토큰 시장의 성장 가능성에 주목하며 새로운 서비스를 내놓고 있다. 그러나 이들 비즈니스 모델을 수직적으로 정리해보면 가장 기반이 되는 기능은 '디지털 자산 보관'이다.

실제로 디지털 자산이 없거나 보관할 수 없는 상태에서는 송금이나 결제, 투자, 파이낸싱 같은 사업 자체가 불가능하다. 디지털 자산 보관 인프라를 단단하게 만들어야 비로소 그 위에 다양한 응용 서비스를 올릴 수 있다. 고객 측면에서 봐도 디지털 토큰을 안전하게 보관한다는 신뢰가 형성되지 않으면 누구도 이를 기반으로 한 서비스에 자신의 소중한 자산을 맡기지 않을 것이다. 결국 디지털 토큰 서비스의 핵심이자 전제조건이 안전한 디지털 자산 보관임을 알 수 있다.

디지털 토큰 서비스 인프라의 조건

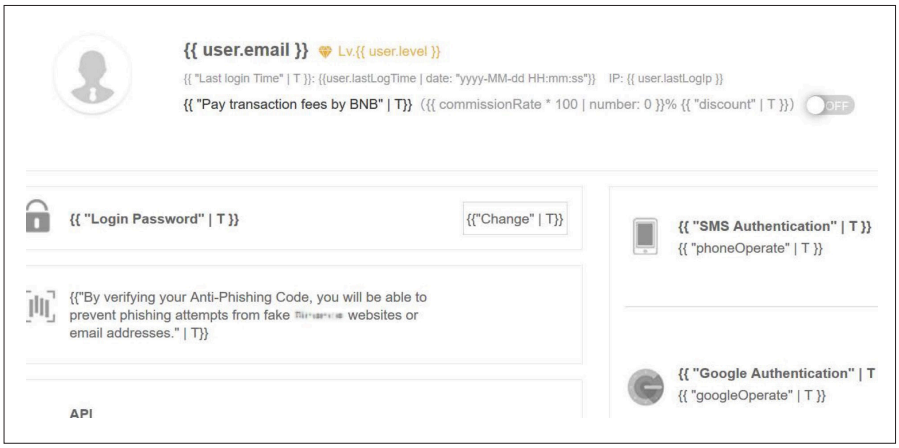
그렇다면 디지털 자산을 안전하게 보관할 수 있는 시스템을 어떻게 만들어야 할까. 디지털 토큰 서비스 인프라의 일반적인 요건은 기존 인프라와 크게 다르지 않다.

먼저 성능이다. 신속한 합의 연산과 읽기 쓰기 작업을 위해 필요하다. 특정 블록체인 참여자가 전체 블록체인 네트워크의 성능을 떨어뜨리는 것을 막기 위해서도 중요하다. 두 번째는 확장성이다. 참여자의 수가 늘어나는 것뿐만 아니라 새로운 합의 알고리즘이나 암호화를 도입하는 등 미래 기술까지 유연하게 수용할 수 있어야 한다. 가용성도 중요하다. 네트워크 참여자 중 특정 시스템이 중단되면 전체 네트워크에 악영향을 주거나 합의가 불가능할 수도 있다. 또한, 장애 상황에서 데이터를 복구해 정상적인 서비스를 제공하기 위해서도 가용성이 필수적이다.

그러나 이러한 일반적 요건보다 더 중요한 것이 있다. 바로 보안이다. 디지털 토큰 서비스 인프라의 존재 이유라고 해도 과언이 아니다. 아무리 성능이 뛰어나도 중간에 코인이 사라지면 소용이 없다. 확장성이 좋아 시스템 폭주를 다 처리할 수 있다고 해도 역시 토큰이나 코인이 해킹당하면 의미가 없다.

이 때문에 디지털 토큰 서비스 인프라의 보안은 기존 시스템보다 더 강력한 요건을 만족해야 한다. 먼저 네트워크 참여자 간의 격리를 보장해야 한다. 네트워크 참여자가 다른 사람의 지갑을 보거나 마음대로 옮길 수 없도록 하려면 완전하게 격리해야 한다. 사이버 공격에 대한 보호도 중요하다. 이때 외부 해킹에 대한 대비는 기본이다. 내부의 특권자(privileged user)나 루트 권한을 가진 관리자, 개발자라도 함부로 디지털 토큰 서비스 인프라에 코드를 추가하지 못하도록 막아야 한다.

마지막은 암호화다. 설사 해커가 토큰을 탈취한다고 해도 '암호화 키'로 보호하면 탈취한 토큰을 사용하지 못하게 하거나 혹은 사후 대응에 필요한 시간을 벌 수 있다. 이 밖에 네트워크와 메모리 덤프를 포함해 엔드 투 엔드로 인프라의 모든 것을 암호화해 보안을 강화해야 한다.



한 가상화폐 거래소의 해킹 사고에서 해커는 이중인증과 SMS 인증을 무력화했다.

디지털 토큰 서비스 인프라에서 보안이 전부인 이유

이처럼 디지털 토큰 서비스 인프라에서 보안이 강조되는 이유는 명확하다. 한 번 해킹되면 되돌릴 수 없는 막대한 피해를 보기 때문이다. 실제로 많은 기업이 보안을 강화하고 있지만 사고가 계속 발생하고 있다. 최근 세계 최대 비트코인 거래소 중 하나인 B사가 해킹돼 비트코인 7,000여 개, 약 500억 원 치를 탈취당했다. 사고 당시 이 기업의 홈페이지는 계정 관련 암호화가 무력화됐고 실소유자가 암호를 바꾸지 못하도록 관련 기능까지 막혔다. 이런 상태에서 해커는 44명의 계좌에서 비트코인을 빼앗아 자신의 계좌로 보냈다.

앞으로 부동산과 미술품 등 더 많은 고가의 현실 자산이 디지털 토큰으로 전환될수록 보안 사고로 인한 피해 규모도 눈덩이처럼 커질 것이다. 디지털 자산 탈취가 근본적으로 불가능한 수준의 보안이 요구되는 것도 이 때문이다.

특히 최근 들어 우려가 커지는 것 중 하나가 특권자 제어다. 기존의 일반적인 인프라에서는 외부 해커가 시스템을 뚫지 못하도록 막는 것에 주력했다. 그러나 많게는 수십조 원 가치를 관리하는 디지털 토큰 서비스 인프라에서는 루트 권한을 가진 내부 사용자를 제어하는 것이 외부 해킹을 막는 것만큼 중요하다. 예를 들어 내부 개발자가 '패스워드 입력 없이 송금하라'는 악의적인 코드를 추가하면 해당 디지털 자산 소유자의 승인 없이 소유권이 옮겨지는 대형 보안 사고가 발생할 수 있다. 실제로 IBM의 설문 조사 결과를 보면, 기업이 직면하는 위협의 80%가 기업 내부의 것이었다. 응답자의 91%는 내부자 위협이 현 수준 이상으로 계속 늘어날 것으로 전망했다.

기존 플랫폼에서는 어떤 시스템도 내부 운영자의 해킹을 근본적으로 막지 못한다. 개발자가 악의적인 코드를 삽입하지 못하도록 감시할 수는 있지만 이를 원천적으로 막는 것은 불가능하다. 따라서 디지털 토큰 서비스 인프라에서는 내부 운영자가 기업이 보관하는 디지털 자산에 접근할 수 없도록 하고, 해커나 개발자가 실제 코드를 바꿀 수 없도록 근본적으로 방어할 수 있는 시스템이 필요하다. 즉, 외부 해커는 물론 루트 권한을 가진 내부 관리자와 개발자도 해킹하지 못하도록 원천적으로 막는 완전히 새로운 접근법이 필요한 것이다. 바로 이

점이 블록체인, 디지털 에셋을 위한 인프라 구축 시 최우선으로 고려해야 할 가장 중요한 요건이다.

IBM LinuxONE, 현존하는 가장 강력한 보안 인프라

이와 같은 디지털 토큰 서비스 인프라의 엄격한 보안 요건을 맞추기 위해 IBM은 블록체인 디지털 자산에 특화된 LinuxONE을 공급하고 있다. IBM LinuxONE을 통해 인프라를 구축하면 외부 해커는 물론 내부의 루트 권한을 가진 관리자나 개발자의 해킹도 원천적으로 막을 수 있다.

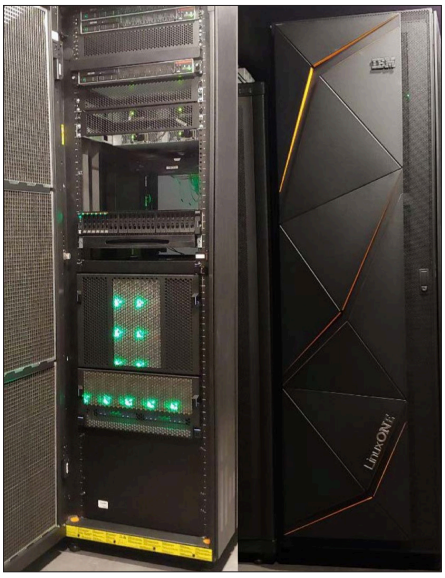
LinuxONE은 오픈소스 리눅스 전용 대형 서버로 강력한 보안 기능이 특징이다. LinuxONE에서 처리하는 애플리케이션과 데이터는 다른 어떤 솔루션보다 더 안전하다. 시스템 관리자의 접근조차 허용하지 않기 때문이다. 즉 일단 애플리케이션 이미지가 만들어지면 운영체제 액세스가 불가능하며, 원격 API를 통해서만 접근할 수 있다. 디스크는 물론 디버그 데이터까지 암호화되고 메모리 액세스도 불가능하다. 특권을 가진 사용자 계정의 오용이나 정보 유출을 원천적으로 막을 수 있다.

LinuxONE이 이처럼 강력한 보안을 제공할 수 있는 핵심 기술이 SSC(Secure Service Container)다. SSC는 거의 모든 잠재적 위험에서 데이터를 보호한다. 예를 들어 일반적인 시스템은 관리자 계정이 유출됐을 때 이를 이용해 앱 혹은 데이터에 접근할 수 있다. 그러나 LinuxONE에서는 SSC 환경에 접근할 수 없다. 또한, 다른 시스템은 데이터베이스 대부분을 암호화하지 않아 해커에 의해 수정, 변조될 수 있지만, SSC는 모든 IO를 자동으로 암호화한다. 이밖에 일반적으로 악성코드나 랜섬웨어는 소프트웨어의 취약점을 활용해 백도어로 침투하는데, SSC는 이러한 방식의 접근을 허용하지 않는다.

SSC의 장점을 가장 잘 활용하고 있는 사례가 블록체인 전문기업 인블록(INBLOCK)이다. SSC 위에 코인 데몬을 올려 운영하는 인프라를 만들었다. 인블록이 인프라를 설계할 때 가장 중요하게 검토한 것이 보안이었다. 외부 침입을 막는 것은 물론 내부자 위협에도 대응할 수 있어야 했다. 심지어 하드 디스크를 가져가도 그 데이터를 열어볼 수 없는 강력한 보안 체계를 구축하는 것이 목표였다. 여러 대안을 검토한 끝에 IBM LinuxONE을 최종 선택했다. 이를 이용해 실제 구축을 시작한 것은 지난해 6월이었고 10월에 블록체인 메인넷을 오픈했다. 현재는 여러 외부 기업과 함께 다양한 블록체인 앱, 즉 디앱(Dapp)을 개발하고 있다.

인블록이 LinuxONE을 선택한 이유는 무엇보다 IBM의 특화된 기술인 SSC였다. 작업자가 접속할 수 없는 것은 물론, 개발자조차 임의로 수정할 수 없을 만큼 강력한 보안을 제공했다. LinuxONE의 하드웨어 보안 모듈(HSM) 플랫폼도 중요한 선택 요건이었다. HSM은 미국 연방정부 정보처리 표준(FIPS) 140-2에서 가장 높은 등급인 레벨 4 인증을 받았다. 기존 타사 제품 중 레벨 3 인증을 받은 경우가 있었지만 레벨 4 인증을 받은 것은 IBM 제품이 처음이다.

레벨 4에는 가장 높은 수준의 보안 정책이 적용돼 있다. 암호 모듈 보호장치



블록체인 전문기업 인블록은 IBM LinuxONE을 이용해 디지털 토큰 서비스 인프라를 구축했다.

에 침입하려는 물리적, 전기적 시도가 있을 때 저장된 암호키를 삭제하는 것은 물론, 외부 환경의 변화를 감지한 경우에도 저장된 암호키를 폐기한다. 의도적인 환경 변화를 암호 모듈 보호장치를 무력화하려는 시도로 보기 때문이다. 이를 통해 해커는 물론 내부 사용자와 작업자에 의한 모든 위협을 막을 수 있는데, 이는 기존 칩 업체 제품이나 클라우드 업체 서비스와 비교해도 차별화된 강점이다.

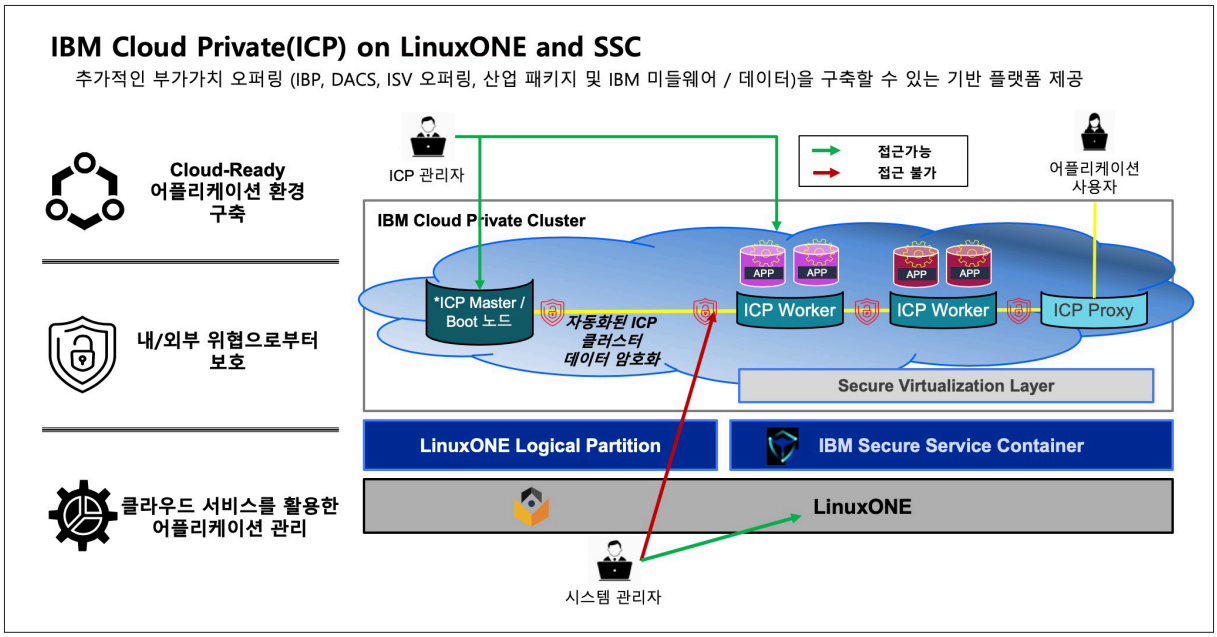
인블록은 LinuxONE을 통해 강력한 보안을 지원하는 인프라를 확보함에 따라 현재는 메타코인(Metacoin) 프로젝트로 사업 중심을 확장하고 있다. 메타코인은 오픈소스 하이퍼레저 기반의 첫 암호통화이자 플랫폼이다. 인블록은 이 메타코인 생태계에 대한 신뢰를 확보하기 위해 강력한 보안을 제공하는 LinuxONE 위에서 노드를 운용한다. 메타코인 프로젝트에는 거래소, 엔터테인먼트, 영화 제작 등 다양한 플랫폼이 들어와 있다. 최종적으로는 이러한 디지털 자산을 IBM LinuxONE에 보관하게 된다.

디지털 토큰의 보안은 아무리 강조해도 부족하다. 특히 인프라는 물론 클라우드 환경에서 유연성과 보안을 동시에 제공하는지 반드시 검토해야 한다. 클라우드 환경에서의 보안은 애플리케이션 환경 구축, 내/외부 위협으로부터 보호, 그리고 클라우드 서비스를 활용한 애플리케이션 관리가 가능해야 외부뿐만 아니라 내부 접근으로부터 안전성을 보장할 수 있다.

IBM은 SSC를 IBM Cloud Private에서도 지원해 내/외부의 위협에 의한 인프라 관리 자격 증명의 오용으로부터 데이터와 애플리케이션을 보호한다. 또한, 모든 사용자가 API를 통해서만 시스템 및 소프트웨어에 액세스할 수 있으며, 데이터가 이동 중 또는 원장에 기록될 때 모든 과정을 암호화할 수 있도록 지원한다. 이는 클라우드 상에 블록체인 플랫폼으로 디지털 토큰 환경을 구축할 때 가장 필요한 요소이며, IBM Cloud Private으로 추가적인 부가가치 오퍼링을 구축할 수 있도록 기반 플랫폼을 제공한다.

IBM Cloud Private은 특히 기업의 최신 IT 요건에 부합하는 솔루션이다. IBM Cloud Private을 이용하면 기업이 사내 IT 인프라를 그대로 유지하는 동시에, 퍼블릭 클라우드 환경의 다양한 혜택을 누릴 수 있다. 퍼블릭 클라우드와 유사한 IT 환경을 기업에 제공해 기업이 스스로 통제 가능한 사내 IT 인프라에서 컨테이너, 마이크로서비스, 오픈소스 등의 클라우드 기술을 자유롭게 활용할 수 있도록 지원한다.

이를 통해 기업은 클라우드 기반의 신규 애플리케이션을 개발하고, 기존의 애플리케이션을 클라우드로 이전해 최신 트렌드에 맞춰 재설계할 수 있다. 또한, IBM Cloud Private은 오픈소스 쿠버네티스(Kubernetes)를 기반으로 도커(Docker) 컨테이너와 클라우드 파운드리(Cloud Foundry)를 동시에 지원하므로 기존 워크로드를 IBM 클라우드를 포함하는 모든 클라우드 환경으로 손쉽게 통합, 이전할 수 있다.



IBM SSC for IBM Cloud Private은 내외부의 위협에 의한 인프라 관리 자격 증명의 오용으로부터 데이터와 애플리케이션을 보호한다.

디지털 토큰화 시대 여는 전제 조건

최근 몇 년 사이 규모가 큰 암호화폐 거래소에서 잇달아 해킹 사고가 발생하고 있다. 지난해에만 전 세계 상위 3곳이 해킹을 당했다.

앞서 언급한 B사 해킹 사건을 비롯해, 일본의 거래소인 C사에서도 580억엔 규모의 암호화폐가 유출됐다. 콜드 월렛(Cold Wallet)이 아닌 핫 월렛(Hot Wallet)에 코인을 보관해 해커가 이를 외부로 빼낼 수 있었다. 콜드 월렛은 온라인이 차단된 장비에 보관하며, 거래를 위해 별도 절차를 거쳐야 한다. 반면 핫 월렛은 온라인 상태여서 거래를 주고받을 수 있는 지갑이다. 엄청난 규모의 디지털 자산 가치를 고려하면 더 안전한 콜드 월렛에 보관해야 했다.

이런 사례를 보면 결국 보안 사고가 암호화폐, 디지털 자산의 위기가 아니라 거래소의 부주의에 의한 관리의 위기임을 알 수 있다. 즉 거래소가 데이터를 어떻게 관리하느냐에 따라 얼마든지 막을 수 있었다. 또한, 사고의 80%가 내부 소행이며, 이러한 내부적 위협은 계속 증가하거나 현재 상태를 유지할 것이라는 전망이 우세하다. 이러한 상황은 국내도 크게 다르지 않다. 현재 국내에는 200여 개 정도의 암호화폐 거래소가 있다. 그러나 10여 개를 제외하면 재정적인 측면은 물론 보안 측면에서도 안심할 수 없는 것으로 보인다.

앞으로 토큰화가 더 가속화될 것임을 고려하면 외부의 해킹은 물론 내부의 위협까지 대응할 수 있는 새로운 방식의 보안으로 눈을 돌려야 한다. 사용자에게 자신의 디지털 자산을 절대 잃어버리지 않을 것이라는 신뢰를 주는 것이야말로 디지털 토큰 서비스 인프라가 제공해야 할 가장 중요한 가치이기 때문이다. 동시에 이것은 앞으로 등장할 거대한 디지털 토큰화 시장이 현실화하는 전제 조건이기도 하다.