外務省 Ministry of Foreign Affairs of Japan | 国家サイバー統括室 National Cybersecurity Office | 警察庁 National Police Agency | 財務省 Ministry of Finance, JAPAN | 経済産業省

Ministry of Foreign Affairs | Australian Government Department of Foreign Affairs and Trade | Global Affairs Canada | Affaires mondiales Canada | Royal Canadian Mounted Police | Gendarmerie royale du Canada

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
Liberté
Égalité
Fraternité

Federal Foreign Office

Ministero degli Affari Esteri e della Cooperazione Internazionale

Ministry of Foreign Affairs of the Netherlands

NEW ZEALAND FOREIGN AFFAIRS & TRADE
Manatū Aorere

Foreign, Commonwealth & Development Office

Office of Financial Sanctions Implementation HM Treasury

Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers

July 31, 2026

North Korea relies upon a network of skilled Information Technology (IT) workers, deployed within and outside of North Korea, to obtain false identities and remotely earn income to fund North Korea's unlawful nuclear weapons and ballistic missile programs.

North Korean IT workers impersonate nationals of other countries to obtain work and income through online platforms operated by private companies for employment, procurement, and contracting of services. These workers seek out contracts with the intent of remitting their salaries to their parent North Korean agencies. They also pose an insider threat to companies and are involved in data exfiltration, cryptocurrency theft, and theft of sensitive information. North Korean IT workers employ increasingly sophisticated methods, including the integration of AI, to obfuscate their identities and expand their activities globally.

Our countries have repeatedly issued information to warn the international community and private sector of the threat posed by North Korean IT workers. Japan, the United States, and the Republic of Korea issued a "Joint Statement on North Korean IT Workers" in August 2025, and the Multilateral Sanctions Monitoring Team (MSMT) released its second report on North Korea's violation and evasion of UN sanctions through cyber and IT worker activities in October 2025. The United States, Japan, Republic of Korea, United Kingdom, Australia, and Canada have all issued advisories regarding the risk North Korean IT workers pose to private companies, governments, and individual citizens. We continue to actively monitor and counter the North Korean IT worker threat.

According to UN Security Council Resolution 2397, all UN Member States must repatriate to North Korea all North Korean nationals earning income in that Member State's jurisdiction, subject to limited exceptions. Additionally, contracting with North Korean IT workers and paying them for services rendered may also violate the domestic laws of many countries, including Japan, the United States, and the Republic of Korea, and may result in legal consequences or financial penalties.

The Financial Action Task Force (FATF) identifies North Korea as a high-risk jurisdiction subject to a call for action (blacklist). The FATF continuously reiterates the need to implement robust targeted financial sanctions consistent with relevant UN Security Council resolutions and calls on all jurisdictions to apply countermeasures to protect their financial systems from North Korean money laundering, terrorist financing, and proliferation financing risks. Yet, North Korea has increased connectivity with the international financial system through diversified revenue generation activities, including IT worker schemes. As spotlighted in the FATF's Complex Proliferation Financing (PF) and Sanctions Evasion typologies report, North Korea frequently uses IT worker schemes to generate revenue that supports its weapons of mass destruction program.

We urge all countries, companies, and other entities to deepen their understanding of North Korean IT worker schemes and implement measures to counter the tactics listed below. Companies operating online platforms should continue to strengthen their countermeasures, such as enhancing identity verification procedures (strict review of identification documents, requirement of in-person interviews, etc.) and detecting suspicious accounts (introduction of systems that notify anomalous information entries, etc.). The following information is provided by states participating in this alert.

[Modus Operandi Used by North Korean IT Workers]

- Many North Korean IT workers register for accounts on online platforms by falsifying their nationality or identity. Typical methods used include forging identification documents and impersonating another person. North Korean IT workers use images of identification documents provided by third parties—such as proxies residing in third countries—to register accounts, while the actual work is conducted by the North Korean IT workers themselves.
- North Korean IT workers are increasingly likely to use third-party proxies to facilitate the creation of online accounts, participate in job interviews, and even establish in-person contact to create a false sense of trust and obtain work contracts.

- North Korean IT workers often attempt to avoid being paid by direct deposit and may request payment via money transfer services or cryptocurrency. In many cases, North Korean IT workers provide employers a third party's bank account as the recipient for payments, request that the third party transfer the funds to a designated foreign account, and provide a part of the payment to the third-party as a fee for use of their bank account.
- North Korean IT workers often possess high-level skills in IT-related work and are seeking work in wider areas—such as the development of web pages, mobile applications, software, and blockchain applications—through online platforms and other channels. In some cases, they also get work contracts directly from companies or individuals.
- While many North Korean IT workers reside in North Korea, China, and Russia, as well as Southeast Asian and African countries, they may conceal the fact that they are working from abroad using third-party proxies, VPNs, remote desktop software, and similar tools.
- North Korean IT workers are known to use third-party proxies as facilitators overseas, such as in the United States, to run "laptop farms" which receive company-provided laptop computers for North Korean IT workers to remotely access, obfuscating their true location.
- In addition to obtaining IT-related work, North Korean IT workers may obtain foreign currency by engaging in fraudulent foreign exchange trading using automated trading systems they themselves developed.

Furthermore, accounts associated with North Korean IT workers often exhibit the characteristics below. If multiple characteristics apply to a job applicant, there is a possibility that a North Korean IT worker is fraudulently seeking work.

(For companies operating online platforms)

- ✓ Frequent changes to registered information (such as account name, contact details, and bank account information for receiving salaries).
- ✓ The account holder's name does not match the name on the registered payment account.
- ✓ Multiple accounts have been created using the same identification document.
- ✓ Identification documents used for identity verification appear forged or altered using image editing software.
- ✓ Multiple accounts are accessed from the same IP address.
- ✓ A single account is accessed from multiple IP addresses within a short period of time.
- ✓ The account remains logged in for an unusually long period of time.

- ✓ The cumulative work hours or related metrics are unnaturally high.
- ✓ An account user posts false reviews for itself, likely to improve the account's rating.

(For those hiring or procuring services)

- ✓ The account's profile contains errors or uses unnatural expressions that appear to be the result of inaccurate machine translation, indicating a lack of proficiency in the language of the country they claim to be from. (However, North Koreans may use translation services or large language models to produce convincing profiles and communications in second languages.
- ✓ Discrepancies appear in video conference meetings, including photo ID mismatches or video feeds that appear to be manipulated or artificially generated.
- ✓ Refuses to participate in video conference meetings.
- ✓ Offers to work at rates lower than the general market rate.
- ✓ Shows signs that the account is being operated by multiple people. North Korean IT workers often operate in teams, and the individual whom a hiring or procuring official interacts with may change depending on the time of day.
- ✓ Requests payment in cryptocurrency.

北朝鮮 IT 労働者に関する各国・企業等に対する注意喚起

令和８年７月３１日

北朝鮮は、不法な核兵器や弾道ミサイル計画の資金源とすべく、偽りの身分を得て、遠隔で収入を得るため、北朝鮮内外に派遣された、技術を有する IT 労働者のネットワークに依拠しています。

北朝鮮 IT 労働者は、他国の国民になりすまし、民間企業が運営する雇用や業務の受発注のためのオンライン・プラットフォームを通じ、業務や収入を得ています。これらの労働者は、北朝鮮における親元の機関に給与を送金する意図をもって契約を探し求めています。また、彼らは、企業に対して内部脅威をもたらし、データ流出並びに暗号資産及び機微情報の窃取に関与しています。北朝鮮 IT 労働者は、身分を隠蔽し、世界的に活動を拡大させるため、AI の統合を含む一層高度な手法を活用しています。

我々各国は、北朝鮮 IT 労働者がもたらす脅威について国際社会及び民間部門に注意を呼びかけるための情報を繰り返し発出してきました。日本、米国及び韓国は、2025 年８月、「北朝鮮 IT 労働者に関する共同声明」を発出し、また、多国間制裁監視チーム（MSMT）は、2025 年 10 月、北朝鮮によるサイバー及び IT 労働者の活動を通じた国連制裁の違反及び回避に関する第２回報告書を公表しました。米国、日本、韓国、英国、豪州及びカナダは、北朝鮮 IT 労働者が民間企業、政府及び市民個人にもたらすリスクに関するアドバイザリーを発出してきています。我々は、引き続き、北朝鮮 IT 労働者の脅威を積極的に監視し、対抗していきます。

国連安全保障理事会決議第 2397 号によれば、限定的な例外を除き、全ての国連加盟国は、当該加盟国の管轄権内において収入を得ている全ての北朝鮮「国民」を北朝鮮に送還しなければなりません。加えて、北朝鮮 IT 労働者と契約を交わし、サービス提供の対価を支払う行為は、日本、米国及び韓国等を含む多くの国の国内法に違反し、法的責任を問われる又は罰金を課されるおそれもあります。

金融活動作業部会（FATF）は、北朝鮮を行動要請の対象となる高リスクの国・地域（ブラックリスト）として位置付けています。FATF は、関連する国連安保理決議と整合した強力な標的型金融制裁を実施する必要性を繰り返し強調するとともに、北朝鮮による資金洗浄（マネー・ローンダリング）、テロ資金供与及

び拡散金融のリスクから自国の金融システムを保護するため、全ての国・地域に対して対抗措置の適用を求めています。それにもかかわらず、北朝鮮は、IT 労働者スキームを含む多様な収益獲得活動を通じ、国際金融システムとの結び付きを強化しています。FATF の複雑な拡散金融（PF）及び制裁回避の類型報告書において強調されているとおり、北朝鮮は大量破壊兵器計画を支える収入を生み出すために、IT 労働者スキームを頻繁に利用しています。

我々は、全ての国及び企業等に対して、北朝鮮 IT 労働者スキームについての認識を深め、以下の手口に対抗する措置をとるよう要請します。オンライン・プラットフォームを運営する企業は、本人確認手続の強化（身分証明書の厳格な審査、対面面接の義務等）や、不審なアカウントの探知（異常な情報の登録が通知されるシステムの導入等）といった対策を引き続き強化すべきです。以下の情報は本注意喚起に参加する各国から提供されたものです。

【北朝鮮 IT 労働者の手口】

- ○　北朝鮮 IT 労働者の多くは、国籍や身分を偽り、オンライン・プラットフォームへのアカウント登録を行っています。代表的な手口には、身分証明書の偽造や第三者へのなりすましが含まれます。北朝鮮 IT 労働者は、第三国に在住する代理人のような第三者から提供された身分証明書の画像を使用してアカウント登録を行う一方、実際の業務は北朝鮮 IT 労働者自身が行っています。
- ○　北朝鮮の IT 労働者は、オンライン・アカウントの作成や、採用面接への参加、更には対面での接触を通じて偽りの信頼感を醸成し、業務契約を獲得するために、第三者の代理人を利用するケースがますます増えています。
- ○　北朝鮮の IT 労働者は、銀行口座への直接振込での支払いを避けようとする場合が多く、送金サービスや暗号資産での支払いを求めることがあります。多くの場合において北朝鮮 IT 労働者は、報酬の振込先として第三者の口座を雇用主に提出し、当該第三者に対し、指定の外国口座への送金を依頼し、銀行口座を利用する対価として報酬の一部を手数料として支払っています。
- ○　北朝鮮 IT 労働者は、IT 関連業務に関して高い技能を有する場合が多く、オンライン・プラットフォーム等を通じて、ウェブページ、モバイル・アプリケーション、ソフトウェア及びブロックチェーン・アプリケーションの制作等といった幅広い業務を探しています。また、企業や個人から業務契約を直接得ている場合もあります。

○　北朝鮮 IT 労働者の多くは、北朝鮮、中国及びロシア並びに東南アジア及びアフリカ諸国に在住しながら、第三者の代理人、VPN、リモートデスクトップ・ソフトウェア及び同種のツールを用いて外国から作業を行っている事実を秘匿している場合があります。

○　北朝鮮 IT 労働者は、米国等の海外の第三者の代理人を利用して、「ラップトップ・ファーム」を運営していることが知られています。この「ファーム」では、企業から支給されたノートパソコンを受け取り、北朝鮮 IT 労働者が遠隔でアクセスすることで、彼らの実際の所在地を隠蔽しています。

○　北朝鮮 IT 労働者は、IT 関連業務の受注のほか、自ら開発した自動売買システムを使用して不正に FX 取引を行い、外貨を獲得している場合もあります。

さらには、北朝鮮 IT 労働者に関連するアカウントには、次の特徴がしばしばみられます。複数の特徴が求職者に当てはまる場合、北朝鮮 IT 労働者が不正に仕事を得ようとしている可能性があります。

（プラットフォームを運営する企業向け）

□　アカウント名義、連絡先及び報酬受取用の銀行口座情報等の登録情報を頻繁に変更する。

□　アカウント名義と登録されている報酬受取口座の名義が一致しない。

□　同一の身分証明書を用いて複数のアカウントを作成している。

□　本人確認に使用された身分証明書が、画像編集ソフトを用いて偽造又は改ざんされたようにみられる。

□　同一の IP アドレスから複数のアカウントにアクセスしている。

□　１つのアカウントに対して短時間に複数の IP アドレスからアクセスしている。

□　アカウントに異常に長い時間ログインしている。

□　累計作業時間が不自然に長い又は関連の指標が不自然に高い。

□　アカウント・ユーザーが、おそらく当該アカウントの評価を向上させるため、自らに対して虚偽のレビューを投稿している。

（雇用又は業務を発注する方向け）

- □　アカウントのプロフィールにおいて、不正確な機械翻訳の結果とみられる誤記載が含まれ、又は、不自然な表現が用いられており、出身地とされている国の言語に堪能でない（ただし、北朝鮮 IT 労働者は、翻訳サービスや大規模言語モデルを用いて、第二言語においても説得的なプロフィールを作成し、コミュニケーションをとる場合もある。）。
- □　写真付き身分証との不一致や、改ざん又は人工生成されたようにみえる映像フィードを含め、ビデオ会議中の不整合がみられる。
- □　テレビ会議形式の打合せへの参加を拒否する。
- □　一般的な相場より安価な報酬で業務を募集している。
- □　複数人でアカウントを運用している兆候がみられる。北朝鮮 IT 労働者は、チームで活動することが多く、採用や発注の担当者がやり取りする相手が時間帯によって変わる場合がある。
- □　暗号資産での支払いを要求する。