なりすまし IT 人材の衝撃

～巧妙化、高度化するなりすまし IT 人材の脅威～

ライフデザイン研究部 主席研究員 柏村 祐

1.なりすましIT人材とは

世界的な DX の進展に伴い、国境を超えて IT 人材を活用する企業が登場している。ビジネスの現場でデジタル化を進めるうえで、高度な技術を有する IT 人材の需要は大いに高まっている。特にプログラミングやデータベースの開発を行える IT 人材は貴重な存在であり、リモートワークの拡大もあってオンラインでの受発注が進んだことから、国境を超えて採用されるようになっている。昨今では、ロシアのウクライナ侵攻に伴い仕事を失ったウクライナの IT 人材を日本企業が採用したことなどが、その典型的な事例と言えるだろう。

国境を超えて IT 人材の活用が進む中、従来の対面での採用では考えられなかった問題として、他人になりすまして応募するという事象が発生している。なりすましとは、悪意のある者が別人を装いシステムを利用したり、あるいは第三者とコミュニケーションしたりする行為を意味する。米国政府は、IT 人材の雇用における脅威として、IT 人材が身元を隠して仕事を受注するなりすましに注目している。

本稿では、悪意のある IT 人材が行うなりすましの実態を概観し、グローバル化が進む IT 人材活用において台頭するこの新たな脅威について考察する。

2.なりすまし IT 人材の実態

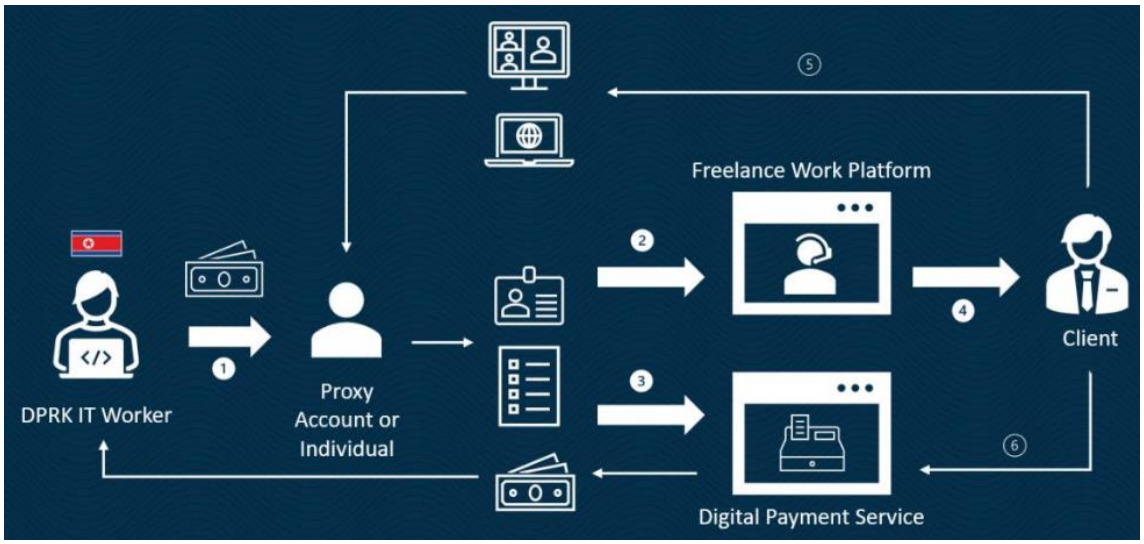
国境を越えて IT 人材採用の活用が進む中、他人になりすまして仕事を受注する不正行為を行う事例として、北朝鮮 IT 人材の活動が挙げられる。

米国政府は、2022 年 5 月 16 日に「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ダンス」を公開している。このガイダンスの中で米国政府は、北朝鮮 IT 人材関連の活動に従事または支援し、関連する金融取引を処理する個人および団体には、風評リスクと、米国および国連当局による制裁指定などの法的影響が生じる可能性を挙げている（注 1）。

米国政府は、ガイダンスの中で、北朝鮮の IT 人材は、兵器開発プログラムなどの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っていると指摘する。また、北朝鮮の金正恩委員長は、IT 人材が重要な外貨収入源であることを認識し、その業務を支援していると分析している。国外で活動する北朝鮮 IT 人材は、国外の工場や建設プロジェクトで働く北朝鮮労働者の少なくとも 10 倍以上の収入を得ているとされる（注 2）。

実際、北朝鮮 IT 人材が身元を隠し、リモートワーカーとして働くためのなりすましは巧妙化している。米国国務省によると、北朝鮮のなりすまし IT 人材がどのようにして報酬を得ているのかが明らかとなっており、その全体像は 6 工程から構成されている（図表 1）。最初に、北朝鮮の IT 人材は、身元を曖昧にするプロキシと呼ばれる仕組みを利用する。プロキシを利用することによりインターネット上における身元が曖昧になる状態を創り出せる。次に、フリーランスプラットフォームにアカウントを開設し、不正または改ざんされた身分証明書や資格情報を提出する。また、デジタル決済サービスのアカウントを開設し、不正に変更された身分証明書や認証情報を提出する。これらの不正行為により他人に成りすました IT 人材は、フリーランスプラットフォーム上で顧客から仕事を受注し、パソコンを通じて顧客との業務コミュニケーションを始める。仕事が完成すると、なりすましに気づかない顧客は、不正に開設された口座とは知らずに報酬を支払ってしまう。

図表 1　北朝鮮 IT 人材がなりすまして働き、報酬を得る手順



資料：米国財務省 HP より「https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_fact_sheet.pdf」

ガイダンスの中では、これらのなりすましリモートワーカーを見極めるための方法として、北朝鮮 IT 人材が活動している可能性を示す 4 つの「危険信号」と、企業が不用意に北朝鮮 IT 人材を雇用することを防ぐ 7 つの「デューデリジェンス手段（取引先の価値やリスクなどを調査すること）」が明示されている（図表 2）。

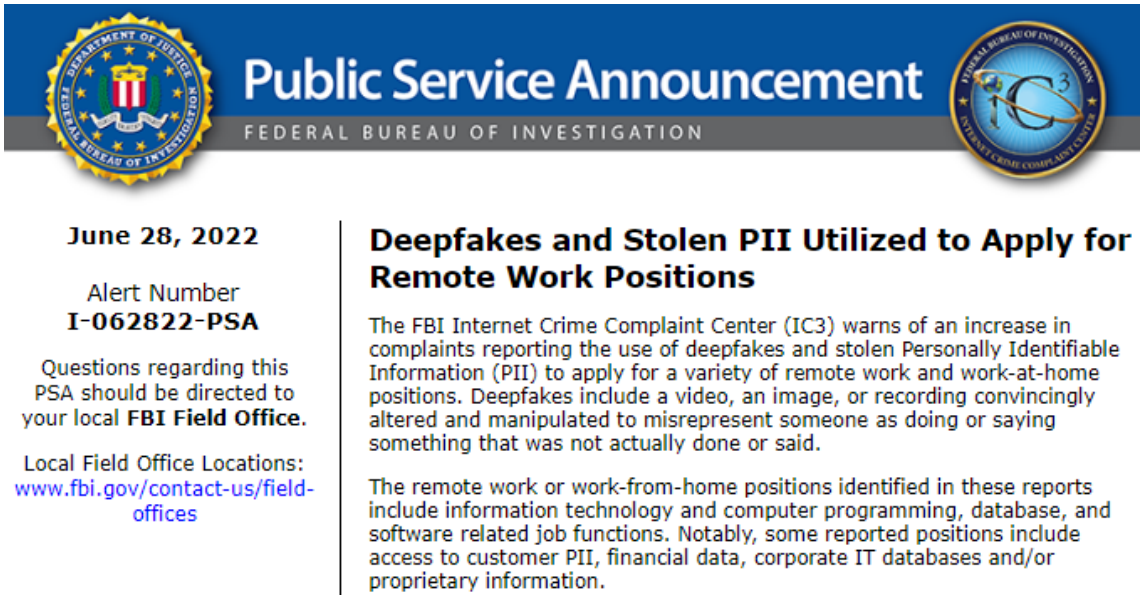
図表 2　北朝鮮のなりすまし IT 人材を見極める危険信号とデューデリジェンス手段

危険信号	比較的短期間に様々な IP アドレスから単一の口座への多数のログインが行われる場合、特にその IP アドレスが様々な国に関係している場合。
	支払いプラットフォームを通じての頻繁な資金移転、特に中華人民共和国にある銀行口座への送金あるいは暗号通貨による支払い要請。
	氏名のつづり方、国籍、申請された就業場所、連絡先情報、学歴、職歴、および開発者のフリーランスプラットフォームでのプロフィール、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でのプロフィール、および査定された場所や時間などの詳細情報における不一致。
	要求された業務時間内に業務を行えない場合、特に即時にコミュニケーション方法を通してタイムリーに労働者に連絡を取れない場合。
デューデリジェンス手段	提案書や雇用申請として提出された書類を（提出書類に記載された連絡先情報を使わずに）リストされた企業や教育機関に直接確認する。
	提出された身元確認書類に偽造がないか丹念に検査する。
	なりすましの可能性があるフリーランス労働者の身元確認のためにビデオ面接を行う。
	身元確認と申請された就業場所を確認するために、雇用前身元調査や指紋・生体認証によるログインを実施する。
	暗号通貨での支払いを避け、他の身元確認書類と合致する銀行情報の確認を求める。
	氏名のつづり方、国籍、申請された就業場所、連絡先情報、学歴、職歴、および申請された就業場所のその他の詳細情報が、開発者のフリーランスプラットフォームでのプロフィール、ソーシャルメディアでのプロフィール、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口座および査定された場所や労働時間などにおいて、一致しているかチェックする。
	開発者が身元確認書類にある住所で品物を受け取れない場合は疑いをもつ。

資料：米国財務省 HP より「https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_fact_sheet.pdf」を基に筆者和訳

また、米国政府は、高度化するなりすましの実態についても報告している。高度化するなりすましの事例として、FBI インターネット犯罪苦情センター（以下 FBI）は、顔や声を他人になりすまし、企業のオンライン面接を経て雇用される IT 人材の存在を挙げている。FBI による警告は、2022 年 6 月 28 日に公開されている（図表 3）。その概要は、様々なリモートワークや在宅勤務の職種に応募するために、他人になりすませる技術であるディープフェイクと盗まれた個人識別情報を使用し、企業の面接を受ける応募者が増加している現状があると警告している。ディープフェイクとは、ビデオ、画像、音声などを利用し、オンライン上の表情や声色を改変・操作し、第三者になりすますことが可能な技術である。ディープフェイクを活用するオンライン面接では、カメラで撮影された面接者の動作や唇の動きが、話している人の音声と完全に一致しておらず、また、咳やくしゃみなどの聴覚的な動作と、視覚的な動作が一致しないことがあると指摘している。この警告文書の中では、リモートワークや在宅勤務の対象となる職種として、情報技術、コンピュータープログラミング、データベース、ソフトウェア関連などが挙げられている（注 3）。

図表 3　FBI インターネット犯罪苦情センターによる警告文書



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 28, 2022

Alert Number
I-062822-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

資料：IC3HP より「https://www.ic3.gov/Media/Y2022/PSA220628」

3.なりすましIT人材を見極める必要性

以上みてきたように、他人になりすまして企業から仕事を受注し、報酬を得ているIT人材が存在する。本稿では、北朝鮮によるIT人材のなりすましの実態を見てきたが、このようななりすましは、北朝鮮に限らず悪意をもつIT人材が不正に仕事を受注する手段の１つと言えるだろう。

世界中で優秀なIT人材の争奪戦が起きており、企業がIT人材の即戦力を求める状況が続いている。国境を超えて活躍するIT人材は、企業のIT実践力を高めるために有効な人的リソースになりうる。技術力のあるIT人材は、世界中どこからでもリモートワークで従事できるため、今後も国境をこえたIT人材雇用は拡大するであろう。

このようにIT人材の雇用がグローバル化する中、国境を越えて活躍するIT人材に仕事を発注するうえで、提出された身元確認書類を精査し、きめ細かいビデオ面接を行うなどのデューデリジェンスの実践が欠かせない時代が到来している。

【注釈】

1) 米国財務省 HP より
https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_fact_sheet.pdf

2) 米国財務省 HP より
https://home.treasury.gov/system/files/126/20220516_dprk_it_worker_advisory.pdf

3) IC3HP より
https://www.ic3.gov/Media/Y2022/PSA220628