新興技術と安全保障
―官民関係の変容がもたらす課題―

齊藤孝祐（上智大学）
saitouk@sophia.ac.jp

1．問題背景

新興技術の利用と管理をめぐる官民関係の変容

- 新興技術分野の役割：AI、量子、次世代通信、宇宙、サイバー・・・
  - 新しい民生・商用技術が、社会のみならず究極的には戦争のあり方を変える
  - 依然として不透明な技術動向＝軍事・経済・社会に対する影響の不明瞭さ
  - 「予測」に基づく対応の進展：想像に基づく利用と規制
- 民生領域と軍事領域の重複
  - オープンイノベーションの進展
  - 民間企業や研究機関（大学等）の技術を安全保障政策に取り込んでいくことの重要性
  - 技術の研究開発・利用・管理をめぐるコンセンサス形成の重要性
- 新興技術は安全保障における官民関係をどのように変えたのか？
  - 事例①：AIの開発と規制をめぐる官民の連携と対立
  - 事例②：技術普及に伴う「軍事力」の意味合いの変容

（参考）新興技術の「遍在性」

オムニユース化する新興技術
安全保障とバランスされる経済社会的価値の拡大

- 「オムニユース（omni-use/omnipresent technology）」としての新興技術（Dekker and Okano-Hejimans 2020）
  - 今日の新興技術の特徴：①デジタルないし無形であること、②民間セクターがその発展において支配的な役割を果たすこと、③無形の技術が軍民問わず広範囲にわたって使われること。
  - 当該技術の社会的偏在がその規制を困難にする。
  - どこまで、どのように民間に広がっているかも重要なポイント。
    cf.実際の兵器システムと紐づけられる傾向の強かった過去の先端技術管理リスト（Jones 2020, p.50）
- オムニユース性がもたらす問題：
  - 安全保障目的の技術管理の進展
  - 管理を要する新興技術が「遍在的」であるほど、経済社会的な価値の地平において守るべき価値の射程も拡大：トレードオフ／調整の必要性

2．米国のAI戦略と民間へのアプローチ

軍事領域におけるAIの導入加速

技術管理の射程の拡大

- 米国におけるサードオフセット戦略（オバマ政権）以来のAI軍事利用
  - 自律型／半自律型兵器システムの運用における「人の判断」介在や制御、法遵守等の確認
  - 2013年「無人化システム統合ロードマップ」：自律化の推進を大きな技術目標とする一方、「法的、政策的、倫理的」問題を勘案して「適切なレベルでの自律性」を追求する方針／AIの運用指針のひとつとして参照
  - DIUなどを通じた官民連携によるAI研究の推進
- National Security Innovation Base（トランプ政権）
  - 兵器やビジネスで用いられる技術の所在がセクター横断で創出されるとの認識
  - 民間セクターにおける技術保護：技術監視、CFIUS強化、カウンターインテリジェンス等を通じた知財保護、査証手続き見直し、STEM学生の制限、ネットワークやデータの保護等
  - 「製造業・防衛産業基盤・サプライチェーンの強靭性に関する報告書」（2018）：AI含む先端技術開発のエコシステムが縮小していることを問題視

3．AIの軍事利用をめぐる官民連携と摩擦

官民連携の推進

特定の利用形態に対する民間の反発

- 兵器の自律化推進路線の加速：ex. NSCAI最終報告書（2021）
  - 国際人道法を含む倫理基準や人の適切な関与を追求する方針の再確認
  - 敵対勢力の動向や軍事的効用、倫理基準の遵守という観点から兵器の自律化余地を残す
- 軍事利用に対する国内企業の否定的反応／潜在的な反発
  - GoogleによるJEDI入札やMAVENプロジェクトからの撤退
  - 原則策定：兵器や人を害する技術を追求しない（2018年6月）
  - DIUのクラウドソリューション事業には参加（2020年5月）
- マルチステイクホルダーによる「AI 5原則」の策定（2020）
  - 責任／公平／追跡（透明性）／信頼／統治
  - Defense Innovation Boardの勧告に基づく検討
  - 「商業界、政府、学界、一般市民の主要AI専門家との15か月間の協議の結果」

４．規制をめぐる連携と負荷

軍事、経済安全保障、社会リスクの管理を目指した官民連携

- AI領域における民間セクターを通じた対中圧力
  - CHIPS法を通じたリスク対応（2022年8月）
  - AIを含む懸念国への投資規制（2023年8月）
  - AI用の先端半導体輸出規制（2023年10月）
  - 民間セクターの利益とのバランスのうえに成り立つ戦略的規制措置
- AIリスクをめぐる「共同規制（co-regulation）」の推進
  - 人工知能大手による「自発的な」リスク管理の約束（2023年7月）
  - 社会的リスク（差別、プライバシー、欺瞞など）のほか、サイバーリスクや兵器転用なども含むリスクへの自主的対応
  - 「安全・安心・信頼できるAIに関する大統領令」に帰結（2023年10月）
  - AI Safety Institute Consortiumのもとで200社以上の連携によるリスク管理・安全性等への対応（2024年2月）
  - リスク管理をめぐる国際連携と米国の主導的立場の確保を目指す

5．ウクライナにおける戦場と民間の接近

技術普及に伴って戦場への関与を強める「一般の人々」

- ウクライナ政府の民間企業からの技術利用
  - 「義勇兵」による民生用ドローンや3Dプリンターの活用
  - スペースX社によるStarlinkの提供：通信や戦力運用への活用
  - マクサー・テクノロジーズ（衛星画像会社）の情報提供によるウクライナ軍の活動支援
- 「一般人」によるサイバー攻撃
  - 戦争開始直後、Twitterを通じたIT Army参加への呼びかけ
  - 匿名ハッカー集団「アノニマス」のみならず、不特定多数の一般人による対ロシアサイバー攻撃
- 戦場へのさまざまな影響
  - 公開された衛星情報等に基づく政府、民間レベルのOSINT
  - マスメディアやSNS等を通じた情報発信による認知枠組みの形成
  - スペースX社による利用可否のコントロール？／ロシア側の利用？

6．技術普及がもたらす「戦争の管理」への課題

民間の「戦争参加」をいかに管理するか

- 民間の戦争参加をいかに管理するかという問題
  - 政府の管理下に置かれていない民間の力の行使
  - 戦争介入手段の管理の難しさ
  - 2000年代以降の民間軍事会社（PMC）の問題との類似性
- 「新たな戦争の手段」はどこまで受容されるか
  - 民間の力の行使による問題
  - 支援元政府の外交的思惑との乖離
  - 指揮命令系統から外れた民間の行動

● 秩序維持と正当性の問題
  - エスカレーションの過程を管理することは可能か
  - ウクライナにおいてのみならず、「ウクライナ後」にどこまで認められるか

7．まとめ／問題提起

能力を持つ民間セクターを前提とした新たな官民連携の模索

- 新興技術（保護）競争の問題構造
  - 安全保障のための利用・管理強化と民間セクターとの調整コスト
  - 「トップダウンの規制」と「自主規制」のバランス／共同規制アプローチ
  - 軍事領域・民生領域双方における、管理しきれない技術普及の効果
- 民間セクターの技術管理能力の向上の重要性
  - すべての技術発展の段階や将来的な可能性を把握し、すべての経済・経営上の利益とのバランスをふまえて技術規制をデザインすることは今のところできない
  - 民間セクターにおける自主的な判断の重要性
  - 技術普及に伴ってますます困難になる管理・ルール形成＝ステイクホルダーの多様化
- 官民のコンセンサス形成のための「説明」「対話」「投資」
  - 誰がコストを負担するか
  - 政策目的をめぐるコンセンサスと民間セクターの利害調整