Joint Statement on North Korean Information Technology Workers

Japan, the United States, and the Republic of Korea remain united in our efforts to counter the threat posed by North Korean IT workers. North Korea continues to dispatch its IT workers around the world to generate revenue, which funds its unlawful weapons of mass destruction (WMD) and ballistic missile programs, in violation of UN Security Council resolutions (UNSCRs). Japan, the United States, and the Republic of Korea express serious concerns over the evolving malicious activities of North Korean IT workers.

North Korean IT workers use a variety of techniques to disguise themselves as non-North Korean IT workers with false identities and locations, including by leveraging AI tools as well as cooperating with foreign facilitators. They take advantage of existing demands for advanced IT skills to obtain freelance employment contracts from an expanding number of target clients throughout the world, including in North America, Europe, and East Asia. North Korean IT workers themselves are also highly likely to be involved in malicious cyber activities, particularly in the blockchain industries. Hiring, supporting, or outsourcing work to North Korean IT workers increasingly poses serious risks, ranging from theft of intellectual property, data, and funds to reputational harm and legal consequences.

In this context, our three countries have taken coordinated actions to disrupt the North Korean IT worker threat. Today, Japan issues an update to its previous alert to provide detailed information on new tradecraft used by North Korean IT workers, and advises private sector entities to mitigate the risk of inadvertently hiring, supporting, or outsourcing work to North Korean IT workers. The United States is designating four entities and individuals furthering North Korean IT worker schemes, including in Russia, Laos, and China. The Republic of Korea issued advisories on North Korean IT worker activities to help companies avoid being targeted or victimized.

On August 26, our three countries hosted an event in Tokyo in partnership with Mandiant to improve public-private partnership and support international industry collaboration in the fight against North Korean exploitation.

Japan, the United States, and the Republic of Korea reaffirm their commitment to enhancing their coordination among the three countries, and deepening collaboration between the public and private sector to counter malicious cyber activities and illicit revenue generation by North Korea.

北朝鮮 IT 労働者に関する共同声明

日本、米国及び韓国は、北朝鮮 IT 労働者がもたらす脅威に対処するための取組において結束し続けている。北朝鮮は、国連安全保障理事会決議に違反して、不法な大量破壊兵器（WMD）及び弾道ミサイル計画の資金源となる収入を生み出すために、IT 労働者を世界中に派遣し続けている。日本、米国及び韓国は、北朝鮮 IT 労働者による進化する悪意ある活動に対して、深刻な懸念を表明する。

北朝鮮 IT 労働者は、AI ツールの活用及び外国の仲介者との協力によるものを含め、偽の身分及び所在地を活用して非北朝鮮 IT 労働者として自身を偽装するために、様々な手法を用いている。彼らは、北米、欧州及び東アジアを含め、世界中で拡大する標的となる顧客からフリーランスの雇用契約を獲得するために、高度な IT スキルへの既存の需要を利用している。また、北朝鮮 IT 労働者自身も、特にブロックチェーン業界において、悪意あるサイバー活動に関与している可能性が極めて高い。北朝鮮 IT 労働者に対する雇用、支援又は業務の外注は、知的財産、データ及び資金の窃取から、評判の悪化及び法的な結果に至るまで、深刻なリスクを一層もたらす。

この文脈において、我々３か国は、北朝鮮 IT 労働者の脅威を阻止するため、連携して行動してきている。本日、日本は、北朝鮮 IT 労働者が使用する新たな手口に関する詳細な情報を提供するために過去の注意喚起を更新し、民間企業に対して、北朝鮮 IT 労働者を不注意に雇用し、支援し、又は業務を外注してしまうリスクを軽減するよう勧告する。米国は、ロシア、ラオス及び中国におけるものを含む、北朝鮮 IT 労働者に関する計画を促進する４つの団体及び個人を関連措置の追加対象に指定する。韓国は、企業が標的とされること又は被害を受けることを避けるために、北朝鮮 IT 労働者の活動に関するアドバイザリを発出した。

８月 26 日、我々３か国は、Mandiant と連携し、東京において、北朝鮮の攻撃に対する闘いにおいて、官民の連携を向上させ、国際的な業界連携を支援するための行事を主催した。

日本、米国及び韓国は、北朝鮮による悪意あるサイバー活動及び不法な資金調達に対処するため、３か国間の連携を強化し、公共部門と民間部門の連携を深化するとのコミットメントを再確認する。