栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

「なりすましエンジニア」にご注意を！
～北朝鮮IT労働者の手口と対策～

北朝鮮は、核兵器や弾道ミサイル開発の資金調達を行うために、身分を偽ったIT労働者を世界中に派遣しています
また北朝鮮のIT労働者は、企業のデータ流出、暗号資産・機微情報の窃取にも関与しています

北朝鮮IT労働者は、次のような方法で不正に収入を得ています
- 他国の国民になりすまし、身分を偽る
- 雇用や業務の受発注のためのオンライン・プラットフォームを利用
- 国外の企業からIT関連の業務を請け負う

令和８年7月31日、日本、米国、韓国等11カ国の関係機関は共同で、
「北朝鮮IT労働者に関する各国・企業等に対する注意喚起」
を公表し、北朝鮮IT労働者による脅威に対処するため、連携し、取組を強化しています

北朝鮮IT労働者の手口

○ 国籍や身分を偽る
　身分証明書の偽造・第三者へのなりすまし
○ アカウントの作成や採用面接に第三者の代理人を利用
○ 報酬の支払先として、銀行口座への直接振込を避けようとする
　国際送金サービスや暗号資産での支払いを求める
○ 「ラップトップ・ファーム」を運営し、所在地を隠蔽
　企業から支給されたノートパソコンを海外の第三者宅に設置し、北朝鮮IT労働者が遠隔でアクセスすることによって、実際の所在地を隠蔽（企業のアクセスログには現地のIPアドレスと支給端末が記録される）

採用・契約時に警戒すべき兆候（雇用または業務を発注する事業者向け）

○ 言語表現、顔写真、ビデオ会議の映像等において不自然な点がみられる
○ ビデオ会議形式の打合せへの参加を拒否する
○ 一般的な相場より安価な報酬で業務を募集している
○ 複数人でアカウントを運用している兆候が見られる
　やり取りする相手が時間帯によって変わる場合がある
○ 暗号資産での支払いを要求する

以上のような特徴が複数当てはまる場合、北朝鮮IT労働者が不正に仕事を得ようとしている可能性があります

雇用の際は身元確認の徹底を！
違和感を感じたら、警察へご相談ください！