アジア系(と思われる)ハッカー集団

活動の背景として指摘される国



青：中国関連の情報窃取
赤：北朝鮮関連の金融・暗号資産攻撃

Lazarus Group
北朝鮮｜金融機関への攻撃・資金窃取

- 代表事件：バングラデシュ中央銀行から8,100万ドルを窃取（2016年）
- 主な手口：銀行間通信網SWIFTを悪用した不正な送金指示
- 指摘・起訴：米司法省が北朝鮮の偵察総局との関係を公表（2018・2021年）
- 名称の関係：警察庁はTraderTraitorをラザルスの一部と説明（2024年12月）

TraderTraitor
北朝鮮｜近年の暗号資産窃取

- 主な手口：偽の採用話で従業員を欺き、認証情報や送金過程を侵害
- DMM事件：委託先Gincoへの侵入を起点に約482億円を窃取（2024年）
- DMMへの関与を特定：警察庁・米FBI・米DC3（2024年12月）
- Bybit事件：約15億ドル流出、米FBIが関与を特定（2025年2月）

APT31
中国｜諜報・企業秘密の窃取

- 国家との関係：米司法省が中国国家安全部の湖北省の機関との関係を指摘
- 主な手口：記者等を装うメールや脆弱性を利用して侵入し、情報を窃取
- 主な標的：政府関係者、企業、記者、中国に批判的な人物など
- 当局の対応：米司法省が7人を起訴、米財務省が関係者等を制裁（2024年3月）

MirrorFace
中国の関与が疑われる｜情報窃取

- 活動の評価：警察庁・NISCが中国の関与が疑われる活動と指摘
- 主な手口：マルウェア付きメールや外部公開機器の脆弱性を利用
- 主な標的：政府・研究機関等の安全保障や先端技術に係る情報
- 分析・公表：警察庁・NISCが2019年頃からの攻撃を共同公表（2025年1月）

地図は活動背景の概略。中国への帰属の確度はAPT31とMirrorFaceで異なる。起訴は有罪確定ではない。

出典は各欄に記載。FBI：米連邦捜査局／DC3：米国防省サイバー犯罪センター。地図：Natural Earth。

欧米系(と思われる)ハッカー集団

活動背景・関係者の所在





赤：ロシア関連の犯罪・国家活動

青：米国・英国（地理的参考）

Qilin
犯罪集団｜ロシア系とみられる

- 暗号化と窃取情報の公開を脅し、身代金を要求
- アサヒグループHD（2025年）で犯行声明
- ロシア系との評価／アサヒ事件は集団自身の声明として記載

分析：NTTセキュリティ・ジャパン（2025年10月）

LockBit
犯罪集団｜ロシア拠点

- 協力者に攻撃ツールを提供し、二重恐喝を展開
- 英米等が共同捜査／運営者の特定・制裁を公表
- 運営側と攻撃を実行する協力者が分業する仕組み

ロシアとの関係を指摘：英NCA・英政府（2024年5月）

DarkSide
犯罪集団｜ロシア拠点

- 協力者が侵入・交渉を担当し、身代金を分配
- Colonial Pipeline（2021年）／FBIが関与を認定
- 事件ではパイプライン操業が停止し、燃料供給に影響

事件への関与を認定：米FBI（2021年5月）

Evil Corp
犯罪集団｜ロシア拠点

- 銀行情報の窃取・不正送金、ランサムウェア恐喝
- 米英が関係者を特定／米国で起訴・制裁（2019年）
- 英NCAはロシア情報機関との関係も公表している

ロシアでの活動・国家との関係を指摘：英NCA（2024年10月）

Sandworm
国家活動｜ロシア軍GRU関連

- 破壊・混乱が目的／NotPetya（2017年）などに関与
- 米司法省がGRUへの帰属を公表し、将校を起訴
- ウクライナの会計ソフト更新を入口に、世界の企業へ感染拡大

GRU将校を起訴：米司法省（2020年10月）

APT28 / Fancy Bear
国家活動｜ロシア軍GRU関連

- 政府・国際機関への諜報、窃取情報による影響工作
- 英NCSCがロシア軍GRUの活動と指摘
- 英NCSCはルーターを悪用した認証情報の窃取も公表

GRU第26165部隊への帰属を指摘：英NCSC（2026年4月）

Scattered Spider
犯罪者群｜米英等にまたがる

- 従業員やIT担当者を装い、認証を突破して恐喝
- FBI等が手口を公表／構成員とされる人物を訴追
- 電話などでヘルプデスクを欺き、認証の再設定を誘導

手口を公表：米FBI・CISA（2023年11月）

注：民間企業の分析・当局の認定・集団自身の犯行声明を区別。起訴は有罪確定ではない。地図：Natural Earth。

NCA：英国家犯罪対策庁／NCSC：英国立サイバーセキュリティセンター／FBI：米連邦捜査局／CISA：米サイバー・インフラ安全保障庁