ISSUE ANALYSIS
제 6호 (2025. 7. 3.)

북한의 가상화폐를 이용한 자금세탁 및 외화벌이 실태

이철민
경제기술안보연구센터

www.kpiri.co.kr

한반도문제연구소
Korean Peninsula Issues Research Institute

북한의 가상화폐를 이용한 자금세탁 및 외화벌이, 새로운 위협으로 부상

이철민
경제기술안보연구센터

국제 사회의 대북 제재는 북한의 핵·미사일 개발 자금줄을 차단하는 데 중점을 두고 있다. 그러나 북한은 이러한 제재를 회피하고 외화를 벌어들이기 위해 다양한 편법을 동원하고 있으며, 그중에서도 가상화폐(Cryptocurrency)는 가장 빠르게 진화하는 수단으로 부상하고 있다. 비트코인(Bitcoin), 이더리움(Ethereum) 등의 익명성이 보장되고 추적이 어려운 가상화폐는 북한에게 제재를 우회하여 자금을 세탁하고 외화를 벌어들일 수 있는 효과적인 도구가 되고 있다.
문제는 이러한 가상화폐 기반의 사이버 범죄가 기존의 금융 시스템들을 통한 자금세탁보다 훨씬 추적하기 어렵고, 국제 공조에도 불구하고 실질적인 제재 효과를 내기 어렵다는 점이다. 북한은 해킹을 통해 가상화폐를 탈취하거나, 자체적으로 가상화폐를 채굴(mining)하고, 이를 다시 현금화하는 방식으로 막대한 외화를 벌어들이고 있으며, 이는 궁극적으로 핵·미사일 개발 자금으로 전용되고 있다는 의혹이 끊이지 않고 있다. 본 보고서는 북한이 가상화폐를 통해 자금을 세탁하고 외화를 벌어들이는 주요 방법들을 분석하고, 실제 사례를 통해 그 실태를 조명하며, 이에 대한 국제 사회와 한국의 대응 방안을 제시하고자 한다.

북한의 가상화폐 외화벌이 및 자금세탁 구조

북한은 국제 사회의 제재를 회피하고 핵·미사일 개발 자금을 확보하기 위해 다양한 경로를 통해 가상화폐를 활용하고 있다.

· 가상화폐 탈취를 통한 외화벌이

북한은 '라자루스 그룹(Lazarus Group)'으로 알려진 국가 주도 해킹 조직을 통해 전 세계의 가상화폐 거래소, 금융 기관, 개인 지갑 등을 대상으로 사이버 공격을 감행하여 가상화폐를 탈취하고 있다. 이들은 정교한 피싱(phishing) 공격, 악성코드(malware) 유포 등을 사용하여 보안 취약점을 공략한다. 유엔 전문가 패널 보고서에 따르면, 북한은 2017년부터 2023년 사이에 수십억 달러에 달하는 가상화폐를 탈취한 것으로 추정된다. 이는 북한의 핵·미사일 프로그램 자금의 상당 부분을 차지하는 것으로 분석된다.

주요사례 : 엑시 인피니티(Axie Infinity) 해킹: 2022년, 블록체인 기반 게임 '엑시 인피니티'의 개발사 스카이 마비스(Sky Mavis)가 약 6억 2천만 달러(약 8천억 원) 상당의 이더리움과 USDC(스테이블코인)를 탈취당하는 사건이 발생했다. 미국 재무부는 이 해킹의 배후로 북한의 라자루스를 지목, 이 자금은 여러 가상화폐의 믹서(mixer)를 통해 세탁된 것으로 알려졌다.

· 가상화폐 채굴 및 거래를 통한 외화벌이

비용 효율성 : 북한은 저렴한 전력 비용과 노동력을 활용하여 비트코인 등 가상화폐를 직접 채굴하는 방식으로 외화를 벌어들이는 시도를 하고 있다. 채굴된 가상화폐는 해외 거래소를 통해 현금화된다.

거래소 이용 : 북한 관련자들이 해외 가상화폐 거래소에 계정을 개설하고, 익명성을 보장하는 다크웹(Dark Web)이나 P2P(개인 간 거래) 플랫폼을 통해 가상화폐를 거래하여 자금을 세탁하고 현금화하는데 이 과정에서 여러 개의 계정을 사용하거나 타인의 명의를 도용하는 경우가 많다.

· 가상화폐 자금세탁 방법:

믹서(Mixer) 또는 텀블러(Tumbler) 활용 : 탈취 또는 채굴한 가상화폐는 추적을 어렵게 하기 위해 '믹서' 또는 '텀블러'라고 불리는 서비스를 이용한다. 이 서비스는 여러 사용자의 가상화폐를 한데 모아 섞은 뒤 다시 분산하여 전송함으로써 자금의 출처를 불분명하게 만든다.

다단계 송금 : 가상화폐를 여러 지갑 주소로 수십, 수백 차례에 걸쳐 소액으로 분할 송금하는 '레이어링(Layering)' 방식을 사용한다. 이 과정을 통해 자금의 이동 경로를 복잡하게 만들어 추적을 따돌린다.

스테이블 코인 활용 : 가격 변동성이 낮은 스테이블 코인(예: USDT, USDC)으로 전환하여 자산을 보존하고, 자금세탁 과정에서 발생할 수 있는 환율 변동 위험을 줄이는 데 활용한다. 이후 스테이블 코인을 법정화폐로 환전하거나 다른 가상화폐로 재전환한다.

OTC(장외 거래) 이용 : 규제가 덜한 장외 거래 시장을 통해 대규모 가상화폐를 현금화하여 추적을 회피한다. 이 과정에서 신분 확인 절차가 미흡한 경우가 많아 자금세탁에 용이하다.

주요 사례 및 국제 사회의 대응

· 대표적인 해킹 및 자금세탁 사례

워너크라이(WannaCry) 랜섬웨어 공격(2017년) : 전 세계를 강타한 워너크라이 랜섬웨어 공격의 배후로 북한 라자루스 그룹이 지목되었다. 이들은 비트코인을 요구하며 피해자로부터 자금을 탈취하려 시도했다.

방글라데시 중앙은행 해킹(2016년) : 국제 송금망인 스위프트(SWIFT)를 통해서 방글라데시 중앙은행에서 약 8,100만 달러를 탈취한 사건 역시 북한 라자루스 그룹의 소행으로 알려졌다. 탈취된 자금의 일부가 가상화폐로 세탁되었을 가능성이 제기되었다.

아데나(Adena) 해킹(2022년) : 2022년 3월, 암호화폐 브리지 서비스인 아데나(Harmony's Horizon bridge)에서 1억 달러 상당의 이더리움이 탈취당하는 사건이 발생했다. 미 연방수사국(FBI)은 북한 라자루스 그룹의 소행이라고 공식 발표했다. 탈취된 자금은 토네이도 캐시(Tornado Cash)와 같은 가상화폐 믹서 서비스를 통해 세탁되었다.

· 가상화폐 자금세탁의 특징

점점 더 정교해지는 수법 : 북한 해커들은 가상화폐 기술의 발전에 발맞춰 자금세탁 수법을 끊임없이 진화시키고 있다. 새로운 믹서 서비스나 익명성 코인(privacy coin)을 활용하는 등 추적을 어렵게 하는 기술을 적극적으로 도입하고 있다.

제재 회피와 연결 : 가상화폐를 이용한 외화벌이는 북한의 핵·미사일 개발을 위한 자금 확보와 직접적으로 연결되어 있다. 유엔 전문가 패널 보고서는 가상화폐 탈취가 북한의 불법 무기 프로그램 예산의 상당 부분을 충당한다고 지적한다.

· 국제 사회의 대응 노력

정보 공유 및 공조 강화 : 미국 재무부, FBI 등 주요 정보 기관들은 북한의 가상화폐 해킹 및 자금세탁 수법에 대한 정보를 전 세계 금융 기관 및 가상화폐 거래소와 공유하고 있다. 또한, 관련국들과의 공조를 통해 자금 흐름을 추적하고 차단하려 노력한다.

제재 대상 확대 : 미국은 북한과 연계된 가상화폐 주소, 믹서 서비스(예: 토네이도 캐시), 개인 등을 제재 대상에 포함하여 가상화폐 기반의 자금세탁 활동을 어렵게 만들고 있다.

가상화폐 규제 강화 : 각국 정부는 가상화폐 거래소에 대한 규제를 강화하고, 자금세탁방지(AML) 및 테러자금조달방지(CFT) 의무를 부과하여 북한과 같은 불법 행위자들이 가상화폐를 이용하기 어렵게 만들고 있다. '트래블 룰(Travel Rule)'과 같은 국제적인 규제도입을 통해 가상화폐 송금 시 발신자 및 수신자 정보를 의무적으로 확인하도록 하고 있다.

가상화폐 기반 자금세탁의 부작용 및 한계

북한의 가상화폐를 이용한 자금세탁 및 외화벌이 활동은 국제 사회에 심각한 부작용을 초래하고 있으며, 북한 자체에도 한계를 내포하고 있다.

· 국제 금융 시스템의 불안정성 증가

규제 회피 수단의 진화 : 북한의 가상화폐 활용은 국제 금융 시스템의 규제 회피 수단들이 점진적으로 진화하고 있음을 보여준다. 이는 기존의 금융 감시 체계를 무력화시키고, 국제적인 자금세탁 방지 노력에 큰 도전이 된다.

가상화폐 시장의 신뢰도 저하 : 북한과 같은 악성 행위자들의 가상화폐 이용 증가는 가상화폐 시장 전체의 신뢰도를 저하시키고, 합법적인 투자자들에게 부정적인 영향을 미칠 수 있다.

· 안보 위협의 증대

핵·미사일 개발 자금의 안정적 확보 : 가상화폐를 통한 외화벌이는 북한이 유엔 제재에도 불구하고 핵·미사일 프로그램을 지속적으로 고도화할 수 있는 자금원을 제공한다. 이는 한반도 및 국제 안보를 더욱 위협하는 요인이 된다.

사이버 안보 위협의 확산 : 북한의 해킹 활동은 단순히 가상화폐 탈취에 그치지 않고, 국가 주요 인프라 및 기업 네트워크에 대한 사이버 공격으로 이어질 수 있어 전 세계적인 사이버 안보 위협을 증대시킨다.

· 국제 사회의 대북 공조 약화 우려

제재 실효성 논란 : 가상화폐를 통한 북한의 제재 회피는 기존의 유엔 제재의 실효성에 대한 의문을 제기하며, 대북 공조를 약화시킬 수 있다는 우려를 낳는다.

추적의 어려움 : 가상화폐의 익명성과 국경을 넘는 특성으로 인해 북한의 자금세탁 활동을 추적하고 차단하는 데에는 기술적, 법률적, 그리고 국제 공조의 한계가 존재한다.

· 북한의 내부적 한계

전문 인력의 한계 : 북한은 사이버 전문가를 양성하고 있으나, 최신 가상화폐 기술과 복잡한 자금세탁 기법을 지속적으로 개발하고 적용하는 데는 내부적인 한계가 존재한다. 외부의 정보 및 기술 교류가 제한적이기 때문이다.

국제 감시망 강화 : 국제 사회의 감시망이 점점 더 강화되고, 가상화폐 추적 기술이 발전함에 따라 북한의 가상화폐 기반 외화벌이 및 자금세탁 활동은 점차 어려움에 직면할 것이다. 특정 가상화폐 믹서 서비스가 제재 대상이 되거나, 가상화폐 거래소의 규제가 강화되면 북한의 활동에 제약이 생길 수 있다.

향후 우리의 대응방안

북한의 가상화폐를 이용한 자금세탁 및 외화벌이 활동에 효과적으로 대응하기 위해서는 국제 사회의 공조 강화와 함께 다음과 같은 다각적인 노력이 필요하다.

· 정보 공유 및 분석 역량 강화

관광 수익 사용의 투명성 요구 : 국제 사회는 북한에 갈마지구 관광으로 얻는 수익의 사용처에 대한 투명한 공개를 요구해야 한다. 이 수익이 핵·미사일 개발이 아닌 주민 생활 개선에 사용될 수 있도록 국제적인 감시와 협력이 필요하다. 특히 러시아를 통한 자금 유입에 대한 국제적인 공조와 감시를 강화해야 한다.

인권 문제 개선 촉구 : 관광 사업의 활성화를 위해서는 북한의 인권 문제가 개선되어야 함을 지속적으로 촉구해야 한다. 인권 문제 해결 없이 지속 가능한 관광 산업은 어렵다. 러시아를 포함한 모든 국가의 관광객에게 동일한 기준이 적용되도록 요구해야 한다.

대북 제재 준수 압박 : 러시아를 포함한 모든 국가가 유엔 안보리 대북 제재를 철저히 준수하도록 지속적으로 압박해야 한다. 갈마지구 관광이 제재 회피 수단으로 활용되지 않도록 국제적 감시망을 강화해야 한다.

· 정보 공유 및 분석 역량 강화

사이버 위협 정보 공유 : 미국, 한국, 일본 등 주요국 간에 북한의 가상화폐 해킹 및 자금세탁 수법에 대한 정보를 실시간으로 공유하는 체계를 더욱 강화해야 한다. 이는 북한의 새로운 수법에 대한 빠른 대응을 가능하게 한다.

가상화폐 추적 기술 개발 및 활용 : 블록체인 분석 기술을 고도화하여 가상화폐의 자금 흐름을 정밀하게 추적하고, 북한과 연계된 불법 자금의 최종 목적지를 파악하는 데 주력해야 한다. 관련 기술 개발에 대한 투자를 확대해야 한다.

전문 인력 양성 : 가상화폐 분석, 사이버 포렌식, 사이버 안보 법률 전문가 등 북한의 가상화폐 위협에 대응할 수 있는 전문 인력을 양성하고, 이들을 유관 기관에 배치하여 역량을 강화해야 한다.

· 가상화폐 규제 및 제재 시스템 강화

국제 표준 규제 도입 확대 : 각국 정부는 FATF(자금세탁방지 국제기구)의 권고를 적극 수용하여 가상화폐 거래소에 대한 자금세탁방지(AML) 및 테러자금조달방지(CFT) 의무를 강화하고, '트래블 룰' 등 국제 표준 규제를 모든 가상화폐 서비스 사업자에게 적용하도록 노력해야 한다.

북한 연계 가상화폐 주소 제재 확대 : 북한과 연계된 것으로 확인된 가상화폐 지갑 주소, 믹서 서비스, 특정 가상화폐 프로젝트 등에 대한 제재 대상을 지속적으로 확대하여 북한의 자금 유통 경로를 더욱 차단해야 한다.

가상화폐 거래소의 책임 강화 : 가상화폐 거래소들이 북한 관련 불법 자금 유입을 막기 위한 내부 통제 시스템을 강화하고, 의심 거래 보고 의무를 철저히 이행하도록 강력하게 요구해야 한다. 규제 위반 시에는 강력한 제재를 부과해야 한다.

· 국제 공조 및 협력 심화

유엔 차원의 공조 강화 : 유엔 안보리 대북 제재 위원회 전문가 패널의 활동을 적극 지원하고, 북한의 가상화폐 활동에 대한 국제 사회의 공통된 인식을 형성하며, 제재 이행을 위한 각국 간의 긴밀한 협력을 유도해야 한다.

다자 및 양자 협력 채널 활성화 : 미국, 일본, 유럽연합 등 주요국들과의 사이버 안보 협력을 강화하고, 북한의 가상화폐 위협에 대한 공동 대응 방안을 논의하는 정례 협의체를 운영해야 한다.

민관 협력 강화 : 정부 기관뿐만 아니라 가상화폐 기업, 블록체인 분석 업체 등 민간 부문의 역량을 활용하여 북한의 사이버 위협에 대한 방어 체계를 구축하고, 정보 공유를 활성화해야 한다.

· 대북 메시지 강화 및 인식 제고:

불법 활동에 대한 경고 : 북한의 가상화폐를 이용한 모든 불법 활동은 국제 사회의 감시와 제재 대상이 될 것이라는 강력한 경고 메시지를 지속적으로 발신해야 한다.

대국민 인식 제고 : 일반 국민과 기업들이 가상화폐 관련 해킹 및 피싱 공격에 노출되지 않도록 사이버 보안 의식을 높이고, 주의를 당부하는 캠페인을 지속적으로 전개해야 한다.

//끝//

이 문건은 집필자 개인의 견해를 바탕으로 작성된 것으로서,
한반도 문제 연구소의 공식 입장과는 무관합니다.