Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration

The United States, Japan, and the Republic of Korea join together to provide a new warning to the blockchain technology industry regarding the ongoing targeting and compromise of a range of entities across the globe by Democratic People's Republic of Korea (DPRK) cyber actors. The DPRK's cyber program threatens our three countries and the broader international community and, in particular, poses a significant threat to the integrity and stability of the international financial system. Our three governments strive together to prevent thefts, including from private industry, by the DPRK and to recover stolen funds with the ultimate goal of denying the DPRK illicit revenue for its unlawful weapons of mass destruction and ballistic missile programs.

The advanced persistent threat groups affiliated with the DPRK, including the Lazarus Group, which was designated by the relevant authorities of our three countries, continue to demonstrate a pattern of malicious behavior in cyberspace by conducting numerous cybercrime campaigns to steal cryptocurrency and targeting exchanges, digital asset custodians, and individual users. In 2024 alone, our governments have individually and jointly attributed multiple thefts, denominated in virtual asset value in U.S. dollars, to the DPRK: DMM Bitcoin for $308 million, Upbit for $50 million, and Rain Management for $16.13 million. The United States and Republic of Korea additionally attribute to the DPRK, based on detailed industry analysis, thefts last year against WazirX for $235 million and Radiant Capital for $50 million.

As recently as September 2024, the United States government observed aggressive targeting of the cryptocurrency industry by the DPRK with well-disguised social engineering attacks that ultimately deploy malware, such as TraderTraitor, AppleJeus and others. The Republic of Korea and Japan have observed similar trends and tactics used by the DPRK.

Additionally, agencies from our governments have published multiple notifications on the DPRK information technology (IT) workers that also present an insider threat to private sector partners: the United States on 16 May 2022 and 16 May 2024, the United States and the Republic of Korea on 18 October 2023, the Republic of Korea on 8 December 2022, and Japan on 26 March 2024. The United States, Japan, and the Republic of Korea advise private sector entities, particularly in blockchain and freelance work industries, to thoroughly review these advisories and announcements to better inform cyber threat mitigation measures and mitigate the risk of inadvertently hiring DPRK IT workers.

Deeper collaboration among the public and private sectors of the three countries is essential to proactively disrupt these malicious actors' cybercrime operations, protect private business interests, and secure the international financial system. Cooperative public-private efforts in the United States through the Illicit Virtual Asset Notification (IVAN) information sharing partnership, the Cryptoasset and Blockchain Information Sharing and Analysis Center (Crypto-ISAC), and the Security Alliance (SEAL) are examples of newly established mechanisms to facilitate information sharing and incident response. The Republic of Korea and the United States also co-host a series of public-private symposiums to strengthen coordination between the government and private sector in disrupting the DPRK's illicit revenue generation, including on 17 November 2022, 24 May 2023, and 27 August 2024. In Japan, the Financial Services Agency, in collaboration with the Japan Virtual and Crypto Assets Exchange Association (JVCEA), warned relevant businesses about the risk of crypto-asset thefts and requested self-inspections on 26 September and 24 December 2024.

The United States, Japan, and the Republic of Korea will continue to work together to counter the DPRK's malicious cyber activities and illicit revenue generation, including by imposing sanctions on DPRK cyber actors and collaborating to improve cybersecurity capacity across the Indo-Pacific region. The United States, Japan, and the Republic of Korea reaffirm their commitment to combatting cyber threats posed by the DPRK and enhancing their coordination through the trilateral working groups.

（仮訳）

北朝鮮による暗号資産窃取及び官民連携に関する共同声明

2025 年 1 月 14 日

米国、日本及び韓国は、北朝鮮のサイバーアクターによる、世界中の様々な組織に対する進行中の標的型攻撃及び侵害に関し、ブロックチェーン技術産業に対して、新たな注意喚起を共同で提供する。北朝鮮によるサイバー計画は、我々三か国及びより広範な国際社会を脅かし、特に国際金融システムの健全性及び安定性に重大な脅威をもたらすものである。我々三か国の政府は、北朝鮮による違法な大量破壊兵器及び弾道ミサイル計画のための不法な資金を途絶するとの最終的な目標の下、民間企業からのものを含め、北朝鮮による窃取を防ぎ、窃取された資産を回復するために共に努力する。

三か国の関連当局により資産凍結等の措置の対象に指定されたラザルス・グループを含む、北朝鮮傘下の高度で持続的な脅威（APT）グループは、暗号資産を窃取するために多数のサイバー犯罪を行い、取引所、デジタル資産の保管者及び個人ユーザーを標的にすることにより、サイバー空間において悪意のある行動パターンを示し続けている。2024 年だけでも、三か国の政府は、暗号資産の米ドル換算で、DMM Bitcoin からの 3 億 800 万米ドルの窃取、Upbit からの 5,000 万米ドルの窃取、Rain Management からの 1,613 万米ドルの窃取といった、複数の窃取事案に関し、個別に又は共同で北朝鮮に帰属すると結論付けた。加えて、米国及び韓国は、詳細な民間の分析に基づき、昨年の、WazirX からの 2 億 3,500 万米ドルの窃取及び Radiant Capital からの 5,000 万米ドルの窃取についても、北朝鮮に帰属すると結論付ける。

最近では、2024 年 9 月に、米国政府は、北朝鮮による、TraderTraitor、AppleJeus、その他のマルウェアを最終的に展開する巧妙に偽装されたソーシャルエンジニアリング攻撃による暗号資産業界に対する積極的な標的型攻撃を観測した。韓国及び日本は、北朝鮮の同様の傾向及び戦術を観測してきている。

さらに、我々の政府機関は、民間部門のパートナーに対するインサイダー脅威となる北朝鮮 IT 労働者に関する複数の文書を公表しており、米国は 2022 年 5 月 16 日及び 2024 年 5 月 16 日に、米国及び韓国は 2023 年 10 月 18 日に、韓国は 2022 年 12 月 8 日に、日本は 2024 年 3 月 26 日に公表してきている。米国、日本及び韓国は、民間企業、特にブロックチェーン業界及びフリーランス業界の民間企業に対し、サイバー脅威の緩和策をよりよく理解し、北朝鮮 IT 労働者を不注意に雇用してしまうリスクを軽減するためのこれらのアドバイザリ及び発表を十分に見直すよう勧告する。

三か国のより深化した官民連携は、これらの悪意のあるアクターによるサイバー犯罪活動を能動的に阻止し、民間ビジネスの利益を守り、国際金融システムを守るために不可欠である。違法暗号資産通知（IVAN）情報共有パートナーシップ、暗号資産及びブロックチェーン ISAC（Crypto-ISAC）、セキュリティアライアンス（SEAL）を通じた米国における官民協力の取組は、情報共有とインシデント・レスポンスを促進するために新たに設立されたメカニズムの例である。韓国及び米国は、また、北朝鮮による不法な資金調達を阻止するための政府と民間部門の連携を強化するため、2022 年 11 月 17 日、2023 年 5 月 24 日及び 2024 年 8 月 27 日に実施されたものを含む一連の官民合同シンポジウムを共催した。日本においては、金融庁が日本暗号資産等取引業協会（JVCEA）と連携し、2024 年 9 月 26 日及び 12 月 24 日に、関連企業に対して暗号資産窃取のリスクに関する注意喚起を行い、また、自主点検を要請した。

米国、日本及び韓国は、北朝鮮のサイバーアクターに対する制裁を課すことやインド太平洋地域におけるサイバーセキュリティ能力の向上に向けた連携によるものを含め、北朝鮮の悪意のあるサイバー活動及び不法な資金調達に対抗するために引き続き共に取り組む。米国、日本及び韓国は、北朝鮮によるサイバー脅威に対抗し、日米韓ワーキンググループを通じて連携を強化するとのコミットメントを再確認する。