

防衛力の抜本的強化に関する有識者会議(部会)(第3回)

1. 日 時 令和7年1月31日(金)1500～1700

2. 場 所 第1省議室

3. 出席者

(有識者)

北岡伸一(部会長)、上山隆大、遠藤典子、落合陽一、栗崎周平、小西美穂、宮永俊一、森本敏、山崎幸二(敬称略)

(防衛省側)

金子防衛大臣政務官、若宮防衛大臣補佐官、番匠政策参与、増田防衛事務次官、加野防衛審議官、萬浪大臣官房長、大和防衛政策局長、青柳整備計画局長、廣瀬政策立案総括審議官、田中地方協力局長、石川防衛装備庁長官、吉田統幕長、小林陸幕副長、齋藤海幕長、小笠原空幕副長、江川情報本部長、松尾防衛政策課長

4. 議事内容

①金子防衛大臣政務官、北岡部会長より開催挨拶

②防衛政策課長より【資料1】について説明。

③各有識者より、防衛力抜本的強化の全体像(指揮統制・情報関連機能／機動展開能力・国民保護)について、意見があった。

④金子防衛大臣政務官より閉会挨拶

5. 各有識者からの意見

上記、4③の各有識者からの意見については以下のとおり。

○今後、宇宙を中心とした統合オペレーションの重要性がますます高まっていくと考える。この際、マルチオービット、ハイブリットなアーキテクチャ、マルチターミナルを接続するネットワークをどのように整備するかが重要。

○衛星に関しては衛星軌道間や軍用と商用をまたいだシステムの構築が必要。その際、衛星製造者、通信プロバイダー、米軍との通信路の最適化等が必要であるが、ネットワークの管理やセキュリティの確保が重要になる。

○AIについて、インターネット上のデータはほぼ学習し終えたというのが人工知能系学会でのトピックによく出てくる。これ以上AIを賢くするためには、クローズドなデータをどう学習させていくのかが重要な観点。

○オープンなデータよりもクローズドなデータの方が遥かに多い。セキュリティを保ちながらクローズドなデータをAIの学習に使いつつ、それを現場の人がどのように活用していくのかが重要。

○AIが進化していく今、生成AIは技術的に進化していく。各企業は様々な使い方をしており、これから更に技術的に進化していくものと考えられ、常に民との交流や、どのようなものが使えるのかという情報交換の場を今後考えていくことが大切。

○AIの脅威が如実に出てきおり、それに対応するための組織をどうするのかポイントである。1番大事なのは早く実行し、情報をキャッチアップして、組織全体にAIを速やかに取り入れるということである。

○情報システムはAI技術などを含めて近代化するということが非常に重要。指揮統制のための情報システムであって、その情報システムが指揮統制をうまく運用出来ていくかということが重要。

○情報戦について、フェイクニュースを作るような生成AIが進化している。フェイクニュースを作るアルゴリズムを検知する技術も進化していくと考えられるので、能力のある人達を集めて情報戦の対策を考えていくのがよいのではないか。

○認知戦がある際に重要なのは、我が方に正義があるということを確立することである。平時から広報外交的なものを通じて、我々が取る行動を明確にしておくことで、認知戦、情報戦における抑止的な取組になるのではないか。

○機動展開について、イスラエルのように、戦闘機が空港の滑走路の下に待機するような地下壕化を検討してもよいのではないか。

○武力攻撃時は、自衛隊に住民の避難を含む国民保護の役割を担って欲しいという声が高い。この期待に応えるため、輸送力の強化や住民の避難等の計画や体制の強化は防衛力の強化と同じくらい重要。

○PFIの事業は育てていくものであり、国として、有用性についてアピールしていき、企業にしっかりと利益が上がっていく体制を作っていくことが重要。そして、様々な分野にPFI事業を拡散していくことが重要。

○国民保護について、大胆な移動だけでなく、選択肢の一つとしてシェルターを作るなど、現地で安全を守るための方策も考えておかなければならないのではないか。

○特定利用空港・港湾とすることによって、運輸の面でも役に立ち、防衛体制を充実するとともに、地方の経済効果と共存共栄していくというところがポイント。沖縄について、この取組を進めていくことが大きな課題。

○国民保護について、原発や発電所などの重要インフラに対する警備が薄い。国家の生命線であるような重要インフラの整備を強化する手段というものも作るべき。

○自衛隊が住民避難において担う役割について、国民との認識や期待にギャップがある。そのため、国民の理解を得るための説明の機会や発信の機会を増やしていただきたい。

○我が国の安全保障、防衛の迅速な意思決定にAI技術や先端技術の取り込み方や、情報戦への対応、先端技術や、それを担う有能な人材育成について、次期科学技術基本計画を取り入れていくこともあるのではないかな。

○サイバーセキュリティにおける脅威、個人の生活、生存、尊厳の脅威、気候変動による脅威、産業サプライチェーンに対する脅威等の対応策として科学技術という視点を取り入れることができれば、次期科学技術基本計画に国家安全保障の問題を正面から取り上げることができる。