KnowBe4

北朝鮮の偽社員はどこにでもいる！

あなたの組織を偽社員から守るには

Roger A. Grimes
ロジャー・A・グライムス著

データドリブン・ディフェンス・エバンジェリスト

北朝鮮の偽社員はどこにでもいる！

あなたの組織を偽社員から守るには

目次

世界中の何千もの組織が、北朝鮮の偽IT労働者を誤って雇用している可能性がある。

はじめに

2024年7月23日に英文ブログで、2024年7月26日に日本語ブログで、KnowBe4が北朝鮮の「偽従業員」に侵入され、発見された経緯に関する情報を公開しました。（ https://www.knowbe4.jp/blog/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us ）。

ある意味で、これはラッキーでしたが、その "ラッキー（幸運）"を可能した懸命な努力があったことをご報告したいと思います。私たちが送ったノートパソコンをこの北朝鮮の偽従業員が異常な方法でアクセスし始めた時点で、この偽従業員をすぐに発見することができました。最初のセキュリティ警告から25分以内に、KnowBe4は、北朝鮮のハッカーのKnowBe4の基幹システムへのアクセスを完全にシャットダウンすることができました。そのため、北朝鮮のハッカーがKnowBe4の顧客データにアクセスすることは一切ありませんでした。

私たちが私たちのこのインシデントを公開した後、いくつかの他の組織や法執行機関が、「北朝鮮の偽従業員」問題について公に投稿してくれたことに感謝のメッセージを受け取りました。そして、このことから、他のどの企業も同じようなことをしていたにもかかわらず、さまざまな理由や恐れからその経験を非公開にしていたことが判明しました。私たちが公表したことをきっかけに、情報共有の連鎖が始まっています。

> 「数週間以内に、北朝鮮の労働者を雇用した、あるいは多数の偽の履歴書や応募書類に殺到しているなど、他の十数社から連絡があった……」。

数週間のうちに、北朝鮮人の従業員を雇用した、あるいは北朝鮮人からと思われる多数の偽の履歴書や応募書類が殺到しているなど、北朝鮮人の労働者が就職を希望する、他の十数社から連絡がありました。私たちに連絡してきた（あるいは私たちが連絡した）多くの組織は、彼らの情報やこの事実を非公開にするか、匿名にするよう求めてきています。「北朝鮮の偽従業員」の問題は、複雑で、国家規模の活動であり、世界中の何千もの組織が北朝鮮の偽従業員を誤って雇用したことがあるか、現在も関与している可能性が高いことが判明しました。

何百もの米国企業がこれまで非公開にしてきたと思われます。私たちは、フォーチュン500の企業が誤って北朝鮮の偽従業員を雇用したことや、同様なことが多くの中小規模の企業（従業員12人とか、20人の企業）で発生していることを確認しています。また、この偽装従業員の問題は、リモートワーカーを多く抱える企業にとっては深刻なリスクであると言えるのではないでしょうか。

このホワイトペーパーでは、北朝鮮の偽装労働者が国家的な産業としてどのようなものなのかを共有し、北朝鮮の偽装労働者に対処するための多くの兆候を共有し、そのような従業員の雇用を防ぐために組織が取るべき従業員の採用ポリシーを再考するための対策を説明しています。

注：北朝鮮の正式名称は朝鮮民主主義人民共和国（DPRK）。

北朝鮮従業員を故意に雇用した場合の法的な罰則

米国の法律と国連（UN）の制裁により、米国を拠点とする組織や米国に所在する組織（およびその他の国連加盟国）が故意に北朝鮮人を雇用することは違法と定められています。2017年、国連安全保障理事会決議2375（https://main.un.org/securitycouncil/en/s/res/2375-282017%29）は、国連安全保障理事会の1718委員会が事前に承認しない限り、国連加盟国や地域が北朝鮮人に仕事をさせることを禁止しました。国連安全保障理事会の米国財務省外国資産管理局（OFAC）は、経済制裁施行ガイドライン（連邦規則集第31編第501 条）および北朝鮮制裁規則（連邦規則集第31編第510条）を通じて、北朝鮮の組織または国民と故意に協力する個人または組織に制裁または罰金を科す権限を有しています。要するに、故意に北朝鮮の人物や組織を雇ったり、一緒に働いたりする者は、懲役刑や米国に拠点を置く企業や銀行と仕事ができなくなるなど、非常に厳しい罰則に直面する可能性があります。

注：米国は、北朝鮮の不正活動に関する情報に対して最大500万ドルの報奨金まで提供しています。

（https://rewardsforjustice.net/index/?north-korea=north-korea）

KnowBe4での北朝鮮偽装社員の採用

KnowBe4は、成長を続ける社内IT部門のAIチームのソフトウェアエンジニアを必要としていました。KnowBe4の求人サイト、https://www.knowbe4.com/careers に求人を掲載したところ、いつものようにたくさんの履歴書が届きました。私たちは履歴書を検討し、何度も面接を行いました。最終選考に残った求職者は、社内のさまざまな社員とZoomを使った遠隔面接を4回行い、推薦状を取り、さらに、この最終候補者から米国政府の公式身分証明書（実際には偽装の証明書）のコピーを送ってもらいました。私たちは通常の身元証明チェックを行いましたが、当時は過去の犯罪行為やその他のこれまでの雇用履歴において問題となる事案がなかったかに重点を置いて本人確認を行っていました。私たちは、同人の推薦状をチェックし、すべてが非常に好意的なものだったことを確認しました。これが雇ったはずの男です、彼はKyle（カイル）と名乗っていました。

この偽従業員の背後にいた偽装ペルソナは、香港で教育を受け、以前は米国を拠点とする複数の大企業で働いていた米国生まれのアジア系市民でした。私たちは、この名前とさまざまな身元保証情報が別の実在の人物から取られた偽装されたものであることを事後に確認することができましたが、これまでの採用プロセスでの身元調査では、この実在する本物の米国人の身元を偽装と判定することができず、身元確認を通過していたのでした。
注：本当のアメリカ市民のプライバシーを守るために、名字は伏せています。

上の写真は、KnowBe4の入社時の業務配属プロセスの一環として当社の人事システムへ登録されたものです。この写真は、私たちが採用プロセスで面接した人物のAIによるディープフェイク画像で、眼鏡をかけ、フォーマルな服装をしたプロフェッショナルに見えるように偽装されたもので、まったく無関係の人物の「ストック写真」の上に応募者の顔をオーバーラップさせて作成されたものです。

採用が決まり、仕事を引き受けた段階で、私たちはこの偽装社員へMacのワークステーションを送りました。このノートパソコンには、KnowBe4のセキュリティポリシーの要件である優れたセキュリティソフトとモニタリングツールがたくさん入っていました。これについては、受け取り本人は知らなかった（あるいは気がつかなかった）ようでした。さらに、KnowBe4のネットワークへログインするための多要素FIDO対応のYubiKeyも送っています。ノートパソコンを受け取る際に、その新入社員はもっともらしい言い訳を付けて、履歴書やその他の提出情報には記載されていない別の場所にノートパソコンンを発送するように依頼し、受け取っています。すぐに理解できるとは思いますが、これは北朝鮮の偽従業員によく見られる共通の兆候の一つです。KnowBe4の社員と契約社員は、それぞれの役割とタスクを実行するために必要なアプリケーションとデータにのみアクセスできるように限定されます。ほぼすべての場合において、KnowBe4では、非常に限られたリソースへのアクセスを許可しています。これは、新規採用の社員にとっては特に厳格です。KnowBe4では、新しく採用された従業員は、1 週間以上のトレーニングを受けた後、チームに配属され、期待される職務を遂行するためにさらなるトレーニングと監視を受ける必要があります。
トレーニング中の新入社員は、基本的に会社のEメール、Zoom、社内メッセージ（Slackなど）にアクセスでき、実際の顧客データにアク セスできない非常に制限されたトレーニングシステムも利用することができますが、共有ドライブへのアクセスは認められません。さらに、ワークステーションに機密データがローカルに保存されることはありません。

2024年7月15日午後9時55分（米国東部標準時）は、この偽従業員がノートパソコンを受け取り、電源を入れた日時です。その時点で、この偽従業員はパスワードを盗むマルウェアとセッション履歴ログを操作するツールをインストールしようとしましたが、何度も失敗しています。最初は、USBデバイスからマルウェアをダウンロードしようとし、それが失敗すると、ローカルネットワーク上にあるサーバーを使って同じことを試行しています。

MacのEDR（Endpoint Detection and Response）ソフトウェアは、マルウェアのインストール未遂によって生成されたアラートを即座に生成しました。当社の情報セキュリティ・オペレーション・センター（SOC）はこのアラートに注目し、数分以内にSlackを使って新入社員に連絡しました。この時点では、当社のSOC担当者は、北朝鮮の偽装社員がいることを知らなかったため、善意の援助を申し出るとともに、予期せぬマルウェアのアップロードやログファイル変更の警告メッセージが発生した正当な理由があるかどうかを確認しました。Slackのメッセージに応答したこの偽従業員は、アラートと一致しない奇妙な言い訳を返してきました。 このリモート従業員は、ローカル・インターネット・ルーターの速度問題のトラブルシューティング中にアラートが発生したのだと説明してきましたが、この説明が納得できなかったSOCの担当者は音声チャット（つまりSlackハドル）に参加するよう求めました。

このリモート従業員は、音声が聞こえない理由を言い訳にし、結局、Slackでのコミュニケーションを途中で打ち切りました。これはすぐにSOCエージェントの警戒心を高めるきっかけとなりました。数分以内に、上級情報セキュリティマネージャーにエスカレーションし、ログと追加の監視情報を収集する間、当社のネットワークから完全に隔離することを決定しました。このノートパソコンは、最初の警告から25分後の午後10時20分（米国東部標準時）頃にロックダウンされました。

さらに、KnowBe4のInfoSecエキスパートが加わり、収集したデータを世界的なサイバーセキュリティの専門家であるMandiant社やFBIと共有し、初動対応の調査結果を検証し、裏付けました。短期間のうちに、このインシデントは北朝鮮の偽装社員詐欺の兆候をすべて備えていることが決定的になりました。また、私たちはノートパソコンから遠隔操作でできる限りの情報を集めました。ノートパソコンで何が試みられたか、また有用なネットワーク情報など、多くのことを学びました。

また、後日判明したこと、Raspberry Pi OSを実行するデバイスがKVM（キーボード、ビデオ、マウス）デバイスとして当社のノートパソコンラップトップにリモートアクセスするように設定されていたために、リモートの北朝鮮従業員と彼を支援するエンジニアは通常のリモートアクセスアプリケーション（Microsoft Remote Desktop Protocol、Virtual Network Computing、SSHなど）が作成する奇妙で予期しないTCP/IPポートトラフィックの存在を当社のSOCに警告することなく、このノートパソコンにアクセスできたことでした。

さらに調査を進めるために、私たちは北朝鮮の偽装従業員計画をよく知っている他のセキュリティコンサルタントにコンタクトしました。そして、念のために、私たちはFBIにも参画してもらうことにしました。ほとんどの被害者組織はFBIに報告も協力を求めていないため、FBIは私たちがFBIに連絡し、協力を求めたことに感謝の意を示してくれました。

私たちは、この新入社員に会社のポリシー違反（WebカメラをONにしない、無許可でソフトウェアをインストールした、など）で解雇されることを告げ、ノートパソコンを送り返すことを依頼しました。驚いたことに、この偽装社員はノートパソコンを送り返してきました。私たちはそれをFBIに引き渡しました。
その後、機器の返却を要請した他の企業も私たちと同様に機器を取り戻したことを知りました。何故返却してきたのかの理由は、関与した加害者である北朝鮮のハッカー集団は違法行為のリストに盗難機器に関する重罪が追加されることを望んでいないためではないかと推測しています。

KnowBe4のCEOであるStu Sjouwermanに、このインシデント判明後即座に、報告がなされました。数日後、毎日の従業員全体ミーティングで、ステュは何が起こったかを共有しました。さらに数日後の2024年7月23日、KnowBe4は、北朝鮮の「偽社員」が偶然採用され、発見された経緯に関する情報を公に発表しました（https://www.knowbe4.jp/blog/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us）。

注：ステュは異例なほど透明性を重んじるCEOです。一つの例として、フィッシングの模擬テストに失敗した時や、本物のフィッシングをクリックした時（そしてすぐにそれを報告した時）など、このようなことも話題にして頻繁に公にしています。他のほとんどのCEOや経営幹部の方々は、自己の過失はなるべく口外しないのが一般です。スチュやKnowBe4を知る人々は、私たちが最新の経験を共有したとき、採用プロセスに問題があったことを世界に公表することになったにもかかわらず、驚きませんでした。

一部の批評家からは否定的な意見もありましたが、大半の反応は圧倒的に肯定的でした。多くの人々が、北朝鮮の偽装従業員の経験を共有した初めての勇気ある企業として感謝してくれました。私たちのブログ記事には大きな反響があり、何十ものメディアが私たちのストーリーを紹介するために記事を書いてくれました、中には事実誤認をしているメディアもありましたが、私たちはその後、以下のような明確なメッセージをブログで発信しました。
https://www.knowbe4.jp/blog/north-korean-fake-it-worker-faq
https://www.knowbe4.jp/blog/how-the-whole-world-now-knows-about-fake-north-korean-it-workers

サイバーセキュリティ業界では、組織が攻撃を受けた場合、法律で義務付けられていない限り、その事実を公に共有しないことがよくあるという長年の通例がありました。また、たとえ法律で義務付けられていたとしても、他の組織がより効果的に自社を保護できるようにするのに十分な有益な詳細情報を提供しないこともよくあります。これは、被害に遭った企業が、セキュリティの脆弱性があったことを認めることによる潜在的な法的影響を懸念し、また、その結果として生じるネガティブな報道や顧客の反応を心配していることが原因であるからであると思われます。

KnowBe4は、北朝鮮の偽装従業員を雇用した（または雇用しかけた）他の多くの組織から情報を収集して、他の組織に北朝鮮の偽装従業員の兆候を認識する方法と情報共有し、従来の採用プロセスを見直すための提案を行う必要があると判断しました。その目的のために、私たちはこの無料のホワイトペーパーを作成し、2つの公開ウェビナーを開催し、さらに多くの関連記事を公開しました。

私たちの経験が他の組織が北朝鮮の偽装従業員を雇用しないことに役立つのであれば、私たちの経験が生かされることになります。これこそが、私たちが目指していることです。

北朝鮮の偽社員の背景

北朝鮮の偽装従業員計画について理解すべき最も重要な点のひとつは、それが北朝鮮の指導者である金正恩を含む北朝鮮政権の最高レベルの指示のもとに、この計画が開発され、承認され、実行されていると いうことです。北朝鮮の偽装従業員プログラムは、他の業界の文献ではしばしば「DPRK ITワーカー」として知られ、北朝鮮、特に核兵器やその他の大量破壊兵器を含む制裁された兵器開発プログラムに多額の収入を提供しています。

北朝鮮は、今日の世界と北朝鮮の将来の成功において、ITとオンラインのサイバー活動とサービスが果たす役割を認識し、その重要性を理解しています。そのため、北朝鮮はITスキルとサイバーセキュリティに特化した多くの学校や大学を設立しています。最も有望なIT卒業生、特に英語が堪能な開発者の多くは、北朝鮮の偽装従業員プログラムに引き抜かれています。

このプログラムには、北朝鮮内外で数千人の北朝鮮人が関与していると思われます。北朝鮮の偽従業員は、北朝鮮のインターネットIPアドレス空間が非常に限られており、知られているという事実も含め、多くの理由から北朝鮮国外にいることが多いと思われます。北朝鮮が、北朝鮮国内からのインターネットアクセスを使って偽装工作を行っていたとしたら、このようなプログラムでは、より多くの隠蔽や経路変更が必要になるか、あるいはより簡単に発見されブロックされてしまうだろうと思われます。これに加えて、北朝鮮はインターネットへのアクセスが不安定で、頻繁に電力が遮断されるなど、インフラに問題があるため、このようなプログラムの実現は難しいだろうと考えられます。

北朝鮮にはこのような内部インフラの課題があるため、偽装従業員計画に関与する北朝鮮人は、中国、マレーシア、ロシア、アフリカ、東南アジア諸国など、外国や大陸にいることが多いです。中国が最も多いようですが、これは中国には強力なインターネットとエネルギーインフラがあり、運営コストが安く、食生活や文化がある程度似ているためだろうと思われています。北朝鮮の偽装従業員プログラムで稼いだ金のほとんどは、北朝鮮政府に送金されています。

偽装従業員プログラムの進化・進展

北朝鮮の偽装従業員プログラムは、まず、Fiverrのような一般的なフリーランスの仕事サイトで「フリーランス」の仕事案件を獲得するから始めているようです。世界中の企業の一時的なリモートワーク（つまり契約労働者）の獲得に成功したことから、ここをきっかけ深耕し、進展させていっているようです。これは、世界中でより多くのIT労働者や開発者に対するニーズが爆発的に高まっていた時期から起こっています。

北朝鮮の偽従業員の仕事は、ソフトウェアやアプリケーションの開発業務が中心で、グラフィックデザインは少ないようです。北朝鮮の偽社員は、特に以下のような「バックエンド」業務において、強力な開発スキルを持っていることが多いと思われます。インターフェイスやAPI（アプリケーション・プログラミング・インターフェイス）、そしてクラウド開発、暗号通貨、人工知能（AI）などの新しいテクノロジーなど多岐にわたっています。

合法的なものであれそうでないものであれ、あらゆる種類の開発者が、ソーシャルメディアやLinkedInやGitHubといった開発者向けサイトで、自分のスキルや過去の仕事を「宣伝」し始めています。今日の開発者は、履歴書と一緒にこれらのリンクを潜在的な雇用者に送るのが一般的で、雇用者はこれらのサイトを候補者が過去にどのような仕事をしているかを確認するために見ることができます。

北朝鮮は、世界中で提供されている新しいワークスタイルのWFH（在宅勤務）の仕事を利用し、ほとんどフリーランスの仕事から、よりフルタイムの仕事へと移行しています。

北朝鮮の偽従業員は、シンプルですが本物そっくりの（そして詐欺的な）履歴書やWebサイトを作成する方法を学びました。これらの偽の履歴書やウェブサイトは、偽の、あるいは盗んだIDを使っています。

COVID-19の流行（2019年～2022年）は、新しいワークスタイルとしての在宅勤務（WFH：Work From Home）シナリオを加速させ、従業員の割合が増加し、多くの場合、物理的な職場に出勤する必要がありません。今日、雇用主が従業員と一度も会ったことがないまま、あるいは従業員が組織の誰とも物理的に直接会うことを期待しないまま、従業員を雇用するのはごく普通のことになっています。これは特に開発者のポジションに当てはまります。開発者にオフィスでの勤務や、何日かはオフィスに出社する「ハイブリッド」な勤務を求める雇用主は、潜在的な従業員のかなりの部分を切り捨てることになるでしょう。

北朝鮮は、世界中で提供されている新しいワークスタイルのWFHの仕事を利用し、ほとんどフリーランスの仕事から、よりフルタイムのポジションに移行させています。北朝鮮の偽従業員は、かなりの部分が偽従業員であることが発覚したり、単に勤務成績が悪かったりするだけで、すぐに解雇されるにもかかわらず、できるだけ長く雇用され続けようとしています。偽従業員が働いていた国や会社にもよるが、偽従業員だと疑われた時点で解雇するには数週間から数カ月かかっています。そしてその間、彼らは北朝鮮のために収益を作り出しているのです。

成長する警告とその他の情報源

私たちが会社として経験をする前から、北朝鮮の偽社員の企てについては周知の事実として知られていました。2023 年10月25日に、英文ブログ（https://blog.knowbe4.com/fbi-warns-of-north- korean-social-engineering）で記述しています。当時、私たちは北朝鮮の偽装従業員計画の範囲、規模、巧妙さには気づいていませんでした。これは、ほとんどの企業でも同様であったと思われます。

かなり最近まで、北朝鮮人のIT労働者は主に暗号通貨会社、メガ企業、フリーランスの仕事を探していました。また、私たちは、身元調査によって、通常こうした詐欺で作成され使用される合成（つまり偽の）身分証明IDを見つけ出すことができると知りました。北朝鮮の偽従業員は、インタビュー中にカメラに映りたがらないことも知られていましたが、私たちは、彼らが盗んだ本物の米国IDを使用し、喜んで複数のオンカメラ•インタビューに応じ、AI合成の写真を作成し、実際の場所で必要なときに偽装IDを使用するとは考えていませんでした。

北朝鮮の偽社員がどのように活動するかは、時代とともに変化しており、以前は成功していた本人確認チェックをすり抜け、活動を拡大し、あらゆる業種や規模の組織を標的にし、大胆さを増しています。このことは、政府の報告書やメディアの記事によって、彼らの巧妙さと拡散の度合いが増していることが、長期にわたって文章にされて公になっています。

2022年5月16日、米国務省、米財務省、米連邦捜査局（FBI）は、「韓国情報技術労働者に関する指 針（GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS）」と題する16ページの詳細な報告書を発表しました（https://ofac.treasury.gov/media/923126/download） 。 この報告書には、大量の詳細情報が含まれてお り、このトピックに関心のある人は誰でも読むべきものです。しかし、当時は、報告書は米国の雇用主に対して、偽のフリーランサーを雇わないように注意するように警告しただけで、偽の正社員を雇わないように警告することには、あまり焦点が当てられていませんでした。

2022年5月のレポートは素晴らしいものでしたが、当時、メディアの注目をあまり集めることができませんでした。同じ時期に報道された、さまざまな偽装雇用主や偽装従業員に関する他のレポートや記事に埋もれてしまったのです。Mandiant（マンディアント）社が、2023年10月10日に、北朝鮮による高度な脅威の数々について長文のブログ記事で、北朝鮮の偽装従業員の兆候について簡単に言及するまでに、さらに1年半近くが経過しました（ https://cloud.google.com/blog/topics/threat-intelligence/north-korea-cyber-structure-alignment-2023/）。

北朝鮮の偽社員がどのように活動するかは時代とともに変化しており、過去にうまくいった身元確認チェックをすり抜け、活動を拡大し、あらゆる業種や規模の組織を標的にし、大胆さを増している。

記事の中で、Mandiant社は「…いくつかの資料は履歴書、職務経歴書、推薦状に焦点を当てていますが、それらはさまざまな求人に応募する際に活用できる可能性がある…」と書いています。
その1週間後の2023年10月18日、FBIは2022年5月に発表した報告書を更新し（https://www.ic3.gov/Media/Y2023/ PSA231018）、今度は北朝鮮の偽従業員の「手口」が正社員の偽従業員に進化していることを指摘しました。この発表は、10月25日のKnowBe4の投稿を含め、メディアの注目を集めました。KnowBe4は2023年12月13日に再び北朝鮮の脅威について、Nisosの新レポート（https://www.nisos. com/research/dprk-it-worker-scam/）に基づいて、ブログ（https://blog.knowbe4.com/north-korean-operatives-infiltrate-job-platforms）を投稿しました。

Mandiant社は、北朝鮮の偽従業員に関する多くのケースに調査し始めました。同社の主席アナリストのマイケル•バーンハートは、2024年2月21日にThe Defender's Advantage（守る側の利点）ポッドキャスト（https://open.spotify.com/episode/0xeaavXjlX2XLm3oibOv6g）で、この問題について語りました。

2024年5月までに、この問題はサイバーセキュリティ業界以外でも知られるようになってきました。ウォール・ストリート・ジャーナルは、300社以上の米国企業が北朝鮮の偽装従業員を雇用しており、アメリカ人やその他の外国人が彼らを支援していることを明らかにしました（https://www.wsj.com/politics/national- security/american-it-scammer-helped-north-korea-fund-nuclear-weapons-program-u-says-65430aa7）。2024年6月7日、ウォール・ストリート・ジャーナルは「ディープフェイク、詐欺師、ハッカーがサイバーセキュリティの仕事を狙っている」というタイトルの関連記事を掲載しました (https://www.wsj.com/articles/deepfakes-fraudsters-and-hackers-are-coming-for-cybersecurityjobs-e2a76d06) 。

報道でしばしば欠落していたのは、偽の社員候補が無防備な企業を欺くために面接プロセスで何をしたかについての豊富な詳細でした。さまざまな業種の組織（大手テレビ局、航空宇宙• 防衛関連企業、自動車メーカーなど）について言及されることもありますが、やはりフリーランサーを雇う大企業に焦点が当てられることが多く、中小企業や、時には非常に小さな企業も標的にされていることには触れられていませんでした。関連する詳細や推奨される防御策が情報共有されかったために、この問題に対応することがより難しくなります。そして最近まで、どのニュース記事も世界的に注目されることがありませんでした。ほとんどの組織は、北朝鮮の偽従業員問題の規模と巧妙さに気づいていなかったのが現実です。

それが2024年7月23日のKnowBe4のブログ投稿で一変しました。このブログで、私たちはこの問題の詳細、偽装従業員の写真入りで、その防御策とともに公にしました。このブログがきっかけで、翌日には何十ものニュース記事が掲載されました。今では、より多くの企業が、自社の北朝鮮偽装従業員の経験を安心して公に共有できるようになりました。

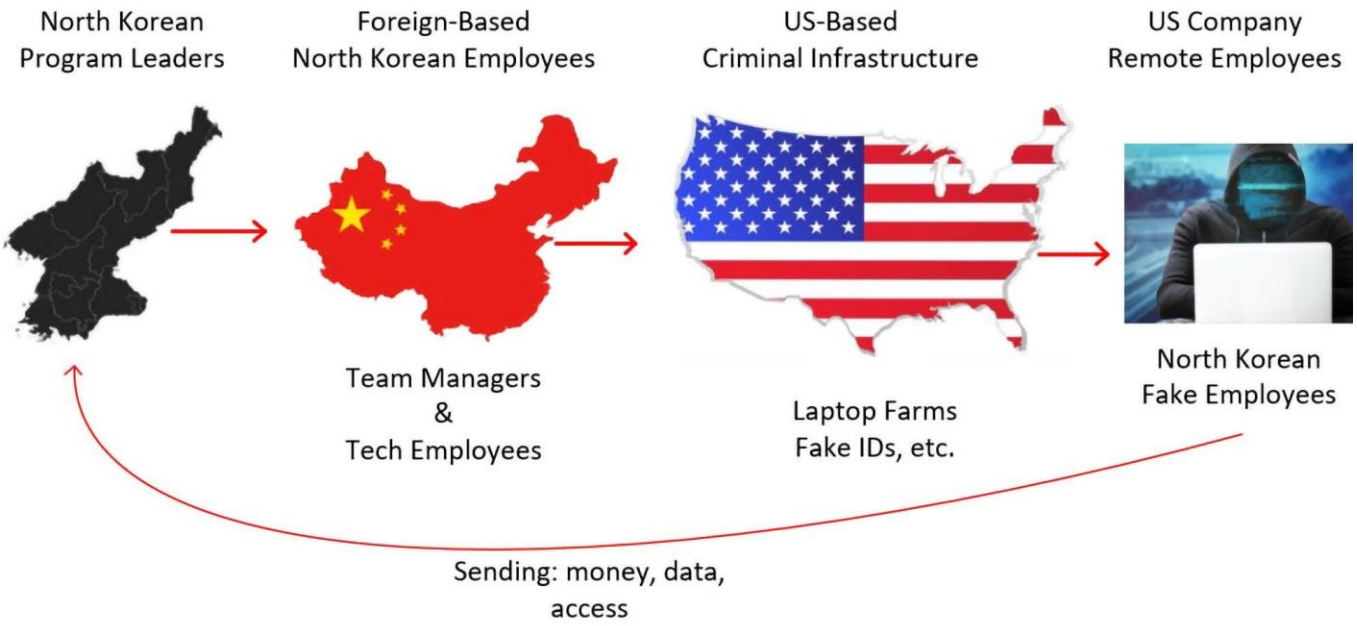
また、あなたが採用しようと考えている従業員が北朝鮮の偽装工作員であるか否かを確認する身元調査サービスを利用することができます。そのほか、誰でも利用できる無料ツールがいくつかあり、それらを使ってオープンソースインテリジェンス（OSInt）調査を自身で行うことができます。（例えば、https://github.com/shortdoom/gh-fake-analyzer/tree/main#malicious-github-accounts） 名前、メールアドレスや北朝鮮の偽従業員のIDについて、情報共有することもできます。(https://github.com/shortdoom/gh-fake-analyzer/blob/main/profiles/INVESTIGATIONS/ZachXBT_15.08.2024/Attackers.jpeg)
北朝鮮の偽従業員は、同じ偽または盗難IDを使用して、異なる組織で多くの仕事をしていることが多いため、確認された偽従業員の名前を知ることは、組織が騙されるのを避けるのに役立ちます。

注：政府のWebサイトに、確認された北朝鮮の偽従業員の名前とID情報の「グローバルリ スト」があれば、誰でも簡単に共有したり照会したりできるのではないでしょうか。

また、米司法省は、アリゾナ州の女性とウクライナ人の男性（https://www.justice.gov/usao-dc/ pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated- north）、テネシー州の男性（https://cyberscoop.com/wp-content/uploads/sites/3/2024/08/ FILED-INDICTMENT-Knoot.pdf）など、北朝鮮による偽装従業員計画を手助けしている米国市民やその他の外国人について、複数の別件の告発と逮捕を発表しました。

私たちは、より多くの組織が北朝鮮の偽装社員に関する経験やデータ搾取事案について共有し、情報共有を通して私たち全員が共に学び、みなさんの組織をこの北朝鮮の偽装社員の問題から守ることができるようになることを願っています。

一般的な北朝鮮の偽装社員の仕組み



北朝鮮の偽装社員スキームには、大まかに4つの部分がある:

- 北朝鮮に本拠を置くプログラムリーダー
- 他国に駐在する北朝鮮の偽装社員およびその管理者
- 韓国人以外の補助役(通常、仕事がある国に拠点を置く)
- 支払いの受領、偽のIDの生成または本物のIDの窃盗、偽装社員関連のWebサイトやプロジェクトの作成、推薦状などのリファレンスの提供、マネーロンダリング、文書偽造サービスなどを提供する支援基盤

北朝鮮の偽装従業員は、多くの場合、北朝鮮の大学で訓練を受けた熟練IT労働者や開発者です。彼らは通常、中国などの外国におり、共同アパート(居住スペース)とワークスペースに居住しています。日々の仕事は通常、忙しいコールセンターのような部屋で行われています。これを裏付けることとして、雇用主候補の多くは、従業員候補と面接した際に外部音で騒がしいことを指摘している。北朝鮮の偽従業員が稼いだ金のほとんどは、北朝鮮政府に送金されますが、現地のマネージャー(または管理者)が北朝鮮に送金する前に売上のごく一部を自分自身と業務遂行のために受け取っています。北朝鮮の偽装従業員は稼いだ収入のほとんどを得ることができません。これらの北朝鮮の偽装労働者にわずかな賃金で長時間労働を強いられています。その裏には、近親者は常に北朝鮮に留め置かれ、ほぼ強制的な労働者として利用されていると考えられています。複数の情報筋では、北朝鮮の偽装従業員は「人身売買」に近い労働条件のもとに強制労働を強いられていると考えられると結論づけています。

北朝鮮の偽従業員計画には、これを支援する支援基盤としての大規模な犯罪エコシステムが存在しています。北朝鮮の偽装従業員は、偽造、盗難、または購入したIDを使用します。これらのIDは、多くの場合、標的とされている国のものです。

北朝鮮の偽従業員は、雇用主から要求されると、多くの場合、偽造の「公式」文書を入手し、提出します。FBI（https://ofac.treasury.gov/media/923126/download）によると、過去に提出された偽造文書には以下のようなものがあります。

- 運転免許証
- 社会保障カード
- パスポート
- ソーシャルセキュリティナンバーカードなどの国家が発行する身分証明書
- 在留外国人カード
- 高校／大学の卒業証書
- 就労ビザ
- クレジットカード、銀行、公共料金の取引明細書

偽造、盗難、購入したID は、仕事の要件を満たしやすく、身元調査やその他のチェッ クに合格しやすいため好んで利用されます。場合によっては、本物の IDの所有者が、面接に参加したり、パソコンなどの会社支給品を受け取ったり、薬物検査を受けたりするなど、報酬を得て、支援しています。また、無関係の個人の IDを 使 う ケ ー ス で は 、多くの場合、不正に作成された公式の偽造 IDを使用しています。いくつかの司法手続きで文書化されているように（https://www.justice.gov/usao-dc/ pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated- north）、盗まれたIDを提供するサービスやWebサイトが数多く存在します。いくつかの報告書には、米国市民に違法に収入を得るチャンスを提供する闇サービスやWebサイト（やDiscordサーバー）について記載されているものがあります。その関係者は、外国人が「差別」されるような仕事を得る手助けをしていると考えることもあるようですが、このような行為は違法であり、北朝鮮人が制裁を迂回する手助けをしていることになっているのです。

Laptop Farm（ラップトップファーム）

通常、雇用主から郵送された機器を受け取るために、雇用主と同じ国に居住する取次役が存在します。彼らは、多くの場合、自宅やレンタルスペースなどにその機器を設置し、遠隔地の北朝鮮人（または彼らの雇った請負業者）がその機器にアクセスできるようにしています。このような場所を「Laptop Farm（ラップトップファーム）」と呼んでいます。ここには、さまざまな雇用主から90種類以上のラップトップが送られてきていて、設置されています。偽従業員を解雇した後、機器を取り戻したいくつかの雇用主は、ラップトップの蓋に組織名が記入された黄色い「付箋」が入っていたと報告しています。ラップトップファームの従業員が、どのラップトップがどの組織のものかを把握するために機器にラベルを貼っていたことは明らかです。

北朝鮮人の偽装労働者は、採用が決まると、ほとんどの場合、雇用主にノートパソコンやその他の機器を履歴書やその他の提出書類で事前に通知している別の場所に発送するよう依頼してきます。これは、北朝鮮の偽装社員の兆候として非常によく見られることです。彼らは、住居の変更や病気の親戚の手伝い、ガールフレンドとの旅行など、様々な偽の言い訳を考え出して、ノートパソコンやその他の機器の郵送を依頼する新しい場所はたいてい特定ができない、雇用主にとっては驚きの場所です。

これはおそらく、北朝鮮の偽装社員は数十から数百の継続的な偽の雇用案件に関与しており、新たな雇用が決まると、新たな取次場所へ新規雇用主の機器へ発送させるようにしています。このように、取次者がこの闇のビジネスから手を引いたり、または万一逮捕されたりすることを想定して、ラップトップファームは所在を特定されないように、北朝鮮はこのラップトップファームの取次者を巧みに変更するための一覧リストを使用しているとのだと考えられます。

注：今後、この北朝鮮の戦術が公になったため、ノートパソコンの発送先が求職の初期段階で一貫して使用される可能性があります。また、北朝鮮の偽装社員に関する現在の兆候も適時、変わると思われます。北朝鮮の工作員は、公になった戦術やこれに対する対抗策に関して常に情報を収集しており、戦術を柔軟に変えてきています。

この機器取次者は、多くの場合、採用された偽装社員の名義の偽造IDを所持しているが、目視確認に備えて本人の顔写真を入ったものになっています。遠隔地にいる従業員に機器を発送する雇用主は、機器の受取人が採用者本人であることを目視によって確認することは必須です。北朝鮮は、ほとんどの配送サービスでの本人確認は、受取人が提示するIDの確認だけで、依頼主が提供したIDとの比較チェックを行っていない現状を悪用しています。比較チェックを行っていれば、同一本人が採用面談から機器受領までを一貫して担当していないかぎり、ほとんどのケースでこの不正の配送は見つかるはずです。

北朝鮮の偽装従業員のスキームは、その国の国民が本物の履歴書を使い、面接に参加し、薬物検査を受け、備品を引き取るなど、雇用詐欺に一貫して関与し、新規採用を成約させます。その結果として生み出した仕事を遠隔地の北朝鮮労働者（または彼らが雇った請負業者）に引き渡すというものです。

北朝鮮の工作員は、その結果生じた仕事を他の外国や国内の請負業者に回すことが多く、この場合、彼らは請負業者に作業の一部または全部を引き継がせ、支払われた給与の一定割合を得えています。雇用主の中には、雇ったつもりの人物が、外見、声やアクセント、関連する知識や仕事の質など、実際の担当者とは異なっていたと指摘する方がいました。また、北朝鮮籍の偽装従業員が、会社の備品 を受け取る以外のすべての仕事をこなすこともケースもありました。

多くの場合、犯罪を支援するサービスがエコシステム全体に関与しています。偽造IDサービス、偽銀行、マネーロンダリング、暗号通貨サービス、暗号通貨取引所や「ミキサー」、「ミュール」、ラップトップファーム、下請け業者、履歴書作成者、ソーシャルメディアやGitHubのアカウント作成者、開発者、就職斡旋業者、偽装ID作成者、VPNサービス、VOIPサービスなどが含まれます。関与している関係者は、しばしば、行われていることが違法または非倫理的であることを知っていますが、北朝鮮が関与していることを知っているかどうかはわかりません

北朝鮮の偽装従業員は、同じ管理グループ内で、おそらくはより大きな組織レベルで、どのような戦術が有効で、どのような戦術が有効でないかを共有していると考えられます。何が失敗の原因なのか、どうすれば失敗を回避できるのか、どのようなサービスが自分たちの仕事を容易にし、成功に導いたのかを調べています。

彼らは、克服しなければならない戦術のタイプに応じて、シナリオごとに異なるテクニックを使っています。北朝鮮工作員は、雇用主が脅威を認識せず、脅威を検知・防止する防御策を導入していないことに大きく依存しています。北朝鮮の偽装従業員によって得られた収入は、北朝鮮政府に数億ドルから数十億ドルをもたらし、その多くは制裁されている兵器プログラムの資金として使用されています。

インバウンド／アウトバウンド戦略

多くの組織が北朝鮮の偽装従業員との「インバウンド」接触を報告していています。この接触は、雇用主のWebサイトで提供された求人や、合法的な求人のWebサイトから開始されました。いくつかのケースでは、北朝鮮の偽装従業員がソーシャルメディア（LinkedInなど）で開発者のマネージャーに接触し、求人がないか問い合わせてきます。

他の多くのケースでは、雇用主は北朝鮮人または偽のプロフィールとは知らずに、北朝鮮人の偽装労働者に接触（つまりアウトバウンド接触）しています。これらのケースのほとんどで、北朝鮮人はソーシャルメディア、GitHub、またはその他の求職サイトで、基本的ですが、信頼できるように見せかけたプロフィールを投稿しています。雇用主は、LinkedInで潜在的な従業員を探し、このような偽装のプロフィールに行き当てしまったケースもありました。

リクルーターは、北朝鮮の偽装従業員との接触において、インバウンドでもアウトバウンドでも大きな役割を果たすことが多く見受けられました。多くの雇用主は、信頼できるリクルーターによって、北朝鮮の偽装労働者を紹介されて、知らずに騙されたケースもありました。最近インタビューしたすべてのリクルーターが、北朝鮮人偽装社員による人材紹介業界の非常に大規模で深刻な問題を報告しています。

多くの雇用主は、昨年、北朝鮮の偽装従業員との複数のインバウンドおよびアウトバウンドの接触を報告していますが、チェックすべき兆候を知った今になって、北朝鮮の偽装従業員であることに気づいています。

偽のリモート従業員や契約社員は、今やすべての組織がこの対策を実施する必要があります。すべての組織は、この新しい脅威に対抗するために、雇用ポリシーとセキュリティトレーニングを見直すことは必須です。ニュースでは北朝鮮の偽装労働者ばかりが取り上げられていますが、実際はどこの国の労働者でも、偽装労働者の可能性はあります。

政府発行の身分証明書を持って本人に直接会うか、身元調査会社など信頼できるエージェントを利用して関連するチェックを行うか、少なくともどの組織は雇用しようとする人物が本当にその人物であることを確認するプロセスを導入する必要があります。また、多くのリモート従業員詐欺では、おとり商法が行われているため、雇用したリモート従業員が本当に働いているかどうかも確認する必要があります。

北朝鮮以外の偽装雇用者と偽装従業員

読者は、偽装雇用主や偽装従業員の問題があふれており、北朝鮮だけが生み出している問題ではないことを理解すべきです。10年以上前から、サイバーセキュリティ業界では（北朝鮮を含む）偽装雇用者や偽装従業員の横行が指摘されており、KnowBe4を始め、メディアでも繰り返しこの問題について記事が掲載されてきました。

https://blog.knowbe4.com/fbi-scammers-exploit-jobposting-sites-with-fake-jobs-to-steal-money-andpersonal-information

https://www.securityinfowatch.com/securityexecutives/article/53079753/the-dilemma-of-fake-jobscams-is-hard-to-stop-at-scale

https://www.linkedin.com/pulse/how-stop-job-scams-roger-grimes

https://blog.knowbe4.com/job-seekers-and-employers-beware

https://blog.knowbe4.com/north-korean-threat-actors-target-software-developers

https://blog.knowbe4.com/heads-up-north-korean-cybercriminals-use-fake-recruitment-emailsin-phishing-scam

https://blog.knowbe4.com/how-nks-cyber-criminals-stole-3-billion-in-crypto-to-fund-their-nukes

また、FBIは過去に何度も、個人を狙った偽装の雇用主について警告しています。

https://www.ic3.gov/Media/Y2024/PSA240604

https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-warns-cybercriminals-are-using-fake-job-listings-to-target-applicants-personally-identifiable-information

https://www.fbi.gov/contact-us/field-offices/newhaven/news/press-releases/fbi-new-havenwarning-college-students-of-employment-scams

多くの偽の求人が合法的な求人サイトに掲載されていることに注意すべきです。合法的な求人サイトを騙して偽の求人情報を掲載しているのは北朝鮮だけでありません。求人広告は、しばしば掲載された求人に正当性を与えることが必要です。確かに、潜在的な求人広告を疑っていない人はいないでしょうが、偽の求人広告に引っかかるリスクは、偽装の雇用ヘッドハンティングに引っかかるリスクよりもはるかに高いと言えます。正規の求人サイトは、多くの場合、偽の求人広告を探し、排除していますが、猫とネズミのゲームに負けることも多いと言わざるを得ません。イラン、南アジア諸国、ロシアを含む多くの国々には、偽の雇用主と従業員のふりをすることに特化した洗練されたグループが多数あると思われます。
偽の雇用主も非常に問題です。
これらの偽雇用者は、多くの場合、すでに働いている従業員を標的にし、その従業員から金を奪おうしています。

被害者から金銭的価値のあるものを奪ったり（例えば、偽の入社前手数料を支払わせたり、仕事を得るために高価な機器を購入•発送させたりする）ような詐欺行為も横行しています。また、このような行為で、雇用主を標的にしているものもあります。攻撃者はマルウェアやランサムウェアを拡散したり、金銭を盗んだり、機密情報を入手したりするために、従業員を感染させて、雇用主にアクセスしているものもあります。

最も悪名高いケースのひとつは、LinkedInの偽の求人広告が暗号通貨会社の既存従業員を誘惑して偽の求人に応募させ、結果的にその従業員の現在の雇用主が5億ドルの暗号通貨を奪われたというものがありまし https://www.techtimes.com/articles/277721/20220706/axie-infinity-hacked-500m-lost-via-fake-linkedin-job-listing.htm。この事件の犯人は、北朝鮮の有名な国家ハッキング•グループであるLazurusグループでした。採用プロセスには、あらゆるタイプの偽装従業員を防ぐための対策を盛り込むべきです。採用プロセスに関わるすべての従業員が偽装雇用者について教育されるべきです。また、偽装雇用主詐欺については、個人的な被害や組織への被害をもたらす可能性があるため、全従業員は偽装雇用主詐欺について教育されるべきです。

北朝鮮の意図

米国政府は、北朝鮮の偽装従業員プログラムの主な意図は給与やその他の契約金などの労働報酬の受け取りを通じて北朝鮮に違法な収入を提供することであると繰り返し述べています。関係する活動ログややりとりから確認された情報の大半は、偽従業員が単に雇われた仕事をこなし、継続的な報酬を得ていたと説明しています。他のケースでは、彼らは要求された仕事を実行しなかった（または、実行が不十分であった、ほとんど実行しなかった）が、他の悪意ある活動やスパイ活動は実行していないと報告されています。北朝鮮の偽装従業員プログラムの主な意図は、長期にわたって継続的な収入を集め、多くの場合、制裁を受けた北朝鮮の兵器プログラムに使用することにあるようです。

同時に、北朝鮮の偽従業員の潜入によって、盗まれた暗号通貨や悪意のある企業の銀行送金など、別の手段による金銭窃盗も多数確認されています。機密情報、知的財産、プロジェクト機密の流出も多く確認されています。また、北朝鮮の偽従業員が関与したソフトウェアプロジェクトに悪意のあるコードが意図的に挿入されたケースもあります。

これらの事例の多くは、関与した取次者が北朝鮮の大きな利益を生みだす侵害の重要性を認識していたケースでありますが、場合によっては、特定の国家組織が特定のスパイ活動の目標を念頭に置いて意図的に標的にされた可能性が高いと考えられています。

これに反する情報がない限り、どのような流出企業であっても、収益以外の目標が関与している可能性があると考えるべきです。とはいえ、調査されたケースの大半は、受託した仕事を通じて収益を得ることを主な目的としていました。被害者企業は、関係するエンドポイントに強力な監視システムを導入し、管理することで、必要に応じて、意図を証明し、すべての作業者の行動を検出するためのデータを収集できるようにする必要があります。

このホワイトペーパーの残りの部分は、北朝鮮の偽従業員の兆候と、雇用主が組織を守るために雇用プロセスをどのように更新すべきかを取り上げています。

北朝鮮の偽社員の兆候

北朝鮮の偽社員によく見られる兆候のいくつかを紹介します。

採用プロセス中

- アジア人（韓国人、中国人、マレーシア人、日本人など）、ヨーロッパ人または米国人であると偽装する。
- 英語が不自由であるにもかかわらず、アメリカに長年住んでいた、アメリカの大学しか出ていない、アメリカの有名企業に勤めていたと主張することが多い。
- 多くの場合、アメリカ／英語風の名前で米国市民を名乗るが、非常に訛りが強い。
- アジアの訛りに慣れている場合、その訛りは主張する国や地域のものではないことが多い（北朝鮮訛りであることが多い）。
- チェックすれば偽造がばれる偽のIDを使うことが多い
- 多くの場合、チェックすれば偽造がばれる偽の身分証明書を提出する。
- 多くの場合、チェックすれば偽造がばれる偽の職歴を主張する。

- 提供された個人のWebサイトやプロフィール、GitHubのサイトは、基本的すぎる、何かを言っているようで内容が何もない、よく似たサイトやプロフィールを見つけることができる。
- しばしば主張されるこれまでの業績は、他者のものを流用している。
- サイトやプロフィールが比較的新しいか、各種の業績が作成／投稿された日付と同じ。
- 提供されたサイトやプロフィール以外でのインターネット上の足跡や履歴がない。
- 履歴書、ソーシャルメディアサイト、プロフィール、面接、質問への答え方、人事採用システムで選択または入力する内容などの間で提供される情報に矛盾がある。(配偶者の有無、住所など）
- すべての接続はVPNを使用
- 騒がしい（コールセンターのような）環境から面接に参加する。
- 提出されるすべての電話番号（候補者および照会先）は、バーチャルVoIP（Voice-Over-IP）番号。
- 候補者および推薦者のEメールアドレスは、常に一般的に使用されているパブリックEメールドメイン（Gmail.com、Hotmail.com、Outlook.comなど）のEメールアドレスを使用する。
- リファレンスに使われている電話番号やEメールアドレスは、実際の企業の電話番号やEメー ルアドレスではない。
- 1回または複数のインタビューでカメラに映ることをためらい、カメラが作動していないと言い訳することがある。

採用後

- 採用応募書類やこれまでの連絡に記載されていない場所への機器の郵送を希望する。
- 提供したデバイスで不要なリモートログインが検出される。
- 提供したデバイスがログインしている IP アドレスが、採用応募書類に記載された所在地と一致していない。
- 提供したデバイスでマルウェアが検出される。
- 提供したデバイスで異常な動作が検出される。
- ログファイルの変更、または提供デバイス上でのその他の隠蔽工作がある。
- 勤務時間が所定の国や地域と一致していない、Eメールや成果物はいつも深夜に送られてくる。
- スペルを間違えてはいけないもの、名前や住所などにスペルミスがある。
- 頻繁にメールアドレスを変更する（古いメールアドレスで検知され、シャットダウンされる）
- プロジェクト提出物の品質が一貫しておらず、インタビューに応じた人物の品質を満たしていない。
- カメラに映すことができなかったり、オンラインチャンネルからタイムリーなレスポンスが得られなかったりする（特に、彼らにとっては睡眠時間となる時間帯）。
- 仮想通貨や通常とは異なる/奇妙な支払い方法を要求する
- 仕事の代金を銀行に振り込むよう要求された場合、支払いのために提供された銀行口座の詳細が見知らぬ銀行であったり、公的記録と一致しなかったりする。
- 仮想通貨、暗号通貨、その他の一般的な両替サイト（PayPal、Venmoなど）への支払いを要求する。
- OSまたはアプリケーションの言語を韓国語に変更する。

従業員候補者が偽従業員であるかを確認する際に、これらの一般的な兆候のすべてに該当する必要はありません。しかし、それぞれのチェック項目を作成し、最終候補として検討されている候補者がこれらの兆候の一部でも合致する場合は、さらに精査し、本人保証の正確性を確認すべきです。最終的に北朝鮮籍の偽装社員や履歴書を発見した雇用主のほとんどが、過去の提出書類をチェックしてみると、さらに北朝鮮籍の偽装社員である可能性の高い候補者（通常の採用プロセスを経て最終選考に残らなかった者）を発見しています。

あなたの組織を守るには

北朝鮮人であろうとなかろうと、偽従業員はすべての雇用主、特に遠隔地でのみ勤務する雇用主にとって深刻な脅威です。リスクのある組織は、全従業員に対して次のような教育を行うべきです。
採用プロセスに関与する可能性のある対象者にリスクについて説明し、以下に挙げる各種の対策に実行することを検討してください。

採用プロセス中

- 経営陣がまだこのリスクを認識していない場合は、経営陣とこのリスクを共有し、経営陣の支持を得る。
- 採用プロセスの脅威を洗い出す。
- 採用プロセスを更新し、偽従業員を雇用するリスクへの対応策を策定する。
- 偽従業員の兆候を採用プロセスで共有する。
- 同時に、共有したプロセスを通して、既存のリモート社員に既存の偽従業員がいないことを確認する。
- 可能であれば、遠隔地で勤務する従業員には、必ず、従業員、チームリーダー、または組織の選ばれた代理人と、公的な身分証明書を持って直接面会し、確認するよう求める。
- すべての従業員候補と従業員は、リモートセッション（Zoom、Microsoft Teams、Slackなど）の間、常にカメラに映っていなければならないというルールを徹底する。
- 面接プロセスにおけるすべてのやり取りとビデオを記録しておく。
- 可能かつ合理的であれば、また従業員候補者が国内以外の訛りを持つ場合、同じ地域の訛りに詳しい信頼できる人物に会議に参加してもらい、アクセントの妥当性を評価する。
- 従業員候補者と推薦者からVoIP電話番号の使用をチェックする。
- 推薦状をチェックする。
- 職業上/仕事上のやりとりはすべて、合法的かつ公的に確認可能な業務用の電話番号とEメールアドレスに行うことを義務付ける（一般的な公開Eメールアドレスは許可しない）。
- 偽の従業員を探す身元調査を利用する。
- 候補者は、採用プロセスにおいて誰に提示する場合でも同じ ID を使用することを義務付け、プロセスにおける追加の身元確認者が最初に提出された ID のコピーを取得するようにする。
- 本人確認のため、候補者に指紋の提出を求める。

オプション：この最後の提案は、採用プロセスで北朝鮮の偽従業員を見抜く際に疑心暗鬼になったときにその候補者が本当に本人かどうかを判断するために使うことをお勧めするいくつかの質問を紹介します。疑わしい場合は、候補者が正直であれば簡単にわかるはずだが、答えをすぐに調べるのは超簡単ではない質問をすることをお勧めします。

例えば

- 社員候補がバージニア工科大学に行ったと答えたら、"ホーキーとは何か"、"フットボールチームがいつもスタジアムに入るあの曲は何か "と聞いてみよう。
- 従業員候補者が、ある特定の雇用主の下で働いていたと述べた場合、その企業で働いていた人なら誰でも容易に理解できるような質問をしてください。例えば、"あなたはマイクロソフトで働いていましたが、何色のバッジを持っていましたか？"と尋ねてみてください。本物のマイクロソフト社員なら、その社員のタイプに合った色を簡単に答えることができます。
- 「野球チームのマスコットの名前は？」
- 「SATは何点だった？」
- 「キャンパス内にある巨大な学生情報センターの名前は？」
- 「キャンパスの隣にある、みんなが通っていたバーの名前は？」
- 「キャンパスの目の前を走る大通りの名前は？」
- 「野球観戦で食べられる主な食べ物といえば？」
- 「あなたの居住するところにはHOA（Home Owners Association）はありますか」？
- 「選択兵役に登録する必要がありましたか？」
- 「その州では何歳で運転免許を取得できたのですか？」
- 「オートデスクで働いていたのですね。どんなインスタントメッセージングシステムを使っていましたっけ？」

現実的に考えて、面接の過程でそこまで疑心暗鬼になるのであれば、おそらくそのポジションの最終候補者として考慮すべきではないと考えられます。

採用後

- 支給されたデバイスは、特に最初の雇用期間中は、必要最低限のアクセスしかできないようにロックする。
- 異常なアクティビティ、マルウェア、予期せぬ言語の変更、ログの変更についてデバイスを監視する。
- 予期せぬリモートログインの兆候を探す。
- 採用プロセスで質問したのと同じ技術的な質問をし、その答えが面接で答えたものと一致しているかどうかを確認する。
- 通常の勤務時間での活動を監視する
- 研修中や他の従業員とコミュニケーションを取る際に、従業員にカメラに映ることを義務付ける。
- 少なくとも最初の試行雇用期間中は、ランダムに数回カメラに映るよう従業員に依頼する。

注：FBIは、米国企業に対し、偽従業員を最寄りのFBI支部に報告するよう奨励しています。

概要

4

偽のリモート従業員や契約社員は、今や誰もが心配する必要があります。すべての組織は、この新しい現実を反映するために、採用方針、プロセス、教育を見直す必要があります。

最近のニュースでは北朝鮮の偽従業員が話題になっていますが、実際にはどの国の人でも、また他人のふりをしたい人間なら誰でもなりえます。少なくとも、どの組織も、採用しようとする人物が本当にその人物なのか、政府発行の身分証明書とともに直接会ったり、関連するチェック を含む身元調査会社など信頼できるエージェントを利用したりするなど、身元を確認するプロセスを設けるべきです。また、多くのリモート従業員詐欺では、おとり商法が行われているため、雇用したリモート従業員が本当に働いているかどうかも確認する必要があります。

かつて私たちは、偽の従業員や雇用主の心配をする必要のない世界に住んでいました。しかし、時代は変わり、採用プロセスや新しい仕事を求める従業員はそれに応じて行動する必要があります。

その他の関連情報

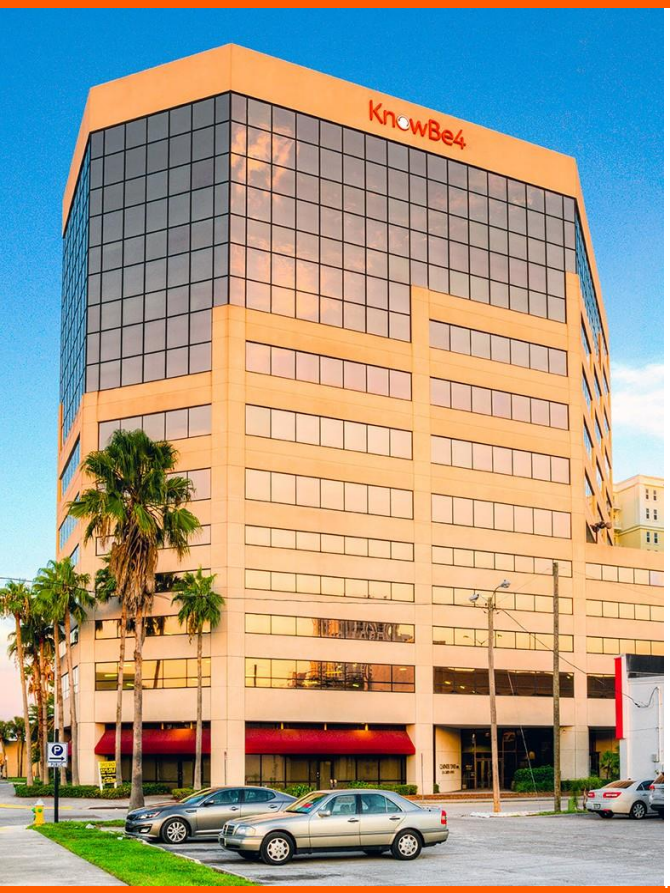
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。.

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alertボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償Email Exposure Checkツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、ビッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、7万社を超える企業や団体がKnowBe4を採用して、防御の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

詳しくは、www.KnowBe4.jpをアクセスしてください。

KnowBe4 Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F EGG 内
Tel: 03-4586-4540 | www.KnowBe4.com／www.KnowBe4.jp |