eISSN 3140-409X

ISSUE BRIEF

이슈브리프 914호
(2026.11.13)

북한 IT 인력의 위장취업 시도: 국내 침투 현실화와 대응의 필요성

제914호

오일석 nusl2006@inss.re.kr
김보미 bomi@inss.re.kr



국가안보전략연구원
Institute for National Security Strategy

INSS
www.inss.re.kr

국문초록

국내에서도 북한 IT 인력이 기업에 위장 취업한 정황이 처음으로 포착되었다. 북한 IT 인력은 국적과 신분을 위장하여 국내외 기업에 취업하거나 정보기술 용역을 수주하고, 이 과정에서 신원 도용, 취업 사기, 기업정보 탈취, 가상자산 절취, 금전 갈취 및 불법 수익 이전 등 다양한 범죄를 저지르고 있다. 이들의 활동은 북한의 불법 외화벌이와 밀접하게 연결되어 있으며, 해킹을 통해 외부에서 기업의 전산망에 침입하는 기존의 사이버공격과 달리 정상적인 취업이나 용역계약을 가장해 기업 내부에 접근한다는 특징이 있다. 그동안 국내에서는 기업의 대면 근무 관행 등으로 인해 북한 IT 인력의 위장 취업 가능성이 낮게 평가되어 왔으나, 이번 사례를 계기로 국내 기업도 더 이상 안전지대가 아님이 드러났다. 이에 따라 기존의 주의보 발표와 위협정보 공유 등 예방적 대응을 넘어, 관련 범죄 네트워크를 추적하고 규명하는 수사 중심의 대응을 강화할 필요가 있다.

이를 위해 첫째, 국가정보원과 경찰청 간 정보 공유 및 수사 협력을 강화하고 경찰청 안보수사국을 중심으로 전문 수사 역량을 집중해야 한다. 둘째, 채용자료와 원격접속 기록 등 디지털 증거와 금융거래 정보를 연계한 통합수사를 통해 실제 행위자와 북한 측 조직의 연계성을 규명해야 한다. 셋째, 해외 전자증거 확보와 현지 조력자 수사, 범죄수익 추적 및 환수 등을 위한 국제공조를 강화해야 한다. 넷째, 민간기업 및 금융기관과의 협력을 통해 의심 징후의 공유와 증거보전, 자금 추적을 위한 민관협력 체계를 구축해야 한다. 마지막으로 이러한 대응을 뒷받침할 법적·제도적 기반을 정비하고 전문인력 및 예산 지원을 확대해야 한다.

키워드: 북한 IT 인력, 위장 취업, 노트북 팜, 외화벌이, 자금세탁, 통합수사, 국제공조 수사, 민관협력

국내에서도 북한의 IT 인력이 기업에 위장 취업한 정황이 처음으로 포착되어 충격을 주고 있다. 2026년 10월 22일 공개된 경찰청 자료에 따르면, 경찰은 지난해 북한 IT 인력이 국내 민간기업에 채용되어 실제 소프트웨어 개발 업무에 참여한 정황을 파악하고 수사에 착수한 것으로 알려졌다. 구체적인 경위와 관련 정보는 아직 공개되지 않았으나, 그동안 국내에서는 발생 가능성이 크지 않은 것으로 여겨졌던 북한 IT 인력의 위장 취업이 현실화되었다는 점에서 적지 않은 의미가 있다. 이는 북한의 사이버 위협이 해킹이나 정보 탈취, 가상자산 탈취 등에 국한되지 않고 국내 기업의 고용 및 업무 환경까지 침투할 수 있음을 보여주는 사례로, 관련 위협에 대한 인식 제고와 대응체계 점검이 필요함을 시사한다.

북한 IT 인력의 위장 취업 수법과 자금 이동

북한 IT 인력의 위장 취업은 최근에 드러난 새로운 사건이 아니다. 코로나19 이후 원격근무와 해외 인력 채용이 보편화된 미국 등에서는 북한 IT 인력이 신분과 국적을 위장해 외국 기업에 취업하는 사례가 지속적으로 보고되어 왔다. 2026년 10월 28일 미국 재무부 해외자산통제국은 북한 IT 인력의 위장 취업과 관련하여 불법 자금 조달에 관여한 것으로 확인된 개인 10명과 단체 1곳을 추가 제재한다고 결정하였다. 이에 앞서 10월 13일에도 미 법무부가 북한 IT 인력들의 위장 취업을 도운 미국인 2명을 체포하고 텍사스 일대 주거지에서 장비 187대를 압수했다.

북한 IT 인력은 다음과 같은 방식으로 기업에 취업하여 활동한다. 타인의 신원정보와 현지 조력자, 온라인 계정 및 원격근무 환경 등을 활용해 신분을 위장하고 해외 기업에 취업한다. 우선 실제와 다른 성명·학력·경력·연락처 및 기술역량을 기재한 허위 이력서를 작성하거나 타인의 신원정보를 도용한 뒤, 링크드인(LinkedIn)

이나 업워크(Upwork) 등 온라인 구인 플랫폼에 이를 등록한다. 이후 기업과 화상면접을 진행하거나 현지 조력자가 면접에 대신 참여하는 등의 방식으로 신원을 위장해 원격근무자로 채용된다.

채용이 확정되면 기업이 업무용으로 지급한 노트북을 해외 조력자의 거점에 설치하고, 북한 IT 인력은 원격으로 해당 장비에 접속해 개발 업무를 수행한다. 이때 해외 조력자는 기업이 지급한 노트북을 보관·관리하고 IT 인력의 원격 접속을 지원하는 역할을 한다. 이들 조력자 중에는 자신이 지원하는 인력이 북한 국적자라는 사실을 인지하지 못한 채 가담하는 경우도 있으며, 노트북 보관·관리 등의 대가로 금전적 보상을 받는 경우도 있다. 미국에서는 이처럼 여러 대의 업무용 노트북을 한곳에 모아 관리하는 시설을 '노트북 팜(laptop farm)'이라고 부르며, 일부 조력자들은 이를 운영하면서 신원을 가장한 북한 IT 인력이 미국 내에서 해당 기업에서 정상적으로 일하고 있는 것처럼 보이도록 지원하기도 한다.

북한 IT 인력들은 위장 취업이나 허위 용역계약 등을 통해 취득한 급여나 용역대금을 비트코인(BTC), 이더리움(ETH), 스테이블코인(USDT·USDC) 등 가상자산으로 전환하여 믹싱한 뒤, 서방의 규제가 닿지 않고 신원인증이 느슨한 러시아 기반 장외거래 및 가상자산거래소에서 루블화로 매도한다. 그러나 최근에는 가상자산 믹서에 대한 고강도 제재로 인해 믹싱을 전혀 거치지 않거나 이를 보완하는 다단계 범죄 네트워크 및 대체 세탁 절차를 활용하기도 한다.

해외 기업 및 공공부문으로 확산되는 위장 취업

북한 IT 인력의 위장 취업은 미국뿐 아니라 영국 등 다른 국가에서도 확인되고 있다. 영국 텔레그래프지는 북한 IT 인력들이

주로 블록체인 네트워크 및 사이버 보안 기업에 취업을 시도하고 있을 뿐만 아니라, 영국의 주요 은행과 제약회사 등도 이들의 표적이 되고 있다고 보도하였다. 다국적제재모니터링팀(MSMT)이 발표한 북한 해외 노동자 실태 보고서에 따르면, 북한 IT 인력의 활동 거점은 17개국에 걸쳐 있으며, 이들은 월평균 1만 달러의 수입을 올려 그중 약 90%를 북한으로 송금하는 것으로 파악된다. 이들이 벌어들인 외화는 궁극적으로 북한의 핵·미사일 개발 재원으로 활용되는 것으로 추정된다.

북한 IT 인력의 위장 취업은 민간기업을 넘어 공공부문과 관련된 사업에서도 적발되고 있다. 2026년 8월 미 연방수사국(FBI)은 연방정부 관련 업무를 수행하던 북한 IT 인력을 적발했다고 공개하였다. 앞서 지난해에도 메릴랜드주에 거주하는 미국인이 중국에 체류 중인 북한 국적자의 미 연방항공청(FAA) 소프트웨어 개발 계약 참여를 지원한 혐의로 징역 15개월을 선고받았다. 미국 정부기관에 직접 채용되기 위해서는 엄격한 신원조회 절차를 거쳐야 한다는 점에서, 이들은 정부가 발주한 사업을 수주한 민간기업의 계약직 인력으로 참여했을 가능성이 크다. 직접적인 정부기관 취업 여부와 관계없이, 이들이 정부 관련 사업에 참여하면서 주요 시스템이나 관련 정보에 접근할 가능성이 있다는 점은 주목해야 할 대목이다.

이처럼 북한 IT 인력의 위장 취업은 해외 노동시장에 침투해 외화를 획득하는 동시에 기업 내부정보와 기술에 접근할 수 있는 복합적인 활동으로 볼 수 있다. 과거 북한의 사이버 활동이 외부에서 기업이나 금융기관의 전산망을 공격해 정보와 자금을 탈취하는 방식에 주로 의존했다면, 위장 취업은 합법적인 고용관계를 가장해 조직 내부로 직접 진입한다는 점에서 차이가 있다. 즉, 외화벌이를 위한 취업 활동 자체가 기업 내부망과 업무 시스템에 접근할 수

있는 통로가 되며, 이를 통해 기업정보 수집과 기술 탈취 등 추가적인 목적까지 추구할 수 있다. 실제로 북한 IT 인력이 취업한 다음 기업의 내부 정보를 탈취하여 경영진을 협박하고 금전을 갈취하거나, 내부 시스템을 장악하고 랜섬웨어를 유포하여 대가를 취득한 사례도 있다. 따라서 북한 IT 인력의 위장 취업은 단순한 제재 회피나 불법 외화 획득의 문제를 넘어 기업의 인적 보안과 내부정보 보호 차원에서도 대응해야 하는 문제이다.

AI를 활용한 신원 위장과 채용 검증의 한계

북한 IT 인력의 위장 취업에는 타인의 신원정보를 도용하는 방식뿐 아니라 미국 내 현지 조력자를 활용하는 방식도 동원된다. 신원 도용 피해자는 자신의 명의로 금융계좌를 개설하거나 정상적인 경제활동을 하는 데 어려움을 겪을 수 있으며, 경우에 따라서는 취업에 제약이 있는 범죄 전력자 등이 북한 IT 인력의 위장 취업을 돕는 조력자로 가담하기도 한다.

최근에는 AI와 얼굴 변조 기술(face-swapping)의 발전으로 신원 위장 수법도 더욱 정교해지고 있다. 북한 IT 인력 수십 명이 챗GPT 유료 계정을 공유하며 영국 기업들의 면접 질문 족보를 실시간으로 학습하는 한편, 영문 이력서와 포트폴리오를 완벽하게 작성하기도 한다. 화상면접에서는 얼굴을 실시간으로 바꾸는 기술(face-swapping)이나, 보이스 변조 AI 기술을 활용해 실제 신원과 다른 인물로 위장하기도 한다. 이처럼 AI 기술은 북한 IT 인력의 신원 위장을 용이하게 하고 해외 기업 취업을 통한 외화 획득을 더욱 수월하게 만드는 수단으로 활용되고 있다.

미 FBI는 북한 IT 인력들의 위장 취업을 방지하기 위한 구체적인 대응 방안도 제시하고 있다. 우선 여러 지원자의 이력서에서

동일한 연락처나 유사한 경력·기술 정보가 반복적으로 발견되는 경우 이를 의심스러운 징후로 간주하고, 지원자의 학력과 경력을 독립적으로 확인하도록 권고한다. 화상면접에서는 지원자에게 카메라를 회전시켜 주변 환경을 보여주거나 손을 흔드는 등 특정 동작을 요구함으로써 얼굴 변조 기술의 사용 여부를 확인하는 방법도 제안하고 있다. 다만 이러한 기술적 검증만으로 신원 위장을 완전히 차단하기는 어렵다는 점에서, FBI는 대면 면접을 실시할 것을 권고하고 있다.

국내 위장 취업 사례의 의미와 대응 방안

그동안 국내에서는 기업의 대면 근무 관행과 실제 근무지에서 업무를 수행하는 구조 등으로 인해 북한 IT 인력의 위장 취업이 상대적으로 어려운 것으로 인식되어 왔다. 이 때문에 다른 사이버 위협에 비해 위장 취업 문제는 크게 주목받지 못했다. 그러나 이번 사례는 북한 IT 인력의 활동이 국내 노동시장과 기업의 업무 환경으로까지 확대될 수 있음을 보여준다.

북한 IT 인력의 위장 취업은 단순한 신분 위장을 넘어 신원 도용, 취업 사기, 기업정보 탈취, 가상자산 절취, 금전 갈취 및 불법 수익 이전 등 다양한 범죄로 이어진다. 특히 정상적인 취업과 용역계약을 가장해 기업 내부에 접근한다는 점에서 외부에서 전산망에 침입하는 기존의 사이버공격과 구별된다. 따라서 외화 획득과 제재 회피뿐 아니라 기업의 내부정보 보호와 인적 보안 차원에서도 대응할 필요가 있다.

우리 정부는 2022년 12월 8일 북한 IT 인력의 활동 방식과 신원 위장 수법을 알리고 국내 기업의 신원확인 강화를 요청하는 정부 합동주의보를 최초로 발표하였다. 이후 2023년 한·미 공동주의보,

2025년 한·미·일 공동성명, 2026년 7월 10개국 공동주의보 등을 통해 북한 IT 인력의 새로운 취업 수법과 AI 활용 실태를 알리고 기업의 예방 조치를 촉구해 왔다.

그러나 주의보 중심의 대응만으로는 위장 취업을 실질적으로 차단하는 데 한계가 있다. 기업이 주의보에 제시된 의심 징후와 예방 조치를 실제 채용 및 용역계약 과정에 반영하지 않으면 실효성을 확보하기 어렵다. 더욱이 북한 IT 인력은 신원이 식별되더라도 새로운 가명과 제3국 신원정보, 현지 조력자 및 위장 기업 등을 활용해 활동을 지속할 수 있다. 따라서 기존의 예방적 대응을 유지하되, 국내에서도 관련 범죄 정황이 확인된 만큼 범죄 네트워크를 추적하고 실체를 규명하는 수사 중심의 대응을 강화해야 한다.

이를 위해서는 우선 국가정보원과 경찰청 간 정보 공유 및 수사 협력을 확대할 필요가 있다. 국가정보원이 북한 IT 인력의 활동과 관련 조직에 관한 정보를 수집·분석하고, 경찰청이 이를 토대로 국내 위장 취업 및 관련 범죄를 수사하는 방식으로 양 기관의 역할을 연계할 수 있다. 이를 위해 양 기관이 참여하는 '북한 IT 인력 범죄 대응 정보·수사 전담반'을 구성하고 정기적인 정보 공유와 공동 대응을 추진하는 방안도 고려할 수 있다.

둘째, 경찰청 안보수사국을 중심으로 수사 역량을 집중하고 디지털 증거와 금융 증거를 연계한 통합수사를 강화해야 한다. 위장 취업은 신원 도용, 원격 접속을 통한 업무 수행, 급여 및 용역 대금의 불법 이전 등 여러 단계에 걸쳐 이루어진다. 따라서 채용자료, 원격접속 기록, 업무용 장비의 포렌식 결과, 금융거래 및 통신 기록 등을 종합적으로 분석해 실제 행위자와 북한 측 조직의 연계성을 규명할 필요가 있다.

셋째, 실효성 있는 국제공조 수사 체계를 구축하고 실제 수사 과정에서 작동시켜야 한다. 공동주의보 발표와 위협정보 공유를 넘어, 해외 전자증거의 신속한 보전·확보, 현지 조력자에 대한 병행수사, 금융정보 교환, 범죄수익 추적 및 환수 등 구체적인 수사 공조를 강화해야 한다. 북한 IT 인력의 활동은 여러 국가에 걸쳐 이루어지는 만큼 국내 수사만으로 범죄 네트워크의 전모를 파악하고 자금 흐름을 차단하는 데 한계가 있기 때문이다.

넷째, 민관협력을 강화해야 한다. 북한 IT 인력의 위장 취업을 식별하고 증거를 확보하려면 수사기관의 강제수사 및 분석 역량과 민간기업의 기술정보·증거보전 능력, 금융기관의 자금 추적 역량을 유기적으로 결합해야 한다. 특히 기업이 채용 및 용역계약 과정에서 발견한 의심 징후를 수사기관과 신속하게 공유하고 관련 자료를 보전할 수 있도록 협력체계를 마련해야 한다.

마지막으로 대응을 뒷받침할 법적·제도적 기반을 정비하고 예산 지원을 확대해야 한다. 북한 IT 인력의 위장 취업은 국내외 여러 주체가 연루되는 복합 범죄인 만큼, 기관 간 정보 공유와 공동 수사, 해외 수사기관과의 공조, 범죄수익 환수 등이 원활하게 이루어지도록 관련 제도를 보완해야 한다. 아울러 디지털 포렌식과 금융 추적, 국제공조 수사에 필요한 전문인력과 예산을 확보해야 할 것이다.

//끝//

본 내용은 집필자 개인의 견해이며,
국가안보전략연구원의 공식입장과는 다를 수 있습니다.