公益財団法人日本国際問題研究所

研究レポート

「朝鮮半島情勢とリスク」研究会「北朝鮮核・ミサイルリスク」部会 2026-1 号　2026 年 3 月 30 日

サイバー空間における北朝鮮の制裁回避と多層的対抗策の必要性

竹内 舞子　経済産業省コンサルティングフェロー

はじめに

国連安保理による北朝鮮制裁は機能しているのか。北朝鮮制裁をめぐる現状は、この問いに集約されるといってよい。制裁は、北朝鮮の核・ミサイル開発に必要な機微物資や資源の移転を抑止し続けている。しかし、現行の制裁体制が確立した 2017 年以降、北朝鮮は制裁回避策として、物理的移動に頼らないサイバー空間上の活動を拡大している。同時に、このような活動には技術的・法的な対抗手段も存在しており、それを利用した多層的な対抗策を整備することが制裁の実効性を左右する鍵となる。

サイバー空間上の活動による資金獲得

北朝鮮がサイバー空間上で行う制裁回避の中核は、サイバー攻撃や IT 技術者のリモートワークなどを通じた資金獲得である。北朝鮮による暗号資産の窃取額は、2025 年に約 20 億ドル、2024 年に約 13 億ドルであったとされる [1]。また、数千人の IT 技術者が海外に派遣され、その平均月収は 1 万ドルに上り、2024 年には年間総額で最大 8 億ドルを政府にもたらした可能性がある [2]。これに対し、北朝鮮の統計上の輸出額は 2024 年から 2025 年にかけて年間約 5 億～6 億ドルにとどまっている。また、2010 年代半ばに北朝鮮が工場などに約 10 万人の労働者を派遣して得ていた額が約 5 億ドルであった。こうした比較から、サイバー空間上での活動は効率的な外貨収入源であり、国家として注力していることがうかがえる。

ただし、暗号資産は法定通貨と異なり、取得して直ちに調達に利用できるわけではない。北朝鮮が暗号資産を調達に利用するための典型的な手段としては、窃取した暗号資産の場合には、少額ずつ多数のウォレットに分散し、ミキサーなどを用いて匿名

化した後、「OTC（Over-the-Counter）ブローカー」と呼ばれる非公開の暗号資産交換業者や規制の弱い取引所などで現金化した後、調達に使用するか、公式・非公式の金融ネットワークを通じて移転することとなる。

安保理決議の課題と有志国による活動

現行の安保理決議にも、暗号資産の窃取や IT 技術者のリモートワークに適用できる措置は含まれている。しかし、その履行には課題もある。第一に、暗号資産の決議における位置づけが明確でない。2024 年まで決議の履行を監視していた安保理北朝鮮制裁委員会専門家パネルは、決議に暗号資産に関する明文の規定がないために、決議の履行における扱いが各国によって異なるリスクを指摘している[3]。しかし、北朝鮮制裁では資産凍結の対象となる資産（Asset）はあらゆる形態を含むとされているため、暗号資産もその対象になると解釈できる[4]。また、北朝鮮のハッカーは朝鮮人民軍偵察総局、IT 技術者は軍需工業部や国防省、国家保衛部、原子力工業省、39 号室といった安保理制裁対象組織やその傘下組織に所属している[5]。そのため、こうしたハッカーや IT 技術者とその所属組織は制裁指定対象団体の傘下にあるので資産凍結の対象であり、それらへの支払いは禁止される。また、ハッカーや IT 技術者が第三国にいる場合は北朝鮮への送還対象となる[6]。また、制裁対象とされていない組織であっても、北朝鮮において IT 関連あるいは海外での活動は厳格に制限されていることから、政府や朝鮮労働党の管理又は指示の下で活動しているとみることができる。そのため、このような組織の資産は、北朝鮮政府や朝鮮労働党の指示の下で活動する団体が直接または間接的に所有または管理する資産として資産凍結の対象になると解釈し得る[7]。

しかし、安保理の決議はただちに各国の国民や法人に適用されるわけではなく、各国が履行のための国内法を制定してはじめてその国の国民や法人に適用可能になる。そのため、暗号資産が資産凍結の対象に含まれるか、また、制裁対象として指定されていない団体や個人が北朝鮮政府や朝鮮労働党、その他の制裁対象団体の管理下にあると認定して制裁措置を適用するかは各国国内法の規定や執行に依存する。

第二の問題は、リモートワークによる就労の扱いである。北朝鮮国内からの業務については、海外での就労を禁止する制裁措置が適用できない（ただし、前述のとおり支払いは禁止し得る）。決議が各国に課しているのは、北朝鮮国民の就労の禁止と、自国内に所在する北朝鮮労働者の送還である。そのため、北朝鮮国内から行われるリモートワークは、これらいずれの義務にも該当しない可能性がある。

このような問題に対処するためには、本来は、安保理決議において暗号資産が資産凍結の対象であることを規定するとともに、サイバー攻撃に関与する個人・団体に対する制裁指定を行うことが必要である。しかし、現在の分裂した情勢下で機能不全に陥っている安保理が制裁強化を進める可能性は低い。

このため、日米韓をはじめとする有志国による活動が重要となる。まず、サイバー空間上の活動に関しても現行の制裁に基づく措置を履行していくことで、当該活動は現行の制裁の対象となるという解釈と履行を国際的なスタンダードとして普及させていくことが求められる。また、2024 年に北朝鮮制裁委員会専門家パネルの任期終了を受けて創設された多国間制裁監視チームの枠組みも活用しつつ、制裁の履行状況の監視・公表や独自制裁を行うことが重要な措置となる。このような有志国の活動は単に安保理や専門家パネルの代替的措置にとどまるものではなく、むしろ、情報収集能力と国際的影響力を有する国々による迅速かつ実効的な対応の先駆けとなる枠組みにもなる。

サイバー分野独自の対抗策

また、制裁回避のための暗号資産の利用は金融制裁における新たな課題でもあるが、同時に、新たな監視手段も提供している。例えば、暗号資産はブロックチェーン上で追跡可能である。そして一般的には、物資の調達のためには上述の通り窃取した暗号資産を法定通貨に換える必要がある。加えて、北朝鮮のサイバー攻撃は、高度な技術に依存するものではなく、ソーシャルエンジニアリング（内部関係者からの情報収集）や脆弱性が利用される。そのため、職員への教育やシステムの脆弱性の確認を含むセキュリティ対策の強化により抑止が可能である。

さらに、IT 技術者の雇用防止には、企業と政府の双方による対応が不可欠である。企業の側では契約時の身元確認を厳格に行うとともに、面接を含む応募者とのやり取りの中で偽装を見抜くことが求められる。そのため、警戒情報が事前に共有され、各人が北朝鮮の手法を認識しているか否かによって対応には大きな差が生じる。その点では、日本政府が実施している注意喚起は有効な手段といえる。また、このような情報提供に加えて、政府は、自国内で IT 技術者の活動を支援する協力者を摘発する必要がある。

加えて、安保理における活動が停滞する中で北朝鮮制裁への関心も薄れがちな状況で、サイバー関連の話題は一般の関心を集めやすく、報道を通じて改めて北朝鮮制裁への関心を高める契機となる。また、サイバー攻撃や IT 技術者の雇用は国家や企業にとって直接の脅威であり、対策を講じるインセンティブが働く。実際に、この分野では、サイバーセキュリティやブロックチェーン分析を担う民間企業が大きな役割を果たしており、変化の速い状況に対し継続的な監視が行われている。

暗号資産を用いた資金獲得や制裁回避は北朝鮮に限られた問題ではなく、ロシアやイラン、ベネズエラによる利用を含め、国際安全保障上の課題となっている。このため、北朝鮮の行動の分析や対応策の検討を通じて、他国による制裁回避行動への対抗策にも応用可能な知見を得ることができる。ただし、サイバー空間上の活動には各国ごとの特性があるので、その適用には個別の状況を踏まえる必要がある。

米国の多層的対抗策にみる可能性と課題

北朝鮮による制裁回避への対抗策を検討するにあたり、制裁、法執行、資産没収、注意喚起といった多層的な対応を展開している米国の取組は、重要な示唆を与える。第一に、米国は、財務省外国資産管理室（Office of Foreign Assets Control、以下 OFAC）による制裁指定により、サイバー空間上の制裁回避に関与する個人・団体に対して資産凍結や米国民・企業との取引禁止措置を課している。この制裁には、制裁対象に北朝鮮以外の国民や団体も多く含まれること、また（本来米国法が及ばない）非米国人が制裁対象者との取引を行った場合に制裁の対象となり得る二次制裁の枠組みを通じて非米国人にも制裁の抑止効果を及ぼしている点が特徴である。

第二に、IT 技術者が所在地や身元を偽って働くには、第三国に設置されたコンピューター端末へのリモート接続や、第三国の個人情報の利用といった支援が必要となる。米国政府は、米国内で、あるいは米国市民の個人情報を利用して支援を行う協力者への対応を重視し、司法省と連邦捜査局（Federal Bureau of Investigation、以下 FBI）が共同で摘発を進めている。米国人以外も対象となっており、最近では、北朝鮮 IT 技術者による米国内の端末を利用したリモート業務を支援したウクライナ人がポーランドで逮捕され、身柄を米国に引き渡され 2026 年に有罪判決を受けた [8]。

第三に、米国は、窃取された暗号資産の没収を実施しており、これは法的措置と技術的措置の双方に基づく。法的措置としては、米国政府は、窃取された暗号資産がロンダリングされる過程で、米国の取引所等を経由した場合、これを根拠に管轄権を行使し、犯罪収益として民事没収の対象とする[9]。技術的には、ブロックチェーン上の取引記録や、複数のウォレットの資金移転の分析を通じて北朝鮮が利用しているウォレットを特定し、裁判所の命令に基づき民事没収手続きを行い、暗号資産の差し押さえと返還を行う。暗号資産は秘密鍵（private key）により管理されるので、当局が秘密鍵を確保した場合には、ウォレットから直接資産を回収することも可能である。

第四に、米国はサイバー犯罪に関する注意喚起を継続的に行っている。例えば FBI は、2025 年には北朝鮮 IT 技術者のリモートワークに関する警告を発出し、2026 年には北朝鮮のハッカーグループによるシンクタンクや専門家を標的としたサイバー攻撃に対する注意喚起を行っている[10]。北朝鮮 IT 技術者の採用を防ぐには、採用者が偽装を見抜く必要があるし、組織へのサイバー攻撃でも、関係者が攻撃の足掛かりとして標的になる。そのため、こうした注意喚起を通じたセキュリティ意識の向上は極めて重要である。

技術と法の課題：ミキサー規制を巡る議論

しかし、このような対応が進む中で、暗号資産ならではの新たな課題も明らかになっている。トルネードキャッシュ（Tornado Cash）に対する制裁は、技術面・法律面双方からミキサーへの対応の難しさを示す象徴的事案である。
トルネードキャッシュは、北朝鮮による大規模サイバー攻撃で得られた暗号資産の匿名化に利用されたことから、2022 年に OFAC の制裁対象となった。また、3 人の創設者のうち、1 名は 2023 年に米国で、1 名は 2022 年にオランダで逮捕され、後に有罪判決を受けた（もう 1 名は起訴されたが逃亡中）。

しかし、このような措置によってもトルネードキャッシュのサービスを停止することはできなかった。技術的な問題として、このサービスはコードが変更できない、自律的に処理を続けるスマートコントラクトであり、管理する主体を持たない。さらに、2024 年には、トルネードキャッシュの利用者らによる OFAC の制裁指定の無効を求める訴訟の控訴審で、米国第 5 巡回区控訴裁判所は、スマートコントラクトは技術であり財産には当たらないとして、OFAC の制裁はその権限を逸脱していると判示した。OFAC はこれを受けて 2025 年にトルネードキャッシュに対する制裁指定を解除した[11]。

加えて、2026 年には、米国財務省によるミキサーへの評価にも変化がみられ、違法行為に利用されるサービスという位置づけから、プライバシー確保のための合法的な手段としての側面も公式に示された[12]。

おわりに

北朝鮮は、新たな技術などを巧みに取り入れながら、サイバー空間上の活動による制裁回避を継続していくだろう。そのため制裁の実効性確保のための重要課題として、これに対処することが必要である。また、北朝鮮の活動の分析は、他国に対する制裁措置に対しても重要な示唆を与える取組でもある。したがって、政府としては、民間のリソースも活用しつつ、制裁回避の手法に関する分析や対応策の検討を推進する必要がある。

同時に、こうした活動の抑止のための国際的連携も不可欠である。将来的には、安保理において暗号資産を資産凍結の対象として明確に位置付けるとともに、サイバー空間上の活動に関与する個人・団体の制裁指定を行うことが必要である。しかし、有志国においては、安保理での進展を待つことなく、既存の制裁枠組みに基づく対応を通じて、サイバー空間上の活動も現行の制裁体制下で制限可能だという解釈と履行を国際的に確立していくことが求められる。また、多国間制裁監視チームの枠組みなども活用しつつ、暗号資産を利用した制裁回避に関する情報共有や共同対応を継続すべきである。

北朝鮮によるサイバー空間上の活動の標的になるのはすべての企業や個人である。政府がこれに対処するのは容易ではない。しかし、暗号資産やリモートワークを利用した活動には暗号資産の取引の追跡のように、固有の対抗策も存在する。また、国内の協力者の摘発も効果がある。さらに、北朝鮮の手法に関する注意喚起を継続的に行い、企業や個人のセキュリティ対策の支援を行うことも不可欠である。制裁の枠組みを維持しつつ、各国においても多層的な対抗策を取ることが、今後の北朝鮮制裁の実効性をも左右する。

制裁の文脈では経済的な面に注目が集まるが、北朝鮮のサイバー攻撃は、機微情報の収集や対外世論工作にも利用されており、さらにはテロ攻撃に使われるリスクもある。政府はこのような安全保障上の脅威にも警戒する必要がある。加えて、サイバー空間上の活動に注目が集まる中でも、物理的な密輸や労働者派遣のリスクが減少したわけではない。むしろ、サイバー空間上の活動による外貨獲得に加え、国境間往来の正常化やロシアとの関係緊密化により、物資の調達や海外での不法就労のリスクは高まっている。日本政府としては、北朝鮮をめぐる外交・安全保障上必要な措置を省庁横断的に推進することが求められる。

（2026 年 3 月 25 日校了）

---

[1] Chainalysis, *The 2026 Crypto Crime Report*, 2026.

[2] Multilateral Sanctions Monitoring Team, *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities*, October 22, 2025, https://msmt.info/Publications/detail/MSMT%20Report/4221.

[3] UN Security Council, *Midterm report of the Panel of Experts submitted pursuant to resolution 2515 (2020), S/2020/840, 28 August 2020,* para. 149, n. 96.

[4] 国連安保理決議第 2270 号 12。

[5] Multilateral Sanctions Monitoring Team, *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities.*

[6] 国連安保理決議第 2270 号 13。

[7] 国連安保理決議第 2270 号 32。

[8] United States Attorney's Office, District of Columbia, "Ukrainian National Sentenced in 'Laptop Farm' Scheme That Generated Income for North Korean IT Workers," February 19, 2026, https://www.justice.gov/usao-dc/pr/ukrainian-national-sentenced-laptop-farm-scheme-generated-income-north-korean-it-workers.

[9] 米国の民事没収は、違法行為に関連したものと考えられる資産を、犯人が特定できなくても没収できる制度である。

[10] Federal Bureau of Investigation, "North Korean IT Worker Threats to U.S. Businesses," July 23, 2025, https://www.fbi.gov/investigate/cyber/alerts/2025/north-korean-it-worker-threats-to-u-s-businesses;

Federal Bureau of Investigation, “North Korean Kimsuky Actors Leverage Malicious QR Codes in Spearphishing Campaigns Targeting U.S. Entities,” January 08, 2026, https://www.ic3.gov/CSA/2026/260108.pdf.

[11] U.S. Department of the Treasury, “Tornado Cash Delisting,” March 21, 2025, https://home.treasury.gov/news/press-releases/sb0057.

[12] U.S. Department of the Treasury, *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets, (Washington D.C., 2026),* p.8, https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.