2022 年 5 月 16 日

朝鮮民主主義人民共和国の
情報技術労働者に関するガイドライン

米国国務省、米国財務省、および連邦捜査局 (FBI)は、朝鮮民主主義人民共和国 (北朝鮮) の情報技術 (IT) 労働者が北朝鮮国籍ではないふりをして雇用を得ようとする企てに対する警鐘として、本勧告を発表するものである。北朝鮮 IT 労働者関連の活動に関与したり支援したり、関連する金融取引を処理したりする個人や企業に対して、米国と国連 (UN) 当局の権限下での制裁指定を含めて、風評被害や法的結果が生じる可能性がある。

北朝鮮は、高度な技能を有する何千人もの IT 労働者を世界中に送り込んでおり、米国と国連の制裁に違反して、大量破壊兵器 (WMD) と弾道ミサイルプログラムに寄与する収入を生み出している。こうした IT 労働者は、ソフトや携帯電話アプリ開発のような特定の IT 技能への既存の需要を利用して、北米、ヨーロッパ、および東アジアを含めて世界中でクライアントからフリーランス雇用契約を獲得している。多くの場合、北朝鮮 IT 労働者は米国在住の、あるいは北朝鮮人ではないテレワーカーを自称している。さらにこうした労働者は、北朝鮮人ではない人々との下請け契約することによって、身元や場所を曖昧にすることもある。北朝鮮 IT 労働者は、通常は悪意のあるサイバー活動ではない IT 業務に従事しているが、契約者として得た優先アクセスを活用して、北朝鮮の悪意あるサイバー侵入を可能にしている。さらに、労働者は強制労働に服している場合もある。

本勧告は、北朝鮮 IT 労働者の活動方法の詳細情報、つまり、フリーランス開発者を雇う企業や、フリーランスや支払いプラットフォームが北朝鮮 IT 労働者を特定するための危険信号となる指標、そして、不注意による北朝鮮 IT 労働者の雇用や活動の促進に対して企業がよりよく防衛するための一般的な被害軽減策を提供している。付属文書は、国連 1718 制裁委員会の北朝鮮専門家委員会により作成された報告書からの北朝鮮 IT 労働者に関する追加情報を提供している。FBI は、北朝鮮 IT 労働者の活動を含む疑わしい活動を FBI 各地域事務所に報告するよう米国企業に薦めている。

北朝鮮 IT 労働者：背景

北朝鮮 IT 労働者は、兵器開発プログラムのような北朝鮮政権の経済および安全保障上の最優先事項の資金源になる非常に重要な収入の流れを提供している。北朝鮮の指導者である金正恩は、IT 労働者が重要な外貨収入源であることを認識し、その活動を支援している。

何千人もの北朝鮮 IT 労働者は海外に送り込まれ、かつ、北朝鮮国内にも在住しており、北朝鮮政府に送金される収入を創り出している。北朝鮮 IT 労働者は、主として中華人民共和国(中国)とロシアに在住しているが、アフリカや東南アジアにも少数ではあるが在住している。こうした IT 労働者は、フリーランスの職を獲得し直接顧客と接するために、海外の人脈に依存することが多い。

北朝鮮 IT 労働者は全員、北朝鮮の指導者金正恩の政権支援のために金を稼いでいる。その大多数は、国連が禁止しているにもかかわらず北朝鮮が行っている WMD や弾道ミサイルプログラム、および先端通常兵器開発と貿易部門に直接関与している組織に従属しており、その利益を優先させて働いている。この結果、北朝鮮 IT 労働者が生み出す収益は、米国や国連の制裁に違反して、北朝鮮が WMD や弾道ミサイル開発のために使用されている。こうした組織の多くは、国連や米国の制裁対象に指定されている。北朝鮮 IT 労働者を派遣している組織は以下の通りである:

- **軍需産業部門(MID)の第 313 総局、これは北朝鮮の兵器研究、開発、および生産を管理しているが、この武器には核兵器と弾道ミサイルをはじめ、その他の軍事機器も含まれる。**MID は朝鮮労働党中央委員会の下部組織であり、第 313 総局を通じて、大半の北朝鮮 IT 労働者を海外に送り込んでいる。朝鮮労働党の全財産と利子は、大統領命令 (E.O.) 13722 に基づいてアクセス禁止になっている。

- **原子力産業省**は、北朝鮮の核兵器開発で重要な役割を果たし、北朝鮮の兵器プログラムの日常的な運営を担っている。原子力産業省は、E.O. 13382 に基づき指定されている。

- **国防部と朝鮮人民軍**に従属する軍事的組織。朝鮮人民軍は、特別指定国民およびアクセス禁止財産表に指定されている。

- **朝鮮教育委員会の対外貿易部や中央委員会科学・教育部の平壌情報技術局**といったあまり知られていない組織。北朝鮮政府の全財産と利子は E.O. 13722 に基づいてアクセス禁止となっている。

海外の北朝鮮 IT 労働者は、工場で働く北朝鮮労働者や海外の建設プロジェクトで働く労働者の少なくとも 10 倍以上の収入を得ている。北朝鮮 IT 労働者は、時には米ドルで年間 30 万ドル以上稼ぐことができ、IT 労働者のチームは全体として年間 300 万ドル稼ぐ場合もある。総収入の大部分は、北朝鮮政権の優先事項を支援しており、この中には WMD プログラムも含まれる。

北朝鮮 IT 企業とその労働者は、通常は様々な複雑性と困難性のある広範囲な IT 開発業務に従事しているが、それには以下のような例がある:

- 携帯電話アプリとウェブ基盤のアプリ
- 仮想通貨両替プラットフォームとデジタルコインの構築
- 一般的な IT 支援

- グラフィックアニメーション
- オンライン賭博プログラム
- 携帯電話ゲーム
- デート用アプリ
- 人工知能関連アプリ
- ハードウェアとファームウェア開発
- 仮想現実と拡張現実プログラミング
- 顔認証や生体認証ソフト
- データベース開発と管理

北朝鮮 IT 労働者によって開発されたアプリやソフトは、ビジネス、健康やフィットネス、ソーシャルネットワーキング、スポーツ、エンターテインメント、およびライフスタイルを含めて、幅広い分野や部門に及んでいる。北朝鮮 IT 労働者は、仮想通貨に関連するプロジェクトも頻繁に請け負っている。北朝鮮 IT 労働者の中には、仮想通貨取引所を設計したり、仮想通貨取引業者のための分析ツールやアプリケーションを構築したり、製品そのものを販売したりしている人たちもいる。

北朝鮮は、何十年もの間、国民に対して数学や科学の教育の重要性を強調してきた。金正恩政権では歴史的に優先事項になってきた科学や技術の進歩に対する重視は、関連分野の研究への資源や人材の投資に反映されている。北朝鮮における現在のサイバー・IT 教育は、このような推進力の上に成り立っており、その結果的として、労働党、研究所、軍と連携した統合カリキュラムが実現されている。

- 金正恩指揮下で、近年では IT 関連の科目での教育・訓練に重点が置かれ、特に金日成総合大学、金策工業総合大学、平壌国立科学技術大学といった北朝鮮を代表する教育機関では、強力な IT 学位プログラムが開発されている。こうした一流大学だけでも、約 3 万人の学生が情報通信技術関連の科目を学んでいる。

- 2019 年の時点で、37 大学が 情報セキュリティを含む高度な科学、技術、工学および数学 (STEM) 科目のコース提供する 85 のプログラムを設置しており、さらに各道には少なくとも一つの中等教育機関が設立され、将来性のある学生を養成していると報告されている。

- 北朝鮮の教育制度は、非常に競争が激しく、最優秀な学生のみがエリート級の科学技術プログラムに受け入れられる。学生は錦城アカデミーや錦城中学校１号館のような中等教育機関から年少のうちに募集される。

- 北朝鮮 IT 労働者は、海外や国内の組織で追加的訓練を受けるが、大抵の場合、北朝鮮国内の地域 IT 研究センター を通じてさらに技能を磨いている。北朝鮮 IT 労働者は、歴史的に東アフリカ、東南アジア、南アジアなどで訓練を受けており、海外での訓練からかなりの特典を得ている。

北朝鮮 IT 労働者の活動方法

北朝鮮 IT 労働者は、北米、ヨーロッパ、東アジアにある国々を含めて、豊かな国々の雇い主からフリーランス契約を得ている。多くの場合、北朝鮮 IT 労働者は、韓国人、中国人、日本人、あるいは東欧や米国在住のテレワーカーを装っている。

北朝鮮 IT 労働者は、時として、第三者の下請け業者と契約することによって自らの身元を曖昧にする。こうした下請け業者は、北朝鮮 IT 労働者のために契約を結ぶ北朝鮮人以外のフリーランス IT 労働者である。北朝鮮 IT 管理者はまた、北朝鮮以外の IT 労働者のチームを独自に雇用している。こうした労働者は通常、北朝鮮の雇い主の本当の身元や雇い主が北朝鮮企業であるという事実に気づいていない。北朝鮮 IT 管理者は、北朝鮮 IT 労働者が正体を知られないように、アウトソーシングされた従業員を使ってソフト購入や顧客との対応を行っている。

北朝鮮 IT 労働者は通常、仮想通貨取引所やウェブサイトの開発のような悪意のない IT 業務に従事しているが、北朝鮮の悪意あるサイバー侵入を可能にするために契約業者として得た特権的アクセスを利用する。IT 労働者自身が悪意あるサイバー活動に関わる可能性は低いとはいえ、海外在住の北朝鮮 IT 労働者の中には、北朝鮮在住の悪意あるサイバー活動家に後方支援を行っている者もいる。北朝鮮 IT 労働者は、仮想インフラへのアクセスを共有したり、北朝鮮サイバー活動家が盗んだデータ販売を促進したり、北朝鮮のマネーロンダリングや仮想通貨移転を支援したりすることがある。

北朝鮮 IT 活動家は、北朝鮮が禁止されている兵器プログラムのために WMD や弾道ミサイル関連品目を調達する際に、北朝鮮当局の支援も行ってきた。

労働者が強制労働を含めて、人身売買の対象となっている例もある。信頼できる報告書は、海外の北朝鮮人労働者の多くが過剰労働時間、北朝鮮政府保安要員による絶え間ない厳しい監視、安全でなく不衛生な生活環境、ほとんど移動の自由がないといったことにさらされている、としている。北朝鮮政府は、海外労働者の賃金の最大 90%までを差し押さえ、それが政府の何億ドルもの歳入となっている。

北朝鮮 IT 労働者: 技能とプラットフォーム

海外の北朝鮮 IT チームは、一般的に、様々なオンラインプラットフォームからフリーランスの仕事を 得ている。企業は、こうしたプラットフォームを使ってフリーランス IT 開発者が入札できるプロジェクトの契約を宣伝している。あまり一般的ではないが、北朝鮮 IT チームは、地元の北朝鮮人ではない人を見つけ、北朝鮮が実際に支配する企業の名目上の責任者として雇うこともある。さらに、例として、北朝鮮 IT チームが書類上は合法的な地元企業のために仕事をするが、独自に事業を展開し、北朝鮮出身であることを隠す代わりに、外国企業に手数料を支払っている場合もある。北朝鮮 IT チームは、英語や中国語など外国語の堪能なメンバーを頻繁にチームに入れている。

北朝鮮 IT 労働者は、世界中の企業から開発契約を獲得するために、主流および IT 産業固有のフリーランス契約プラットフォーム、ソフト開発ツールやプラットフォーム、メッセージアプリ、およびソーシャルメディアやネットワーキングウェブサイトを幅広く使用し、かつ、その仕事からの支払いを受け取るために数々のデジタル支払いプラットフォームやウェブサイトを活用している。さらに北朝鮮 IT 労働者は、受け取る資金をロンダリングして移動させたり、契約業務から受け取るデジタル支払いを管理するために、仮想通貨取引所や取引プラットフォームも利用している。

北朝鮮 IT 労働者: 身元を隠す

北朝鮮 IT 労働者は、オンライン上でわざとその身元、所在地、国籍を隠蔽し、しばしば朝鮮人以外の名前を偽名として使っている。さらに、仮想プライベートネットワーク (VPN)、仮想プライベートサーバー(VPS)、あるいは 第三国の IP アドレスを使って目立たない場所からインターネットに接続しているように見せかけ、北朝鮮での場所や人間関係が調査される可能性を減らそうとしている。北朝鮮 IT 労働者は一般的に、テレワークの匿名性に依存し、口座開設と維持のためにプロキシーを使い、仲介者を利用して、ビデオチャットの代わりにテキストでのチャットによる連絡を好む。

北朝鮮 IT 労働者は、フリーランスソフト開発者向けウェブサイトのプロジェクトに入札、落札、作業、かつ支払いのためにプロキシー口座を使う。こうしたプロキシー口座は第三者の個人に属しており、この中には北朝鮮 IT 労働者に自らの身元証明書と口座情報を売る人もいる。北朝鮮 IT 労働者が合法的なプラットフォーム口座を使うために個人に使用料を支払う場合もある。 北朝鮮 IT 労働者は、フリーランスプラットフォームのプロフィールに、代理人の実際の所属先や職務経験を入力することもある。

北朝鮮 IT 労働者は時には、開発プロジェクトでの協力を提案するために、北朝鮮人以外のフリーランス労働者とプラットフォーム上で契約することもある。北朝鮮 IT 労働者は、こうした取引関係を利用して、米国、ヨーロッパの仮想インフラ上で IT 作業を行うための新規契約や仮想通貨口座へのアクセスを得て、不正アクセス防止を目的とするセキュリティ方策を回避している。他のフリーランス労働者の協力を得て口座を開設する際、北朝鮮 IT 労働者は、より多く金を稼ぐために米国やその他の西側の身元証明書とフリーランスプラットフォーム口座を必要とする第三国国籍者だと主張することがある。

本当の所在地を隠すことによって、北朝鮮 IT 労働者はその活動に使うオンラインプラットフォームと業務の利用規約に違反することが可能となる。さらに、不正防止、制裁遵守、マネーローンダリング防止対策による検出を回避するために、北朝鮮 IT 労働者は、特に銀行サービスの口座ごとに単一の専用デバイスを使うこともある。

北朝鮮 IT 労働者は、日常的に、身元証明書を含む偽物、変造、または改ざんされた文書、フォトショップなどのソフトを使って自分で作ったもの、あるいは文書偽造業者に依頼して本人または提供された写真と実在の人物の識別情報を組み合わせて改造した偽造署名を使用している。北朝鮮 IT 労働者がよく調達する偽造文書には以下のようなものがある:

- 運転免許証
- 社会保障カード
- パスポート
- 国籍身元証明カード
- 在留外国人カード
- 高校や大学の卒業証書
- 労働ビザ
- クレジットカード、銀行や公共料金請求書

これらの中には、身元が盗まれる場合もあるが、北朝鮮 IT 労働者が北朝鮮国籍ではない人に自らの個人情報を使ったり、あるいはアクセスできる情報を使ったりして口座を開設するよう勧誘し、その後手数料を払って口座の管理権を北朝鮮 IT 技術者に移転させるという場合もある。これによって、北朝鮮 IT 労働者は、クライアントのためにフリーランスのプロジェクトをオンラインで入札完了する際に、リモートデスクトップのアクセスを通じて実際の口座所有者のインフラを使用し、自分の身元を隠すことができる。各 IT 労働者は複数の身元証明書と口座を使用することが多く、同じチームの IT 労働者間で共有される場合もある。こうした口座と身元証明書は、世界のあらゆる国の出身者を装っている。

北朝鮮 IT 労働者は、フリーランスプラットフォーム、支払い提供者、および北朝鮮 IT 労働者を雇う企業に対して本人確認を行うために、米国や海外の銀行の顧客口座情報を盗む可能性がある。少なくとも一つの事例では、北朝鮮 IT 労働者は盗んだ銀行口座情報を使って小切手を偽造した。北朝鮮 IT 労働者の代理人としての口座と履歴書には、教育機関や以前の雇い主の連絡先情報を含めて、改ざんされた、しかし現実的で詳細な学歴・職歴情報も含まれていることが多い。

さらに北朝鮮 IT 労働者は、プロジェクトに入札する際に、評判のいい米国人や欧州人と思われるように、オンライン開発者のプロフィールの雇用欄に、欧米の中小企業の名前を記入することもある。実際の従業員の氏名や欧米企業の合法的なドメインと似通っているメールアドレスを使うこともある。

北朝鮮 IT 労働者は、さらにフリーランスプラットフォームで使われる作業合意書、請求書、顧客とのコミュニケーション文書、およびその他の書類を改ざんし、顧客確認とマネーロンダリング防止(KYC/AML) 措置やプラットフォームがユーザー活動の合法性を保証するための同様な手順を満足させようとする可能性がある。こうした偽造文書は、確認を妨害するために最小限の連絡先しか記載されていないこともある。

北朝鮮 IT 労働者は、自らを韓国人つまり、単に「朝鮮」国民として称することで国籍を隠そうと試みることもある。

フリーランスの職を意識のない企業で得た北朝鮮 IT 労働者は、さらに後に別の北朝鮮 IT 労働者をフリーランスで雇用するようその企業に推薦することも知られている。

北朝鮮 IT 労働者の履歴書

北朝鮮 IT 労働者は、システムやプログラム開発、データベース管理システム、および様々な共通言語、フレームワーク、ツールやクラウドリソースの活用に関する技能を宣伝している。この中によく含まれるのは、数々のコーディング言語やマークアップ言語での高度な技能である。北朝鮮 IT 労働者のプロジェクトの大多数は、携帯電話とウェブのアプリ開発である。北朝鮮 IT 労働者は、データやワークフロー管理のためのコラボレーションプラットフォーム、ホスティングサービスも使うことがある。こうした労働者は、様々なデータベースの使用経験があり、主要なプロバイダー向けのクラウドや分析商品・サービスにも詳しいと報告している。さらに、北朝鮮 IT 労働者は、業務にデジタル支払いや電子商取引プラットフォームを取り入れている。

北朝鮮 IT 労働者は、一般的にデザインはシンプルで、彼らの偽造されたフリーランス開発者の外的人格の信用性を高める努力として「ポートフォリオ」ウェブサイトを構築する。こうした仮想ポートフォリオは、北朝鮮 IT 労働者の外的人格を表し、オンラインフリーランス開発者口座とリンクしていることが多い。連絡先情報や所在地を含めてこうしたウェブサイト上の情報は、職歴や学歴と同様に偽りであることが多い。

危険信号の兆候

フリーランス業務と支払いプラットフォーム企業は、自社のプラットフォームを使っている可能性がある北朝鮮 IT 労働者の兆候や行動と考えられる以下の活動に気をつけるべきである。

- 比較的短期間の間に、様々な IP アドレスから一つの口座に複数回のログインがあり、特に IP アドレスが別々の国に関連している場合、
- 一つの IP アドレスから同じプラットフォームにある複数口座に開発者がログインしている場合、
- 同時に 1 日以上継続して口座に開発者がログイン中である場合、
- 口座アクセスに使われるルーターのポート 3389 のように、リモートデスクトップ共有ソフトの活用に関連するルーターポートやその他の技術機器構成、特にリモートデスクトップ共有ソフトの活用が企業で一般的な慣行ではない場合、
- 開発者口座が開発者口座格付けを上げるために不正な顧客口座を使うが、しかし顧客と開発者の両方の口座 がお金の送金・引き出しに同じ PayPal 口座を使う場合 (自らの金で自らに支払っている)、
- 入札書類やプロジェクトコミュニケーション方法のような文書テンプレートを頻繁に使い、特に様々に異なる開発者が同じテンプレートを使っている場合、

- 短期間に一人の顧客口座から高い格付けを受ける複数の開発者口座で、開発者口座・顧客口座の設置に使われた文書が類似、あるいは同一である場合、

- プロジェクトへの広範な入札が行われ、開発者によるプロジェクト入札数に比べて、落札されたプロジェクト数が少ない場合、

- 特に中国にある銀行口座への、支払いプラットフォームからの頻繁な送金、および資金の最終的な目的地をごまかすために一つ以上の企業を通じてのルートを使っていることがある場合。

フリーランス開発者を雇い入れる企業は、北朝鮮 IT 労働者の兆候や行動に該当する可能性がある以下の活動に注意するべきである。

- フリーランスソフト開発者のウェブサイトや支払いプラットフォーム口座が閉鎖された場合、あるいは労働者が別の口座（特に異なる名前に登録されている場合）の使用を要求する雇い主に連絡した場合、

- デジタル支払いサービス、特に中国に連関したサービスの利用、

- 開発者のフリーランスプラットフォームのプロフィール、ソーシャルメディアのプロフィール、外部ポートフォリオウェブサイト、支払いプラットフォームのプロフィール、査定された場所や時間などにおいての氏名のつづり方、国籍、主張された勤務地、連絡先、学歴、職歴などの情報に矛盾がある場合、

- 驚くほど単純なポートフォリオウェブサイト、ソーシャルメディアプロフィール、あるいは開発者プロフィール、

- ソフト開発企業の経営幹部を装った人々からのサービスを勧誘したり能力を広告するための直接メッセージやコールドコール、

- クライアントが IT 労働者を見つけた元のフリーランスプラットフォームサイトとは別のプラットフォーム上で、クライアントや潜在的なクライアントとコミュニケーションを取りたいという要請がある場合、

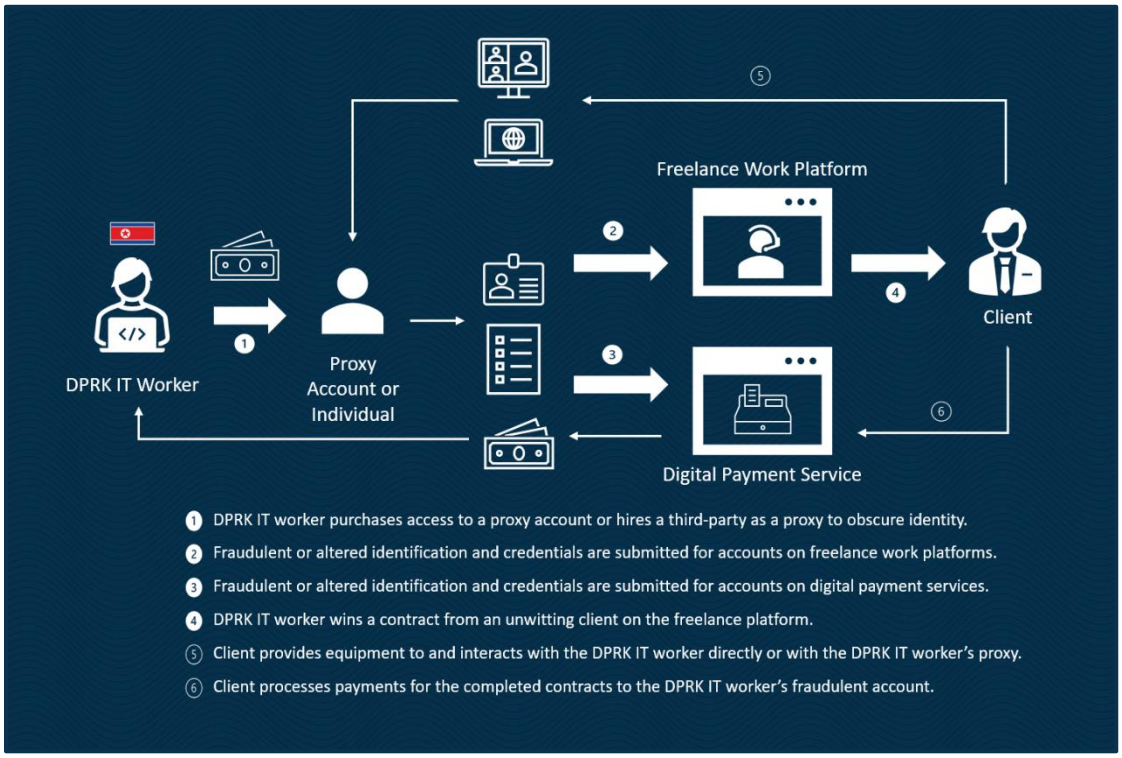
- 雇い主が書類やノートパソコンのような業務用機器を送ることを開発者に提案し、開発者がその身元証明書に記載されていない住所に送付するように要求してきた場合。開発者が身元証明書に記載されている住所では送付物を受け取れないと主張する場合には、特に疑うべきである、

- KYC/AML 対策や正式な金融システムの活用を回避するために、仮想通貨で支払いを求める場合、

- 生産ベンチマークやチェックインミーティングをせずに、契約金の支払いを求めてくる場合、

- 必要な営業時間内に業務を行うことができない場合、
- 連絡先情報、特に電話番号とメールアドレスの誤記、変更、
- 申請者と一致しないと思われる経歴情報、
- 時宜を得た方法で作業を完了できない、あるいは作業に対応できない場合、
- 特に「即時」コミュニケーション方法を通じて、時宜を得た方法で連絡できない場合、
- 他の契約を獲得するために同僚に個人情報の一部を貸してもらうよう頼む場合。

北朝鮮 IT 労働者の活動の概要



考えうる被害軽減策

フリーランス向けと支払いプラットフォーム企業向け

- 提案書審査や契約時のデューデリジェンス手続きの一部として提出された書類の確認をすること、つまり、提出された書類に記載されている連絡先ではなく、企業データベースに登録されている連絡先情報を使ってリストにあるクライアントに連絡を取ることによって、請求書や業務委託契約書を独自に確認する、

- 提出された身元確認書類に偽造がないか精査し、地元の法執行機関に支援を求める可能性もある。身元確認のために提出される低品質画像を拒否する、

- 口座開設のために提供されたウェブサイトの存在を確認し、口座開設のために消滅したウェブサイトを利用した口座への精査を強化する、

- 初期デューデリジェンス契約作成プロセスと更新方針の一部として、身元確認用ビデオの提出を義務付け、または身元確認のためのビデオ面接を実施する、

- 特に口座アクセスのためにリモートデスクトップ共有ソフトや VPN サービスを使用することが標準的でない場合、ポートチェック機能を定期的に使用して、デスクトップ共有ソ

フトあるいは VPN や VPS を使ってプラットフォームにリモートアクセスされているかどうかを判断する、

- クライアントや開発者の口座で、口座開設に同じか似通った文書を使用しているか、同じデジタル支払いサービス口座を使用している場合。追加レビューするために自動的にフラグを立てる、
- 異なる開発者口座間で、入札やプロジェクトのコミュニケーション用に同じもしくは似通った文書テンプレートを使用した場合、追加レビューするために自動的にフラグを立てる、
- 短期間に単一のクライアント口座から高評価を得ている複数の開発者口座で、特に口座開設に同じもしくは似通った文書が使用された場合、追加レビューするために自動的にフラグを立てる、
- プロジェクト入札数に比べて落札数が少ない口座と、高い入札率の開発者口座を追加レビューするために自動的にフラグを立てる、さらに、口座ログイン回数に比べてプロジェクト入札回数の多い口座にフラグを立てる、
- 完全な口座検証の前には、新設に開設された口座の活動は一切許可しない、
- 新規に開設された口座には特別な精査を行う。

フリーランスプラットフォームでプログラマーや開発者を雇う企業向け

- フリーランス候補者の身元を確認するためにビデオ面接を行う、
- 雇用前の前歴調査、薬物検査、指紋/生体認証ログインを行い、身元と主張された場所を確認する。仮想通貨での支払いを避け、他の身元証明書に対応する銀行情報の確認を義務付ける、
- リモートデスクトップアプリのようなリモートコラボレーションアプリを使用してフリーランス開発者と対話する際には特に注意する。フリーランス開発者に提供されるすべてのコンピュータのリモートコラボレーションアプリを使用不可とするよう検討する、
- 採用候補者やそのプロフィールから入手するのではなく、検索エンジンやその他の企業データベースを使って確認された連絡先を使って、リストに掲載された企業や教育機関に職歴や進学歴を直接確認する、
- 採用候補者の氏名のつづり方、国籍、主張された場所、連絡先、学歴、職歴、その他の詳細 が、開発者のフリーランスプラットフォームのプロフィール、ソーシャルメディアプロフィール、外部ポートフォリオウェブサイト、支払いプラットフォーム口座、ならびに査定された場所と勤務時間において一致しているかどうかを点検する。ポートフォリオウ

ェブサイト、ソーシャルメディアプロフィール、あるいは開発者プロフィールが単純な場合には、特に注意すること、

- 企業が最初に IT 労働者を見つけた元のフリーランスプラットフォームウェブサイトとは別のプラットフォームで通信することを開発者が要求している場合には注意する、
- 開発者に書類やノートパソコンのような業務用機器を送る場合、開発者の身元証明書に記載されている住所にのみに送り、開発者がノートパソコンや他の品を知らない住所に送るよう要求した場合には、追加の書類を確保する。開発者が身元証明書に記載された住所で物品を受け取れない場合は、疑いをもつこと、
- 契約した IT 労働者が不正に行う可能性がある承認を得ていない小口取引に用心すること。ある事例では、米国企業に開発者として雇われた北朝鮮 IT 労働者がその企業の支払い口座に不正に請求し、数カ月のうちに少額の課金を 30 回も続けて合計 5 万米ドルを盗んだ。この米国企業は開発者が北朝鮮人だったことを知らず、金額が少額だったため、継続的な窃盗行為にも気づかなかった。

禁止中の、あるいは制裁を受けるべき行為に関わった場合の結果

関連する金融取引の処理を含めて、北朝鮮 IT 労働者関連の活動に関与または支援する個人や企業は、禁止あるいは制裁対象になる行為に関与した場合、起こりうる法的結果を認識すべきである。

国連安保理事会決議 2321、2371、2397 には、海外の北朝鮮労働者から得られる収益が北朝鮮の核兵器や弾道ミサイルプログラムに寄与していると強調している。国連安保理事会決議 2375 は、国連安保理事会の 1718 委員会の事前承認がない限り、国連加盟国が自国領土への入国に関連して、その管轄内の北朝鮮国籍者に新規の労働許可証を提供したり、失効した許可証を更新することを禁止している。国連安保理事会決議 2397 は、
全加盟国に対し、労働許可が発行されたか、発行がいつ行われたかにかかわらず、2019 年 12 月 22 日までに、自国管轄内で収入を得ている北朝鮮国籍者を本国に送還するよう求めている。

財務省の外国資産管理室 (OFAC) は、特に以下のようなことを行ったと判断される人に金融制裁を発動する権限を有する:

- 北朝鮮政府や朝鮮労働党のために、サイバーセキュリティを損なうような重大な活動に従事した、
- IT 産業において北朝鮮のために活動した、
- その他の悪意あるサイバー対応活動に従事した、

- 北朝鮮からの物品やサービス、あるいは技術の重大な輸入や輸出に少なくとも一回従事した、

- 受け取られたいかなる収入あるいは物品が北朝鮮政府または朝鮮労働党の利益になるような、北朝鮮へ、または北朝鮮から、あるいは北朝鮮政府や朝鮮労働党を代理して動いている人物へ、または当該人物から、直接あるいは間接的にソフトを販売、供給、譲渡、あるいは購入した、

- 北朝鮮政府や朝鮮労働党に対して、あるいはその支援のために、財政的、物質的、技術的支援、もしくは物品やサービスを実質的に支援、後援、提供した。

例えば、2018 年に米国は、延辺銀星網絡科技有限公司という中国に拠点を置く技術企業を制裁に指定した。この会社は名目上は中国の IT 企業だが、実際には北朝鮮人により運営管理されていた。この会社は、フリーランスの雇用フォーラムでの身元証明要件を回避するために、ロシアに拠点を置くダミー企業 Volasys Silver Star 社を設立していた。

さらに、外国金融機関が北朝鮮との重大な取引を故意に行ったり促進したことや、北朝鮮関連の大統領命令もしくは北朝鮮関連活動に関する大統領命令 13382（大量破壊兵器拡散者とその支援者）に基づいて指定されている人物のために重要な取引を故意に行ったり促進したりしたことを、財務長官が国務長官と協議の上、判断した場合には、その金融機関は、他の制限の可能性もあるが、米国内でコルレス口座や銀行経由支払口座を保持する能力を失う。

OFAC は、経済制裁施行ガイドライン 31 C.F.R. part 501 付録 A に記載されている通り、制裁規制の明らかな違反を捜査し、施行権限を行使する 。また、31 C.F.R. part 501 の北朝鮮制裁規則に違反する者は、適用可能な法定最大限の罰金または原取引の価値の倍のいずれか大きい方の民事金融処罰を受ける可能性がある。

さらに、米国の対敵対者制裁措置法 (CAATSA; Public Law 115-44) Section 321(b) (22 U.S.C. § 9241a)は、2016 年(22 U.S.C. § 9241 et seq.)北朝鮮制裁と政策強化法を修正したものであるが、世界のどこかで北朝鮮国籍者や北朝鮮国民によって全部あるいは一部が採掘、生産、製造された重要な商品、製品、物品が 1930 年関税法(19 U.S.C. § 1307)の下で輸入が禁止されている強制労働品であるという反証可能な推定を作り出した。これは、こうした商品が米国のいかなる通関地からも入国が認められず、拘束、差し押さえ、没収の対象となる可能性があることを意味する。違反すると、民事罰金や刑事訴追という結果もありうる。しかし、CAATSA に基づき、米国税関国境警備局(CBP) 長官が、その商品が受刑者労働、強制労働、年季奉公労働により生産されたのではないという明白かつ説得力のある証拠を見つけた場合には、米国への輸入は可能である。刑事上の制裁に基づく受刑者労働、強制労働、年季奉公労働（強制、年季奉公の児童労働を含む）で生産された商品の輸入禁止は、1930 年関税法の下に創設され、かくして 90 年近く実施されてきている。

司法省は、適用できる連邦諸法の捜査と訴追の責任を担っており、この法律の中には 国際緊急経済権限法 (IEEPA) 50 U.S.C. §§ 1701 et seq.、および銀行機密保護法 (BSA) 31 U.S.C. §§ 5318 と 5322 が含まれる。IEEPA 下では、北朝鮮関連の大統領令（例えば、大統領令 13722

と 13801）、大統領令 13382、北朝鮮制裁規則 31 C.F.R. part
501 を含む IEEPA に従って発行された免許、命令、規則、禁止に故意に違反する、違反を試みる、違反を共謀する、あるいは違反を引き起こすことは犯罪である。故意に IEEPA 違反をした者は、最高 20 年の禁固刑、最高 100 万ドルあるいは総利益の倍の罰金、およびこうした取引に関係する全資金の没収を問われる可能性がある。BSA は金融機関に、他のことと共に、効果的な反マネーランドリング防止プログラムの維持と、FinCEN への特定報告書の提出を義務付けている。BSA に違反する者は、最高 5 年の禁固刑、最高 25 万ドルの罰金、そのような違反に関わった財産の没収を問われる可能性がある。IEEPA、BSA、およびその他の適用可能な連邦諸法に違反する企業やその他の団体も刑法上の訴追を受ける可能性がある。司法省は、外国のパートナーと協力して、米国や海外での犯罪捜査や訴追の支援のために、証拠を共有している。

財務長官や司法長官は 31 U.S.C. § 5318(k)に基づき、米国内のコルレス銀行口座を維持する外国金融機関の海外保管記録を召喚することができる。財務長官や司法長官は、外国金融機関が召喚に応じなかったという書面による通知を米国金融機関に出す場合には、米国金融機関は 10 日の営業日以内にコルレス銀行関係を停止せねばならない。それができなかった場合には米国金融機関は日割りの民事罰金の対象となることもある。

司法のための北朝鮮報奨金

サイバースペースでの北朝鮮の過去または進行中のものを含む、不正活動に関する情報を持っている場合には、国務省の司法のための報奨プログラムを通じてそのような情報を提供すれば、最高 500 万ドルまでの賞金を獲得できる資格を得る可能性がある。詳細については、以下を閲覧のこと。https://rewardsforjustice.net/index/?north-korea=north-korea.

付録

北朝鮮 IT 労働者に関する国連専門家委員会の報告

国連安保理事会の北朝鮮に関する 1718 制裁委員会は、北朝鮮に対する国連安保理事会決議に概略が説明されている措置の実施に関して、国連加盟国、関連国連機関やその他の関係者から情報を収集、検討、分析する専門パネル（パネル）によって支援されている。さらにパネルは、1718 委員会に中間、最終報告書を提出することによって、制裁実施状況を改善するための勧告も行う。こうした報告書は以下で閲覧できる:
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

パネルは、国連指定の軍需産業部 (MID)の下に属するような北朝鮮 IT 労働者の多数の事例を調査し、パネルの中間報告書にこうした調査の情報を掲載しているが、以下のような内容が含まれる:

パネルは、2019 年中間報告において北朝鮮 IT 労働者について初めての報告を行ったが、北朝鮮の核と弾道ミサイルプログラムの監督的役割を果たしてきたとして指定された MID は、傘下の商社を利用して、ソフトのプログラマーや開発者のような北朝鮮の情報技術労働者を海外に派遣し、外貨獲得に役立てていると指摘した。当時、ヨーロッパ、アジア、アフリカ、中東にいた北朝鮮 IT 働者は、その身元を偽ってフリーランスの仕事を海外のウェブサイトから得てていた。悪意のない情報技術業務と並行して、北朝鮮 IT 労働者 は、北朝鮮サイバー活動家の金融制裁回避を支援するために、仮想通貨などの資産の窃盗を含めて不法な業務を行っていた。

パネルは 2020 年最終報告書において、北朝鮮 IT 労働者への調査を続け、海外の北朝鮮 IT 労働者の大半は MID の従属下の企業によって雇われていることを明らかにした。2019 年までに、MID は収益創出のために少なくとも 1 千名の IT 労働者を海外に派遣し、頻繁にその下部組織やダミー会社を使ったという疑いがあった。しかし、彼らの曖昧にするテクニックのため、海外および北朝鮮内の IT 労働者の本当の数は明らかではない。パネルは、北朝鮮 IT 労働者はその身元を明かさずにフリーランスの IT 業務を獲得するためにさまざまな方法を使っているが、その中には、フリーランス開発者プラットフォームに口座を開設して、特に中国、ロシア、ウクライナ、セルビア、カナダ、および米国といった世界中の無意識のクライアントから仕事を得ている、と指摘した。さらにパネルは、北朝鮮 IT 労働者チームと中国、ネパール、およびベトナムにおける関連企業に関するいくつかの具体的事例について調査した。

パネルは、中国とロシアでの数々の北朝鮮 IT チームを調査し、2020 年中間報告書にその調査の詳細を記した。パネルは、MID の従属下にある何百人もの北朝鮮 IT 労働者が 2019 年、2020 年に中国で活動しており、第三国の個人名義のフリーランスプラットフォーム口座に不正にアクセスしたと指摘した。さらにパネルは、北朝鮮 MID の従属下にある IT 労働者の数々のグループが 2019 年、2020 年にロシアで活動し、情報技術フリーランスプラットフォーム、仮想通貨ウェブサイト、支払いウェブサイトに偽りの外国人身元証明を使ってアクセスしたことを指摘した。

パネルの 2021 年最終報告書によると、北朝鮮 IT 労働者は、偽りの身元証明書提出、VPN サービスの活用やダミー会社の設立などを含めて、北朝鮮が国際金融制度へのアクセスのために利用しているのと同じような曖昧化の方法を使って雇い主のデューデリジェンス努力や KYC/AML 実施要領を回避することができる。さらにパネルは、北朝鮮が使う大半の口座は中国国内の拠点で運営されている、と指摘した。精査を避けるために、これらの口座は IT 業務の採用を求める可能性のある顧客との連絡が確立されると「オフサイト」となってしまう。北朝鮮とつながりがあるユーザーは、さらに、セキュリティレベルが低いか、あるいはデューデリジェンス手続きがあまり厳格でない IT フリーランスプラットフォームを標的にすることもある。パネルは、IT フリーランスプラットフォームがコンプライアンス義務を履行する上で直面する危険性や、国際支払いシステムへの北朝鮮のアクセスを無意識に促進する危険性を特に強調し、国連加盟諸国がフリーランス IT 企業と協力して制裁コンプライアンス実施能力を促進・強化するよう勧告している。