資料１

最近のロシア発の諸問題と世界秩序

内閣府国際政治経済懇談会
2021年7月１日

慶應義塾大学総合政策学部教授
廣瀬　陽子

概要【最近のロシア発の諸問題と世界秩序】

ハイブリッド戦争(サイバー攻撃を含む)の脅威：サイバー攻撃は2000-01年に特に活発に

旧ソ連地域の混乱＝ロシアの勢力圏の揺らぎ：ロシアの求心力低下？

反民主的動向の高まり：コロナ禍で加速。ベラルーシも。

ユーラシア・北極圏におけるパワーバランスの変化：中露関係、トルコの台頭

民主主義／国際リベラル主義（欧米）と専制主義国家（中露）の断絶の拡大

ロシアへの対応

ロシアのハイブリッド戦争は日本にとっても脅威

(※ 参考文献 1)

- 2018年12月、「防衛計画の大綱」と「中期防衛力整備計画」を改訂し、宇宙やサイバー部門を強化　（前回の改定から5年。通常は10年）

  → なぜか？

  ⑴北朝鮮が核ミサイルの能力を顕著に増強させた

  ⑵露のクリミア併合以後、戦い方が変わった、つまり「ハイブリッド戦争」の脅威が高まった

  → ミサイル防衛システムの改善、宇宙やサイバーへの対応が重要に

  参考：「ロシアのクリミア併合から戦い方が変わった」（小野寺元防衛相）

  https://business.nikkeibp.co.jp/atcl/report/16/082800235/111400011/

- 20年10月19日：英外務省がロシアの情報機関であるロシア軍参謀本部情報総局(GRU)が、東京オリンピック・パラリンピックを狙う目的で、関係各所にサイバー攻撃を行っていたと発表。

→ ロシアのハイブリッド戦争を理解し、対策しなければ、安全は保証されない

ロシアのハイブリッド戦争

- 「ハイブリッド戦争」＝政治的目的を達成するために、軍事的脅迫とそれ以外の様々な手段[政治、経済、外交、サイバー攻撃、プロパガンダを含む情報・心理戦などのツールのほか、テロや犯罪行為も]が組み合わされた、非正規戦と正規戦を組み合わせた戦争の手法。
- クリミア併合で話題になったが、新しい事象ではない。世界では、古代から使われ、ロシアでも1990年代から議論され、ロシア・ソ連も歴史的に多用してきたとされる。
- ロシアでは「ハイブリッド戦争(Гибридная война)」という言葉は用いられない(マスコミなどが欧米の現象として使用することはある）　→　　新世代戦争、現代型戦争、現代戦など…。
- ロシアにとってのハイブリッド戦争は、欧米が作り出した概念であり、欧米が行っているもので、ロシアはその「被害者」
- ロシアにおける「ハイブリッド戦争」はそれ自体が戦略というわけではなく、作戦であり、クリミア併合を経て、軍事コンセプトからロシアの外交政策の理論に準じるものに変わった。
- **ロシアは火のないところを炎上させる能力はないが、小さな煙を炎上させることに長けており、その際、ハイブリッド戦争は極めて有益。**

国家戦略としての新世代戦争

- プーチン大統領は、2014年12月25日にロシアの新軍事ドクトリンに署名（2010年2月版を改定）。
- 新ドクトリンでは、現代の軍事紛争の特徴として、「軍事力と政治、経済、情報、その他の非軍事的手法が統合的に使用される」ことや、非正規の武装グループや民間軍事会社の参加、間接的・非対称的な手法の使用などが書かれている。
- 同ドクトリンの草案は、2013年7月（ウクライナ危機の前）に提出されていた

  ※ウクライナ危機での「ハイブリッド」な作戦は既定路線だった

特に諸外国への影響が大きいサイバー攻撃１

- **露のサイバー攻撃の担い手（横の協力はない）**

1. 犯罪者(ランサムウエア攻撃など)
2. 国家などが目的・意図をもって行うもの（GRU(ロシア連邦軍参謀本部情報総局), FSB(連邦保安局), SVR(連邦対外情報局)などが関与）
3. 民間のサイバー攻撃会社など
4. 愛国者

→ 特に政府系のAPT28 /ファンシー・ベアなど(GRU); APT29/コージー・ベアなど (FSB, SVR)の行動は活発。

特に諸外国への影響が大きいサイバー攻撃２

■露のサイバー攻撃の性格

- 国家支援型（米国の兵器に関する情報を狙った1996年の「Moonlight Maze」 が最初）が特に深刻な影響を及ぼしている　　ex. 2007年、エストニア ；2016年、米国大統領選挙
- 高いスキル（ネットワークへの侵入からPCやデバイスの乗っ取り、システムをダウンに至るまでの作業をわずか18分で完了できる。世界最速。2位は北朝鮮の2時間20分）
- 防衛力が弱い（ジョージアの事例；米国のやり方の模倣）
- 攻撃の内容が目的や相手によって変わる　※特にハイブリッド戦争との絡みで

  ＊欧米諸国の政治を混乱させることが目的の場合は、情報の入手・拡散という手段が目立つ

  ＊軍事的な戦争を展開しながら同時にサイバー攻撃を行う場合や相手国への懲罰的な意味合いが大きい場合（具体的には旧ソ連諸国に対する攻撃が中心）は、政府関連、インターネット網や電力システム、銀行システムなど、重要インフラを狙う

諸外国の政治介入や政治妨害：効果的心理戦

- フェイクニュースや宣伝キャンペーンをSNSなどで拡散し、インフルエンス・オペレーション(誘導政策)を展開
- IRAなどは、一人が10個以上のアカウントを持ち、書き込みを継続（次第に、一般人も拡散を始める）。
- 最も大きな成功を収めたのは2016年の米国大統領選挙（反クリントンキャンペーン）
- アフリカ諸国、ベネズエラなどの協力も確認される
  → 英語の上達；スペインの事例

＊サイバー攻撃、諜報などともリンクさせて、政治介入を行う

ロシア（政府系）はコロナ禍でも多くのサイバー攻撃・情報戦を展開
※世界的なテレワーク増が「隙」を多く生み出したことも背景

- コロナ禍でもサイバー攻撃・情報戦を展開し、自国に有利な国際的状況を生み出そうとした。
- ロシアの国家主体による主たるサイバー攻撃の事例：
  - 4月15日:英国家サイバーセキュリティセンター（NCSC）が、米国の米連邦捜査局（FBI）や米国土安全保障省（DHS）と合同で、コロナ禍に乗じたロシア政府によるサイバー攻撃への注意を喚起。
  - 7月16日：NCSCが、新型コロナウイルスのワクチンを開発している研究機関や大学、製薬会社、シンクタンク、政府機関などに対して、ロシアのハッカー集団がワクチン情報や知的所有権を盗み出すために4月ごろからサイバー攻撃を仕掛けていると発表（カナダ通信保安局（CSE）と米国家安全保障局（NSA）との連名）。APT29が実行犯とされ、これまで使われてこなかった「WellMess」と「WellMail」と呼ばれる、任意のシェルコマンドの実行やファイルのアップロード・ダウンロードを可能にするよう設計された軽量なマルウエアが用いられた、個人をターゲットにしたフィッシング攻撃やスピアフィッシング攻撃で、ログイン認証情報を取得し、情報を搾取する手法も多用された。
  - 11月13日：マイクロソフト社が、ロシアと北朝鮮の国家による支援を受けたハッカー集団が、新型コロナウイルスのワクチン開発を行うアメリカ、カナダ、フランス、インド、韓国の著名な７つの企業のシステムにサイバー攻撃を仕掛けていたことを明らかに。実行犯はAPT28で、パスワードスプレーとして知られる、ブルートフォースアタック（総当たり攻撃）を実行。
    cf. 8月11日には、ロシアは世界初となる新型コロナウイルスのワクチン「スプートニクV」を認可。ロシアのサイバー攻撃の成果ともみなされた。
  - 10月19日：英外務省がロシアの情報機関であるロシア軍参謀本部情報総局（GRU）が、東京オリンピック・パラリンピックを狙う目的で、関係各所にサイバー攻撃を行っていたと発表。
  - 12月：ロシアが3月から米ソーラーウィンズ社のソフトウェア・オリオンの脆弱性を悪用した大規模なサイバー攻撃を行なっていたことが明らかに。米国の複数の政府機関や地方政府の他、重要な民間企業等の重要情報が想像を絶する規模で盗まれた。被害は米国史上最悪レベルで、全容解明には数年を要するとも。
- 情報戦では、コロナが米国発祥であること、欧米のワクチンの誤情報など、多くのフェイクニュースを展開。