

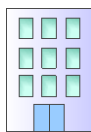
北朝鮮IT労働者に注意



警察庁は、令和7年8月27日、「北朝鮮IT労働者に関する企業等に対する注意喚起」を発表しました。北朝鮮がIT労働者を海外に派遣、IT労働者は、身分を偽って仕事を受注することで収入を得ており、これらを北朝鮮の核・ミサイル開発の資金源として利用していると指摘しています。

また、これらの人物を雇用してしまうと、北朝鮮の資金源となるだけでなく、会社の機密情報が窃取される可能性があります。

本年、京都府下で、こうした北朝鮮IT労働者と思われる人物による業務契約の事例がありましたので紹介します。



IT関係の求人サイトを通じて採用

リモート面談を実施



- ・ 海外居住
- ・ 日本とのハーフを自称
- ・ 流ちょうな日本語を話す

京都府内の企業A

外国人

企業Aは、外国人と業務委託契約を締結後、リモートワークのための業務用PCを送付。その後、同人からは、「PC送付先を恋人宅に変更してほしい」（一般住宅ではない住所を指定）「海外送金サービス宛てに給与を振り込んでほしい」などの話があった。さらに、短時間に複数のIPアドレスからの接続や夜間のログイン試行などの不審点が多数みられたことから、契約を解消した。

不審だった点

- ✓ 本人のプロフィールに、経験年数が比較的短いにもかかわらず、知識の習熟に時間を要するようなIT関連の資格や経験を多数保有と記載
- ✓ 日本に来日することができない理由を述べ、海外で仕事を請負う
- ✓ 当初、テレビ会議には応じたが、以降は様々な理由をつけて応じない（顔を出さない）
- ✓ 業務用PCの送付先について、存在しない住所やプロフィールと異なる住所を指定
- ✓ リモートワーク時に、アメリカやロシアなどの様々なIPアドレスから接続
- ✓ 夜間・休日を問わず、短時間に複数のIPアドレスから接続（→複数人からの接続の可能性）
- ✓ 振込先口座を海外送金サービスを指定

雇用する際に注意すべきこと

- ◆ 採用段階において、リモートのみではなく、直接面接するなど、身分確認を徹底
- ◆ 外国人による日本人へのなりすましや、北朝鮮を支援する日本人が業務契約や振込先口座を仲介するケースに注意
- ◆ 情報流出に繋がらないよう、企業データに適切なアクセス範囲を設定しておく
- ◆ 定期的に各種ログを確認し、不審なアクセスがないかを確認
- ◆ リンクトイン等SNSに掲載されている完璧（ハイスペック）すぎる経歴には注意

ご相談頂ければ、技術流出の手口などを個別に紹介させていただきます。
まずは、最寄りの警察署または、事務局までご相談ください。

京都府警察本部モノづくりプリアーズ事務局

075-451-9111

府警HPリンク

