STRIDER

シャドー・ネットワークの実態

北朝鮮のIT労働者とその中国の支援者

目次

概要

本報告書では、Strider独自のリスク評価手法とオープンソースのデータ収集を活用し、朝鮮民主主義人民共和国（以下、北朝鮮）関係者が用いる戦術、技術、手順（TTP）を詳細に解説します。これには、偽造身分証明書やフロント企業の利用、グローバルなフリーランス・プラットフォームの活用などが含まれます。また、中国、ロシア、東南アジア、アフリカ、中東にまたがる北朝鮮IT労働者の活動拠点を示すとともに、北朝鮮のサイバー活動を実質的に支援しているとして最近制裁対象となった遼寧中貿実業有限公司（Liaoning China Trade Industry Co., Ltd.）のような、中国に拠点を置く組織の役割についても明らかにします。

Striderでは、独自のサードパーティ・デューデリジェンス・ツールであるCheckpointを用いて、制裁対象団体とつながりのある35の関連組織を特定しました。この情報は企業が知らず知らずのうちに北朝鮮に関連する活動を支援することを回避するのに役立ちます。リスク軽減のため、企業はより厳格なデューデリジェンス・プロセスを導入し、制裁違反を未然に防ぎつつ、グローバルな人材パイプラインによってもたらされる巧妙化する脅威に常に注意を払う必要があります。

はじめに

技術系人材への需要増大とリモートワークの広がりとともに、グローバルな雇用ネットワークの裏側に見えにくい脅威が出現しています。偽造または盗用した身分証明書を用いて活動する北朝鮮のIT専門家らが、米国をはじめとする西側諸国の企業で続々と働き口を獲得しているのです。これらの人物は、フリーランスの開発者やエンジニアを装っていることが多いですが、実際には、**機密情報へのアクセス、地政学的な目標の推進、そして北朝鮮の資金調達を目的とした国家ぐるみの活動の構成員です。**このようにして得られた資金は、禁止されている兵器開発計画の支援や国際制裁逃れのために使用されます。不正な労働者を雇用した場合、西側諸国の企業は金銭的損失、知的財産の窃盗、データの侵害、風評被害のリスクを負うことになりますが、特に北朝鮮出身者を雇用した場合のリスクはきわめて深刻です。

2024年12月12日、米司法省は**数年間にわたり大陸をまたいで展開された大規模な詐欺作戦を指揮したとして、北朝鮮国籍の14名を起訴した**と発表しました。リモートの契約社員を装ったこれらの人物は、身元を偽り、時には実在の人物になりすまして数百社の企業に潜り込み、就職を果たし、資金を盗み、収益を直接平壌に送金していました。米財務省によれば、彼らの収益の最大90%が北朝鮮政府によって大量破壊兵器（WMD）と弾道ミサイル計画の資金源として使用されたといいます。

2025年1月までに、米国政府は取り締まりの手を一層強めました。米国財務省の外国資産管理局（OFAC）は、この計画に関与していた複数の個人と団体に対して制裁措置を発動し、西側企業が知らず知らずのうちに北朝鮮の国家支援活動のパイプ役になっている実態をより鮮明に浮かび上がらせました。そのわずか数日後、連邦捜査局（FBI）と司法省は、新たな起訴と公共広告を通じて脅威の重大性を強調し、北朝鮮のIT労働者を雇用することが知的財産の窃盗、データ侵害、米国および国連の制裁措置に対する直接的な違反につながる可能性があると警告しました。

これらの計画は単独で実行されているわけではありません。米国政府の起訴状や制裁措置に詳しく述べられている作戦の多くには、中国を拠点とする仲介業者やフロント企業が関わっています。中国には、北朝鮮の工作員がしばしば居住しており、グローバルなインターネットにアクセスしています。中国を拠点とする仲介業者は、北朝鮮がデジタル・プラットフォーム、決済システム、雇用市場を利用可能にする上で重要な役割を担っており、労働者の出所を曖昧にし、不正な収益の資金洗浄を容易にするための国境を越えたインフラを構築しています。

リモートワークとグローバル化した人材市場への依存度をますます高めている世界において、「革新」は「侵入」と隣り合わせです。

本報告書では、北朝鮮のIT工作員がデジタル労働者としてどのように潜り込むのか、どのようなシステム上の脆弱性を突いてくるのか、そして西側企業が現在直面している戦略的、法的、風評的リスクについて探ります。

戦術、技術、手順

北朝鮮のIT労働者は、目的を達成するためにさまざまな戦術、技術、手順（TTP）を駆使しています。これらのTTPは洗練されており、彼らの真の出所や意図を曖昧にするように設計されているため、検出や対策が困難になっています。

偽装身分証明書とフロント企業

北朝鮮のIT労働者が用いる主な戦術の1つが、偽の身分証明書とフロント企業の利用です。彼らはしばしば偽名で活動し、偽造した文書を使用して外国の企業に就職します。多くの場合、彼らは真っ当なITサービス企業に見せかけたフロント企業を設立します。このような企業を活動の隠れ蓑とすることで、疑いを抱かれることなく、世界中の顧客とやりとりできるようにするのです。

報告された事例の1つに、デンマークの電気自動車会社Fiskerが、2022年に北朝鮮のIT労働者を知らずに雇用したケースがあります。リモートワーカーであるKou Thaoは、自分の住所としてアリゾナ州の家を記載していました。しかし、その家は実際にはクリスティーナ・チャップマンという女性のもので、彼女は北朝鮮のためにラップトップ・ファームを運営し、給料を北朝鮮に送金していました。Fiskerは2023年にFBIから通告を受け、この従業員を解雇しました。

別の例では、暗号通貨企業のKrakenが、北朝鮮工作員の疑いありとしてFBIによってマークされていたのと同じメールアドレスを使用してリモートIT職に応募してきた北朝鮮工作員を特定しました。

フリーランス・プラットフォームの活用

北朝鮮のIT労働者は、Upwork、Freelancer、Fiverrなどのオンライン・フリーランス・プラットフォームを利用することがあります。これらのプラットフォームは、グローバルな顧客に向けてITサービスを匿名で提供する手段を提供します。西側企業のプロジェクトに入札することで、これらの労働者は北朝鮮のために外貨を稼ぎながら、同時に機密性の高い情報にアクセスする機会を得ることができます。これらのプラットフォームは匿名性が高いため、労働者の真の身元を追跡することは困難です。

サイバー犯罪とランサムウェア

北朝鮮の労働者の中には、サイバー犯罪に関与している者もいます。これには、ランサムウェアの展開、フィッシング攻撃、ハッキングなどが含まれます。これらの作戦は、ラザルス・グループのような北朝鮮の国家支援型ハッキング・グループと連携して実行されることがよくあります。このようなサイバー犯罪の収益は、北朝鮮政権に還流され、核およびミサイル開発計画の資金調達を支えています。

ソフトウェアとアプリの開発

海外で働く北朝鮮IT労働者の大部分がソフトウェアやアプリの開発に従事しています。彼らは、しばしば外国企業の看板の下で、グローバルな顧客に向けて販売されるアプリケーションを開発しています。これらのアプリには、北朝鮮の工作員によるユーザーの監視やデータ窃取を可能にする悪意のあるコードが埋め込まれる場合があります。また、こうしたアプリから生じた収益も、政権の資金源となります。

暗号通貨市場の操作

北朝鮮は、国際制裁を回避するために暗号通貨への関心を高めています。IT労働者は、マルウェアを使用した暗号通貨のマイニングや、取引所のハッキングに加え、身分を偽ってICO（イニシャル・コイン・オファリング）に参加するなどして、暗号通貨市場の操作に関わっています。

西側企業へのリスク

北朝鮮のIT労働者の活動は、西側企業に複数の重大なリスクをもたらします。こうしたリスクは、直接的な金銭的損失にとどまらず、知的財産の窃盗、データ侵害、風評被害など、より幅広い問題に及びます。

01 規制および法的リスク

北朝鮮のIT労働者と知らずに関与した西側企業は、国際制裁に違反してしまう可能性があります。これらの制裁は、北朝鮮政権を孤立させ、グローバル金融システムから切り離すことを目的としています。制裁違反が発覚した企業は、巨額の罰金、法的措置、国際的な事業活動への制約に直面する可能性があります。

02 風評被害

北朝鮮のIT労働者との関わりは、西側企業の風評を損なう可能性があります。フリーランス・プラットフォームのような正当なルートであっても、企業が北朝鮮工作員を意図せずに雇用していたことが露見すれば、その企業は世論の反発を受け、法的な影響に直面する可能性もあります。このリスクは、国防、金融、技術などの機密性の高い業界で事業を展開する企業にとって特に深刻です。

03 知的財産の窃盗

正当なITプロジェクトに身を置くことで、労働者はその企業が独自開発したソフトウェア、企業秘密、その他の形態の知的財産にアクセスする機会を得ます。窃取された知的財産は、北朝鮮の技術力向上に活用されるか、敵対国家や犯罪組織を含む第三者に売却される可能性があります。

04 データ侵害とスパイ活動

北朝鮮のIT労働者は、機密データにアクセス可能なプロジェクトに携わることが少なくありません。対象となるデータには、個人情報、財務記録、企業秘密などが含まれます。彼らが盗み出して北朝鮮に送信したデータは、スパイ活動に利用される可能性があります。このようなデータはダークウェブで売買される可能性もあり、被害を受けた企業は重大な財務的、風評的被害を受けることになります。

05 サイバー犯罪による金銭的損失

西側企業が北朝鮮のIT労働者に関連するサイバー犯罪活動の標的になるケースが増えています。とりわけランサムウェア攻撃は重大な脅威となっています。ランサムウェア攻撃は、身代金の支払いと、復旧にかかるコストの両方で、多額の金銭的損失を招く可能性があります。北朝鮮のIT労働者がこれらの活動に関与すると、その収益が敵対政権の資金源となることから、問題は一層複雑になります。

こうしたリスクを軽減するため、西側企業は採用活動において細心の注意を払う必要があります。特にフリーランスやサード・パーティのITサービス事業者と関わる際には注意が必要です。北朝鮮のIT労働者がもたらす脅威から身を守るには、デュー・デリジェンスの強化、強固なサイバー・セキュリティ対策、国際制裁の遵守が極めて重要です。

海外の北朝鮮IT労働者

多くの北朝鮮IT労働者が海外、特に中国、ロシア、東南アジアの一部、アフリカ、中東などの国々に派遣され、フロント企業の下で働いたり、偽名を使ったりしています。その拠点がどこにあるのかを把握しておくことで、組織は、該当する地域で活動するベンダー、フリーランス、下請け業者に対して、より厳しい審査を優先して実施することができます。

中華人民共和国

中国は、その巨大なデジタル経済圏と、北朝鮮に近いという地理的近接性により、北朝鮮のIT労働者にとって理想的な活動拠点となっています。その多くは大連、瀋陽、北京などの主要都市で活動しています。通常は中国企業や合弁企業に雇用されており、場合によってはフロント企業を設立することもあります。これらのIT労働者は、比較的規制の緩い環境を利用してサイバー活動に従事し、しばしば西側企業を標的にしています。

ロシア連邦

ロシア、特に極東地域には、相当数の北朝鮮IT専門家が居住しています。ロシアは、西側諸国との複雑な関係に加え、国際制裁への対応を迫られている状況にあることから、北朝鮮の工作員にとって活動しやすい環境となっています。ロシア在住の労働者は、多くの場合、ロシアのテック企業に就職するか、ロシアのサイバー犯罪ネットワークに協力しています。ロシア政府と北朝鮮の関係が一層緊密化する中、これらの労働者には一定の保護と活動の自由が与えられています。

アフリカと中東

北朝鮮のIT労働者は、ナイジェリア、ケニア、アラブ首長国連邦などの国々でも活動しています。これらの地域では、ソフトウェア開発から、ハッキング、ランサムウェア配布などのより悪質なサイバー活動まで、幅広い活動に従事しています。これらの労働者は、当該地域のサイバーセキュリティ・インフラストラクチャが整っていないのをいいことに、比較的処罰を受けることなく活動しています。

東南アジア

マレーシア、ベトナム、カンボジアは、急成長するテック産業と比較的規制の緩い環境を利用して活動を行う北朝鮮のIT労働者が居住していることで知られています。彼らはITアウトソーシング企業で働くことが多く、時には自ら事業を立ち上げることもあります。これらの国々では主に、ソフトウェア開発、ウェブ・デザイン、その他世界市場に容易に輸出できるITサービスに活動の重点が置かれています。

中国に拠点を置く組織の役割

Striderの調査は、他に類を見ないグローバルなデータによって支えられています。Striderは、高度なAI技術を用いて、世界中の65,000の独自のソースから100以上の言語でオープンソース・データを収集および処理しており、そのドキュメントの総数は160億件を超えています。このような幅広く奥深いデータにより、複雑なグローバル脅威ネットワークを明らかにすることができます。Striderは、そのグローバルな組織データを使用して、北朝鮮のリモートワーカー向けに機器を出荷するために虚偽の身分証明書を使用している可能性のある中国の仲介業者を特定しました。

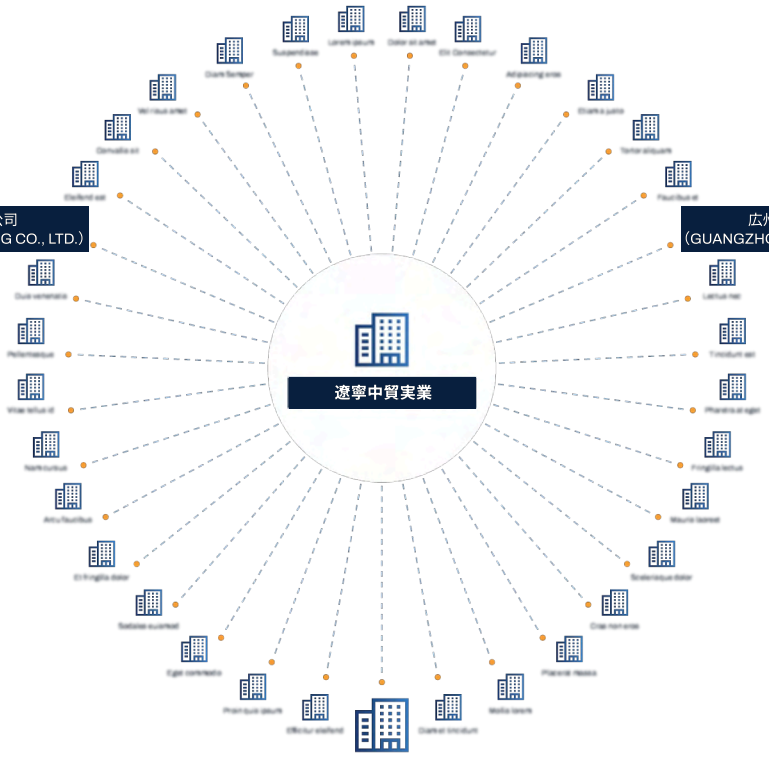
Striderは、2025年1月16日に発行された米国財務省外国資産管理局（OFAC）の制裁通知で言及されている中国関係組織を特定しました。

遼寧中貿実業有限公司（以下、遼寧中貿実業）は、北朝鮮の人民武力省第53局（以下、第53局）に機器を出荷し、海外でのIT労働者活動を可能にしている中国拠点の企業です。出荷されている物品には、コンピューター、グラフィック・カード、HDMIケーブル、ネットワーク機器などが含まれます。第53局は北朝鮮国防省の下部組織で、情報技術（IT）やソフトウェア開発を含むさまざまな分野のフロント企業を通じて収益を上げていることで知られています。

OFACの制裁条項には、「上記の指定対象者の米国内にある、または米国人の所有もしくは管理下にある、すべての財産および財産上の権利は凍結され、OFACに報告しなければならない。さらに、直接的または間接的に、個別または合計で、1人以上の凍結対象者によって50%以上所有されている事業体も凍結される」と規定されています。OFACは遼寧中貿実業を、大統領令13687号に基づいて財産および財産上の権利が凍結されている者である第53局に対し、実質的な支援、後援、または財政的、物資的、技術的支援や物品またはサービスの提供を行ったとして指定しています。

Strider独自のサードパーティ・デューデリジェンス・プラットフォームであるCheckpointを使用して遼寧中貿実業をさらに調査したところ、組織的および個人的なつながりを通じて同社と関連がある35の組織が追加で特定されました。Striderのデータは、これら35の組織が遼寧中貿実業と関連しており、したがって第53局を実質的に支援している可能性があることを強く示しています。このネットワークは、西側企業にとって重大なリスクとなっており、企業が知らず知らずのうちに北朝鮮の活動に関連する事業体と関わりを持ったり、その事業体に依存したりすることで、制裁違反の可能性や深刻な風評被害にさらされる恐れがあります。

ここでは、特定された35の組織のうち、3社を抜粋します。



01

オープンソース・データによると、この企業は中国において、繊維製品、建築資材、日用品、電子機器などの卸売および小売業として、また文化および芸術交流活動の主催者、技術の輸出入業者として登録されています。

02 オープンソース・データによると、この企業は中国において、鉱物製品、建築資材、化学製品の卸売業者として登録されています。

03 オープンソース・データによると、この企業は中国において、化粧品、個人用衛生用品、衣料品、日用品の卸売業者として登録されています。ただし、これは同社がオンライン上で宣伝している内容（業務用IH調理器、浴室用ミラー・キャビネット、バックパックの製造・卸売業者）とは若干異なっています。

画像1：StriderのCheckpointツールにおける遼寧中貿実業と関連する組織のスクリーンショット。

striderintel.com/jp

結論

この調査は、中国に拠点を置くフロント企業が、北朝鮮の不正なIT労働者の世界での活動をいかに促進しているかを明らかにしています。虚偽の事業関係の提供、収益の洗浄、国際プラットフォームへのアクセスの確保によって、これらの事業体は、より広範な不正エコシステムの重要な促進要因として機能しています。このネットワークの範囲と規模は、ほとんどの西側企業が認識しているよりもはるかに大きく、企業はセキュリティ、コンプライアンス、風評リスクの高まりにさらされています。このネットワークに対処するには、官民が連携して警戒する必要があります。

北朝鮮がこのような戦術を用いていることはよく知られていますが、身元を偽った労働者の脅威は、はるかに広範かつ組織的なものです。Striderはまた、中国、インド、パキスタンからのリモートワーカーが、偽の身分証明書、偽造された職歴、偽造された資格証明書を使用して西側企業内で雇用を確保し、しばしば機密システムやデータへのアクセスを獲得している事例も明らかにしてきました。この増大する脅威に対応するため、Striderは、組織が採用プロセス中に履歴書の詐称を検出し、フラグを立てることで、従業員の真正性を強化し、国家支援型の脅威のリスクを軽減するよう設計された新しいツールを提供開始する予定です。

遼寧中貿実業に関連する組織の一覧、本報告書に述べた情報の詳細、または今後のStriderのツールの情報については、info@striderintel.comまでメールでお問い合わせください。