広　報　資　料
令和８年９月 18 日
警　　察　　庁
国家サイバー統括室

北朝鮮サイバー攻撃グループ「WaterPlum」（ウォータープラム）及び北朝鮮 IT 労働者に関する我が国、米国、豪州及びドイツによるパブリック・アトリビューションについて

令和８年９月 18 日、警察庁及び国家サイバー統括室は、米国、豪州及びドイツとともに、北朝鮮を背景とするサイバー攻撃グループ「WaterPlum」（ウォータープラム）（関連名称： Contagious Interview）の攻撃手口や、北朝鮮 IT 労働者による外貨獲得活動及び採用応募活動の実態について、合同で文書を公表しました。これら実態は、民間事業者からの情報提供、警察庁関東管区警察局サイバー特別捜査部及び都道府県警察の捜査･分析等を通じて明らかになったものです。

このような悪意あるサイバー活動は、我が国だけでなく世界にとっての安全保障、経済活動上の脅威となるものです。

本件について注意喚起を行い、国内外に広く周知することは、我が国、そして世界のサイバー安全保障の強化に資するものであり、また、サイバー安全保障分野での国際連携の強化にも繋がります。

IT 技術者や民間事業者におかれては、本件注意喚起の内容を参考に、適切なセキュリティ対策を講じていただきますようお願いいたします。

１．公表資料の概要

- 北朝鮮を背景とするサイバー攻撃グループ「WaterPlum」が、世界各国の IT 技術者に対して暗号資産の窃取を目的としたサイバー攻撃を実行
  - 日本を含む 100 以上の国と地域で、少なくとも３万台以上とみられるマルウェア感染が判明
  - 約 7 千件の暗号資産ウォレットの情報が窃取されたほか、少なくとも約 17 億円相当の暗号資産が送金されたことを把握
- 北朝鮮 IT 労働者による活動実態を把握
  - 北朝鮮 IT 労働者が遠隔操作する「ラップトップ・ファーム」を国内で初めて把握のうえ、暗号資産を含め数億円の海外送金を把握
  - 国内暗号資産取引所（エンジニア職）へ北朝鮮 IT 労働者から応募があり、同社が面接を実施し活動実態を把握
- 「WaterPlum」及び北朝鮮 IT 労働者が朝鮮労働党中央委員会軍需工業部 313 総局の指揮下にあると特定

２．公表資料

- 北朝鮮サイバー攻撃グループ「WaterPlum」による IT 技術者を標的としたサイバー攻撃並びに北朝鮮 IT 労働者の我が国、米国及び欧州における活動実態等について