資料1. サイバー攻撃 主要各国特徴比較表　ーアメリカ、中国、ロシア他

国	機関	特徴	主な事例	日本への影響	最近の事例	リスク評価	攻撃手法の分類
アメリカ	NSA / USCYBERCOM	ゼロデイ活用 世界最先端の攻撃・防御	①Stuxnet（2010） ②Equation Group活動 ③PRISM監視（2013） ④対ISIS作戦 ⑤SolarWinds調査（2020）	日本は攻撃対象ではなく同盟国として協力 防衛省とNSAの情報共有 共同演習	対中露サイバー攻撃への反撃作戦 （2023–2025）	低	ゼロデイ攻撃 マルウェア（Stuxnet） 大規模監視、情報操作
中国	MSS / PLA戦略支援部隊	世界最大規模 産業スパイ・重要インフラ潜伏	①Operation Aurora（2009） ②OPM侵入（2015） ③Cloud Hopper（2017） ④Salt Typhoon（2024） ⑤Volt Typhoon（2023–25）	2020防衛装備庁攻撃 2022JAXA情報流出 2023警視庁がPLA部隊関与を認定 防衛・宇宙・大学が狙われる	AT&Tや州兵ネットワーク侵害 （2024–2025）	高	APT、スピアフィッシング クラウド侵入、重要インフラ潜伏
ロシア	GRU（APT28/Fancy Bear）、FSB系	政治工作・破壊型攻撃	①エストニアDDoS（2007） ②ジョージア侵攻連動（2008） ③米大統領選 ヒラリー候補メール介入（2016） ④NotPetya（2017） ⑤Outlook「NotDoor」（2025）	外務省や大使館職員へのAPT28攻撃 ウクライナ支援に伴い政府・シンクタンクも標的化	OutlookマルウェアNotDoor（2025）	中	DDoS、フィッシング マルウェア 選挙介入
ウクライナ	SBU / GUR	防御中心だが反撃も	①BlackEnergy対応（2015） ②IT Army設立（2022） ③露鉄道侵入（2022） ④国営メディア改ざん（2022） ⑤露兵士スマホ追跡（2023）	直接攻撃はなし 日本人がIT Army参加呼びかけに関与し法的議論	ロシア軍システムへの継続的攻撃 （2024–2025）	低	DDoS、ウェブ改ざん ハクティビズム
イスラエル	Unit 8200	攻撃・防御とも世界最高水準	①Stuxnet（2010米国と） ②Flame（2012） ③Operation Orchard（2007） ④イラン港湾攻撃（2020） ⑤イラン鉄道攻撃（2021）	日本企業が防御技術導入 2022年日イスラエル間でサイバー協力協定	イラン関連施設への妨害 （2024–2025）	低	ゼロデイ攻撃 スパイウェア 重要インフラ妨害
トルコ	MIT / 親政府系ハクティビスト	地域紛争中心 クルド人勢力を標的	①RedHack活動（2012～） ②クルド団体攻撃（2016～） ③シリア関連攻撃（2019） ④欧州反トルコ団体サイト改ざん（2020） ⑤アルメニア系団体攻撃（2021） ⑥日本国内クルド人コミュニティ攻撃（2024）	在日クルド人団体WebやSNSがDDoS・改ざん被害 外交摩擦が日本国内に波及	在日クルド系団体への攻撃（2024）	中	DDoS、ウェブ改ざん 政治的ハクティビズム
イギリス	GCHQ / NCSC	防御重視だが攻撃力も保有	①ISISプロパガンダ破壊（2017） ②WannaCry対応（2017） ③対ロシア工作反撃（2018） ④Huawei調査（2019–20） ⑤ウクライナ支援で露妨害（2022–24）	2023年日英がサイバー協力協定を締結 共同演習・情報共有を強化	ロシアAPT対抗作戦（2024–2025）	低	DDoS防御 情報公開 プロパガンダ妨害
北朝鮮	RGB / Lazarus Group	外貨獲得目的 仮想通貨窃取	①Sony Pictures攻撃（2014） ②バングラ中央銀行事件（2016） ③WannaCry（2017） ④暗号資産取引所攻撃（2018～） ⑤AI・暗号資産窃取（2023–25）	2018年以降、日本の暗号資産取引所が複数回被害。数百億円規模流出。 2022年警察庁がLazarus関与を警告。	仮想通貨取引所からの資金窃取 （2024–2025）	高	ランサムウェア 暗号資産窃取 フィッシング