能動的サイバー防御

JCA-NET セミナー

2023 年 7 月 22 日

小倉利丸

toshi@jca.apc.org

「能動的サイバー防御」？？？

「サイバー」が安全保障分野で強調されるが ...

- そもそも「サイバー」とは何を意味しているのか
- サイバー領域の「安全保障」とは何のことか
- サイバー戦争とはどのような「戦争」なのか
- 従来の「戦争」から類推することができるのか

国家安全保障戦略における「サイバー」

「本戦略は、外交、防衛、経済安全保障、技術、サイバー、海洋、宇宙、情報、政府開発援助（ＯＤＡ）、エネルギー等の我が国の安全保障に関連する分野の諸政策に戦略的な指針を与えるもの」

「サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性がい。」

国家安全保障戦略における「サイバー」

「宇宙・サイバー・電磁波の領域及び陸・海・空の領域における能力を有機的に融合し、その相乗効果により自衛隊の全体の能力を増幅させる領域横断作戦能力に加え、侵攻部隊に対し、その脅威圏の外から対処するスタンド・オフ防衛能力等により、重層的に対処する。また、有人アセットに加え、無人アセット防衛能力も強化すること等により、様々な防衛能力が統合された防衛力を構築していく。」

国家安全保障戦略における「サイバー」

我が国を全方位でシームレスに守るための取組の強化

「軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開され、グレーゾーン事態が恒常的に生起している現在の安全保障環境において、サイバー空間・海洋・宇宙空間、技術、情報、国内外の国民の安全確保等の多岐にわたる分野において、政府横断的な政策を進め、我が国の国益を隙なく守る。」

サイバー安全保障分野での対応能力の向上

「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防御の強化、政府内外の人材の育成・活用の促進等を引き続き図る。」

国家安全保障戦略における「サイバー」

「その上で、武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。

そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。」

国家安全保障戦略における「サイバー」

「（ｱ） 重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

（ｲ） 国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

（ｳ） 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。」

国家安全保障戦略における「サイバー」

「能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。これらの取組は総合的な防衛体制の強化に資するものとなる。

また、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化する。

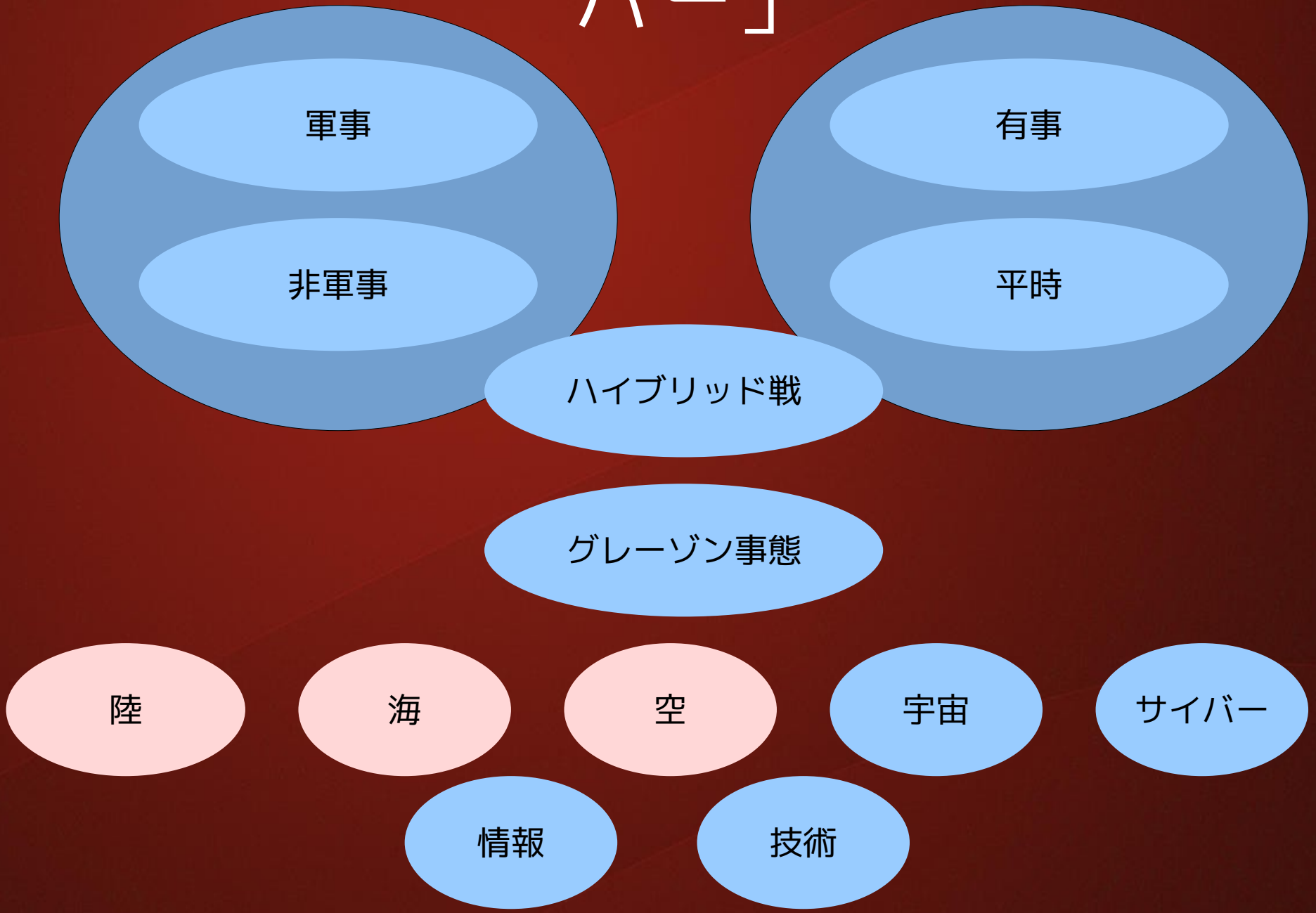
さらに、同盟国・同志国等と連携した形での情報収集・分析の強化、攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために引き続き取り組む。」

国家安全保障戦略における「サイバー」

自衛隊の組織再編だけでなく内閣サイバーセキュリティセンターの改組が強調されている。

- 自衛隊の組織再編は行われる
- それに加えて政府組織の横断的な再編を計画している。内閣サイバーセキュリティセンターは現在でも省庁横断的性格をもっているが、これを「庁」のレベルに格上げする？
- 法制度の整備（どの法律を改変するつもりか？）
  - プロバイダーの守秘義務への例外規定？
  - プロバイダーの政府への協力義務？
  - プロバイダーによるサイバー攻撃を可能にする？
- 自衛隊の動向だけを見ていてもダメ

国家安全保障戦略における「サイバー」



国家安全保障戦略における「サイバー」

「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」

能動的サイバー攻撃の条件

- 武力攻撃に至らない重大なサイバー攻撃のおそれ
- 安全保障上の懸念に該当し、かつ「重大」である

疑問点

- 現実の攻撃は存在しない。「懸念」「おそれ」の判断は？
- 導入される能動的サイバー防御の定義がない

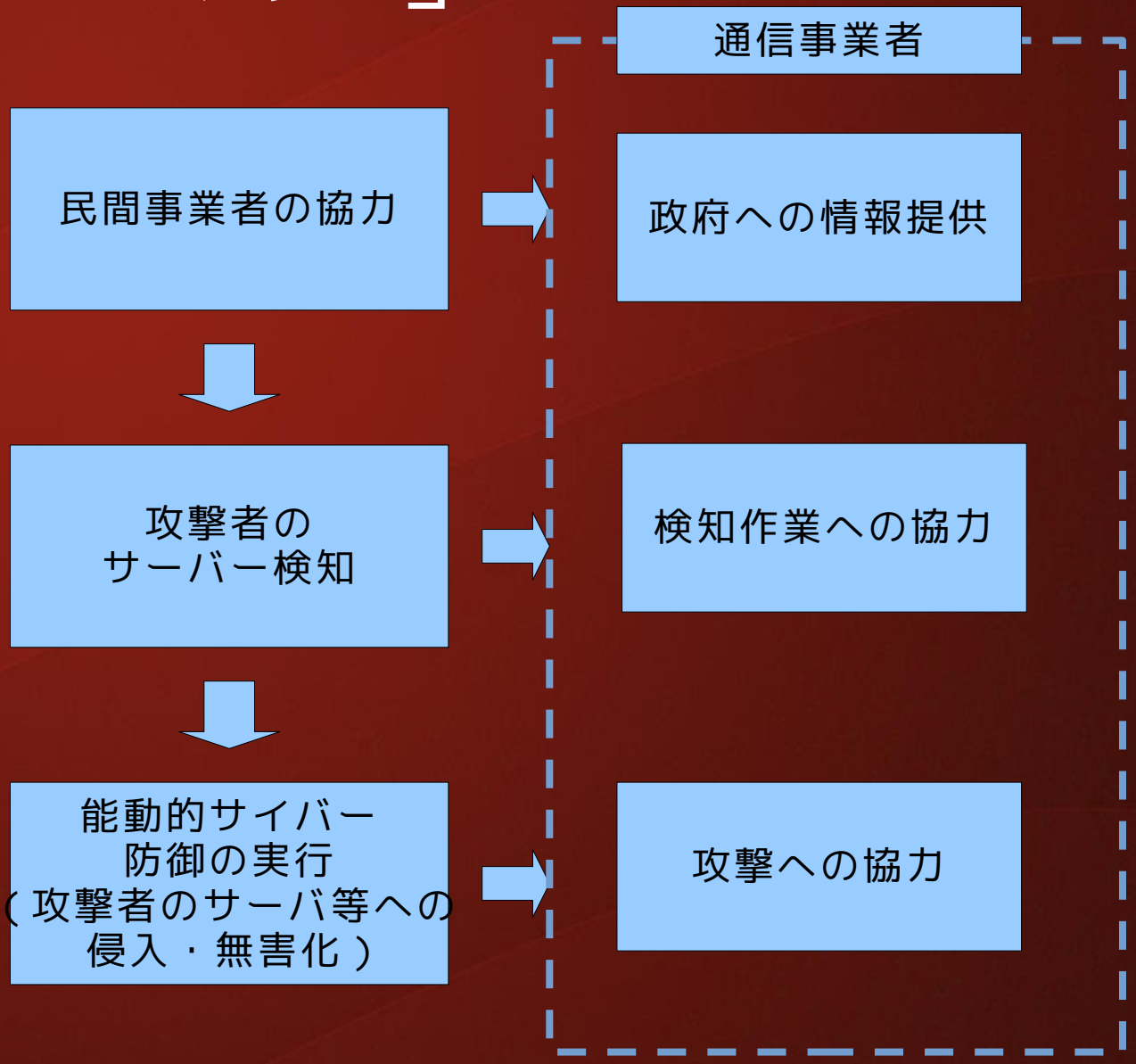
国家安全保障戦略における「サイバー」

能動的サイバー防御の実施のための体制を整備の問題点

- 民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有→民間の通信事業者が保有する個人情報を政府（自衛隊）に提供する
- 民間事業者の情報を活用し攻撃者の利用が疑われるサーバ等を検知→監視と情報収集。民間事業者に協力させてサーバのデータに国の機関がアクセス。
- 攻撃者のサーバ等への侵入・無害化。「検知」にとどまらず標的に対して攻撃を行なう。

国家安全保障を理由としたハッキングなどの免責を法制化

国家安全保障戦略における「サイバー」



国家防衛戦略におけるサイバーの位置付け

重視される七つの領域

- スタンド・オフ防衛能力
- 統合防空ミサイル防衛能力
- 無人アセット防衛能力
- 領域横断作戦能力 ——→ **能動的サイバー防御**
- 指揮統制・情報関連機能
- 機動展開能力・国民保護
- 持続性・強靱性

国家防衛戦略におけるサイバーの位置付け

高い軍事力を持つ国が、あるとき侵略という意思を持ったことにも注目すべきである。脅威は能力と意思の組み合わせで顕在化するところ、意思を外部から正確に把握することには困難が伴う。国家の意思決定過程が不透明であれば、脅威が顕在化する素地が常に存在する。

このような国から自国を守るためには、力による一方的な現状変更は困難であると認識させる抑止力が必要であり、相手の能力に着目した自らの能力、すなわち防衛力を構築し、相手に侵略する意思を抱かせないようにする必要がある。

戦い方も、従来のそれとは様相が大きく変化してきている。これまでの航空侵攻・海上侵攻・着上陸侵攻といった伝統的なものに加えて、精密打撃能力が向上した弾道・巡航ミサイルによる大規模なミサイル攻撃、偽旗作戦を始めとする情報戦を含むハイブリッド戦の展開、宇宙・サイバー・電磁波の領域や無人アセットを用いた非対称的な攻撃、核保有国が公然と行う核兵器による威嚇ともとれる言動等を組み合わせた新しい戦い方が顕在化している。こうした新しい戦い方に対応できるかどうかが、今後の防衛力を構築する上で大きな課題となっている。

国家防衛戦略におけるサイバーの位置付け

平素から有事まで政府全体が取り組むなかで自衛隊が連携

「サイバー領域においては、諸外国や関係省庁及び民間事業者との連携により、平素から有事までのあらゆる段階において、情報収集及び共有を図るとともに、我が国全体としてのサイバー安全保障分野での対応能力の強化を図ることが重要である。政府全体において、サイバー安全保障分野の政策が一元的に総合調整されていくことを踏まえ、防衛省・自衛隊においては、自らのサイバーセキュリティのレベルを高めつつ、関係省庁、重要インフラ事業者及び防衛産業との連携強化に資する取組を推進することとする。」

国家防衛戦略におけるサイバーの位置付け

領域横断作戦能力

「サイバー領域では、防衛省・自衛隊において、能動的サイバー防御を含むサイバー安全保障分野における政府全体での取組と連携していくこととする。その際、重要なシステム等を中心に常時継続的にリスク管理を実施する態勢に移行し、これに対応するサイバー要員を大幅増強するとともに、特に高度なスキルを有する外部人材を活用することにより、高度なサイバーセキュリティを実現する。このような高いサイバーセキュリティの能力により、あらゆるサイバー脅威から自ら防護するとともに、その能力を生かして我が国全体のサイバーセキュリティの強化に取り組んでいくこととする。

このため、2027 年度までに、サイバー攻撃状況下においても、指揮統制能力及び優先度の高い装備品システムを保全できる態勢を確立し、また防衛産業のサイバー防衛を下支えできる態勢を確立する。

今後、おおむね 10 年後までに、サイバー攻撃状況下においても、指揮統制能力、戦力発揮能力、作戦基盤を保全し任務が遂行できる態勢を確立しつつ、自衛隊以外へのサイバーセキュリティを支援できる態勢を強化する。」

国家防衛戦略におけるサイバーの位置付け

情報本部と能動的サイバー防御

「情報本部は、電波情報、画像情報、人的情報、公刊情報等の収集・分析に加え、我が国の防衛における情報戦対応の中心的な役割を担うこととし、他国の軍事活動等を常時継続的かつ正確に把握し、分析・発信する能力を抜本的に強化する。

さらに、領域横断作戦能力の強化及びスタンド・オフ防衛能力の強化に併せ、既存の体制を強化するとともに、関係する他機関との協力・連携を切れ目なく実施できるように強化する。

防衛省・自衛隊においては、能動的サイバー防御を含むサイバー安全保障分野に係る政府の取組も踏まえつつ、我が国全体のサイバーセキュリティに貢献する体制を抜本的に強化することとする。」

※ 能動的サイバー防御については、自衛隊が中核的な役割を果すのか、それとも他の政府諸組織と横並びなのか、不明

国家防衛戦略におけるサイバーの位置付け

下記の箇所は非常に重要。さりげなく、目立たないような位置に置かれているが、相手の利用を妨げ、無力化することを明記している。

「宇宙・サイバー・電磁波の領域において、相手方の利用を妨げ、又は無力化するために必要な能力を拡充していく。」（領域横断作戦能力の項）

※「国家安全保障戦略」では「無力化」という言葉は使われておらず、「無害化」という言葉がある。言葉のニュアンスとして無力化の方が力＝武力を破壊する可能性も含まれているように思う。

防衛力整備計画におけるサイバーの位置付け

サイバー領域における能力

サイバー攻撃を受けている状況下において、指揮統制能力及び優先度の高い装備品システムを保全し、自衛隊の任務遂行を保証できる態勢を確立するとともに、防衛産業のサイバー防衛を下支えできる態勢を構築する。

このため、最新のサイバー脅威を踏まえ、境界型セキュリティのみでネットワーク内部を安全に保ち得るという従来の発想から脱却し、もはや安全なネットワークは存在しないとの前提に立ち、サイバー領域の能力強化の取組を進める。

「ネットワーク内部に脅威が既に侵入していることも想定し、当該脅威を早期に検知するためのサイバー・スレット・ハンティング機能を強化する。

防衛省・自衛隊のサイバーセキュリティ態勢の強化のため、陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編し、サイバー要員を育成する教育基盤を拡充する。さらに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の構築に係る取組を強化する。

これらの取組を行う組織全体としての能力を強化するため、2027 年度を目途に、自衛隊サイバー防衛隊等のサイバー関連部隊を約 4,000 人に拡充し、さらに、システム調達や維持運営等のサイバー関連業務に従事する隊員に対する教育を実施する。これにより、2027 年度を目途に、サイバー関連部隊の要員と合わせて防衛省・自衛隊のサイバー要員を約２万人体制とし、将来的には、更なる体制拡充を目指す。

防衛力整備計画におけるサイバーの位置付け

統合運用体制

「サイバー領域における更なる能力向上のため、防衛省・自衛隊のシステム・ネットワークを常時継続的に監視するとともに、我が国へのサイバー攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力を抜本的に強化し得るよう、共同の部隊としてサイバー防衛部隊を保持する。」

航空自衛隊に新組織（基幹部隊の見直し）

「領域横断作戦能力を強化するため、対空電子戦部隊を新編するとともに、島嶼部の電子戦部隊を強化する。さらに、情報収集、攻撃機能等を保持した多用途無人航空機部隊を新編する。また、サイバー戦や電子戦との連携により、認知領域を含む情報戦において優位を確保するための部隊を新編する。」

防衛力整備計画におけるサイバーの位置付け

陸上自衛隊

「領域横断作戦能力を強化するため、対空電子戦部隊を新編するとともに、島嶼部の電子戦部隊を強化する。さらに、情報収集、攻撃機能等を保持した多用途無人航空機部隊を新編する。また、サイバー戦や電子戦との連携により、認知領域を含む情報戦において優位を確保するための部隊を新編する。」

海上自衛隊

「認知領域を含む情報戦への対応能力を強化し、迅速な意思決定が可能な態勢を整備するため、所要の研究開発を実施するとともに、情報、サイバー、通信、気象海洋等といった機能・能力を有する部隊を整理・集約し、総合的に情報戦を遂行するため、体制の在り方を検討した上で海上自衛隊情報戦基幹部隊を新編する。」

防衛力整備計画におけるサイバーの位置付け

情報本部：情報戦を担うことがあらたに明記

「情報戦対処の中核を担う情報本部において、情報収集・分析・発信に関する体制を強化する。さらに、各国等の動向に関する情報を常時継続的に収集・分析することが可能となる人工知能（ＡＩ）を活用した公開情報の自動収集・分析機能の整備、各国等による情報発信の真偽を見極めるためのＳＮＳ上の情報等を自動収集する機能の整備、情勢見積りに関する将来予測機能の整備を行う。」

※ 情報本部： 1997 年に創設。防衛省の中央情報機関。「我が国最大の情報機関」約 2000 人　https://ja.wikipedia.org/wiki/情報本部

- 情報収集・分析・発信に関する体制の強化
- 人工知能（ AI ）を活用した公開情報の自動収集・分析機能の強化
- 各国による情報発信の真偽を見極めるためのＳＮＳ情報等を自動収集する機能の整備
- 情勢見積りに関する将来予測機能の整備

https://www.mod.go.jp/dih/2024_joho_web.pdf

自衛隊の組織

安保防衛３文書に記載された部隊の新規編成

•(空自)対空電子戦部隊を新編。認知領域を含む情報戦において優位を確保するための部隊を新編

•(海自)海上自衛隊情報戦基幹部隊を新編

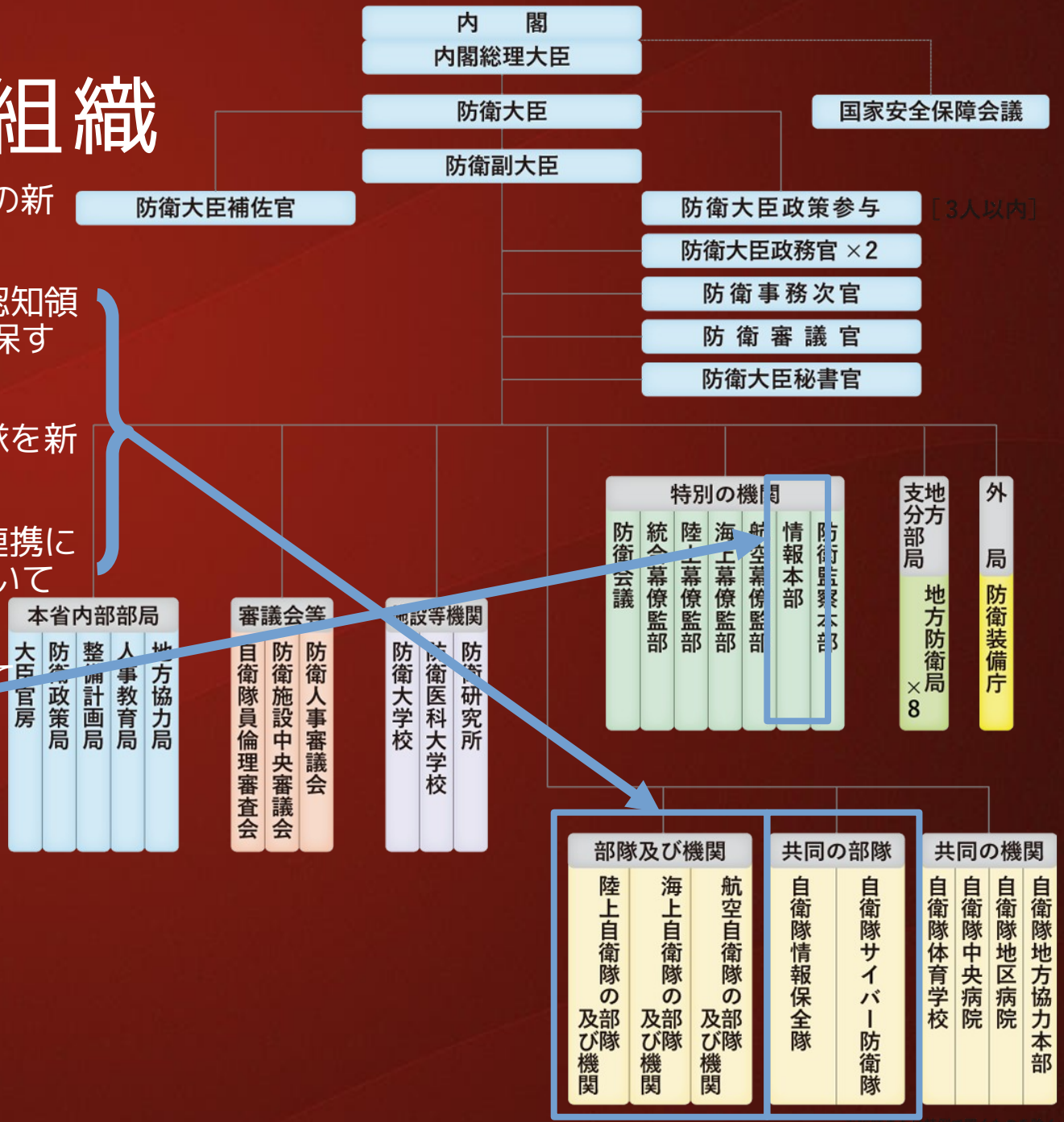
•(陸自)サイバー戦や電子戦との連携により、認知領域を含む情報戦において優位を確保するための部隊を新編

•情報本部 情報戦の中核部隊としての役割追加

自衛隊サイバー防衛隊等のサイバー関連部隊を約 4,000 人に拡充

防衛省・自衛隊のサイバー要員を約２万人体制

※陸自 15 万人、海自・空自各 45000 人



https://www.mod.go.jp/j/profile/mod_sdf/images/mod20220713.png

2023 年度予算規模

サイバー領域における能力強化 約２６４３億円

リスク管理枠組み（ RMF ）の導入（ ３３９億円）

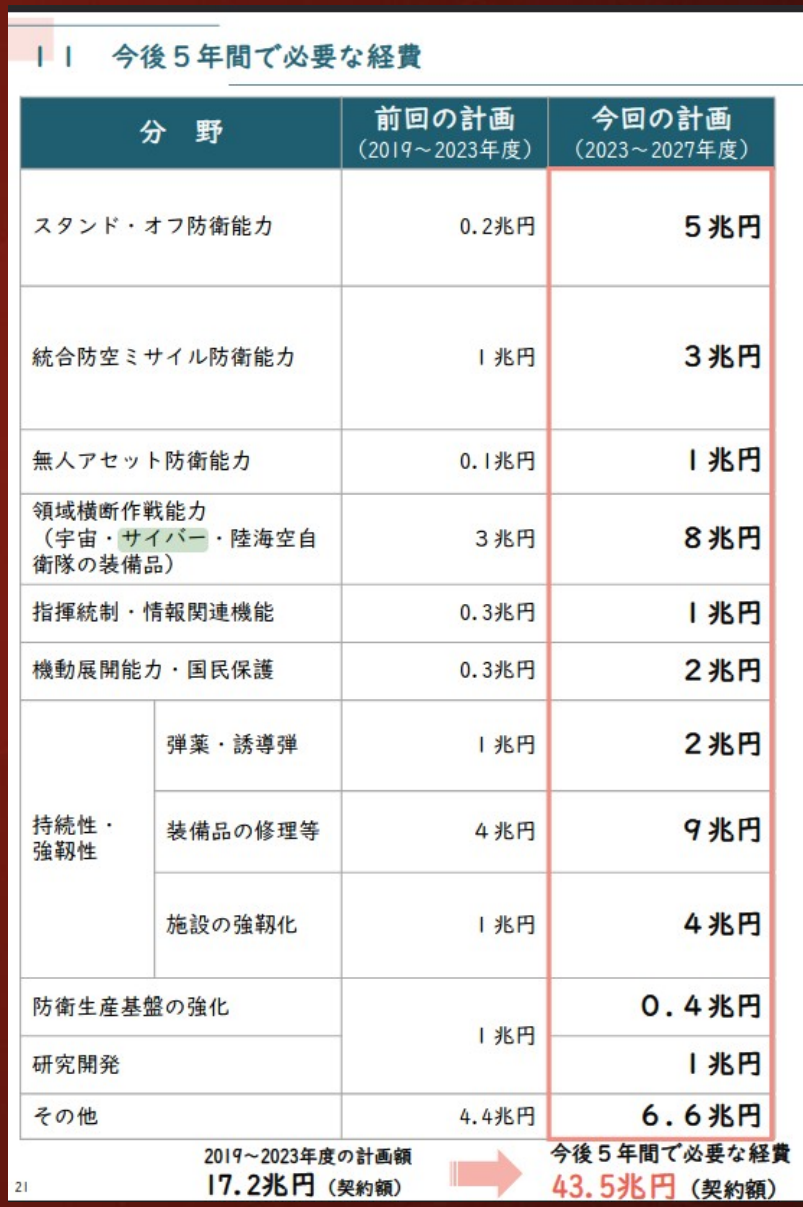
一過性の「リスク排除」から継続的な「リスク管理」へ
考え方を転換し、情報システムの運用開始後も常時継続的にリスクを分析・評価し、必要なセキュリティ対策を実施

情報システムの防護

装備品や施設インフラを含む情報システムの防護態勢を強化
○　クラウド整備
中央クラウドの整備（４３４億円）
空自クラウドの整備（７５６億円）等
〇 スレットハンティング器材の整備（２８億円）内部の潜在的脅威を継続的に探索・検出するスレットハンティング器材を整備
○　サイバー防護分析装置の整備（２８億円）防衛省に対するサイバー攻撃に関する手法の収集・分析等を行うサイバー攻撃対処のための装置の監視・評価機能等を強化
○　システムネットワーク管理機能（ SNMS ）の整備（８０億円）陸上自衛隊の全システムの防護、監視、制御等を
一元的に行うシステムを整
○　施設インフラにおけるサイバーセキュリティ対策（４４億円）施設インフラにおける物理的対策や可搬記憶媒体及び
プログラムへの不正接続を感知・通報・遮断するシステムの導入

サイバー分野における教育・研究機能の強化（22 億円）

防衛省：「我が国の防衛と予算（案）令和５年度予算の概要～防衛力抜本的強化「元年」予算」 https://www.mod.go.jp/j/yosan/yosan_gaiyo/2023/yosan_20221223.pdf



Ⅱ　今後５年間で必要な経費

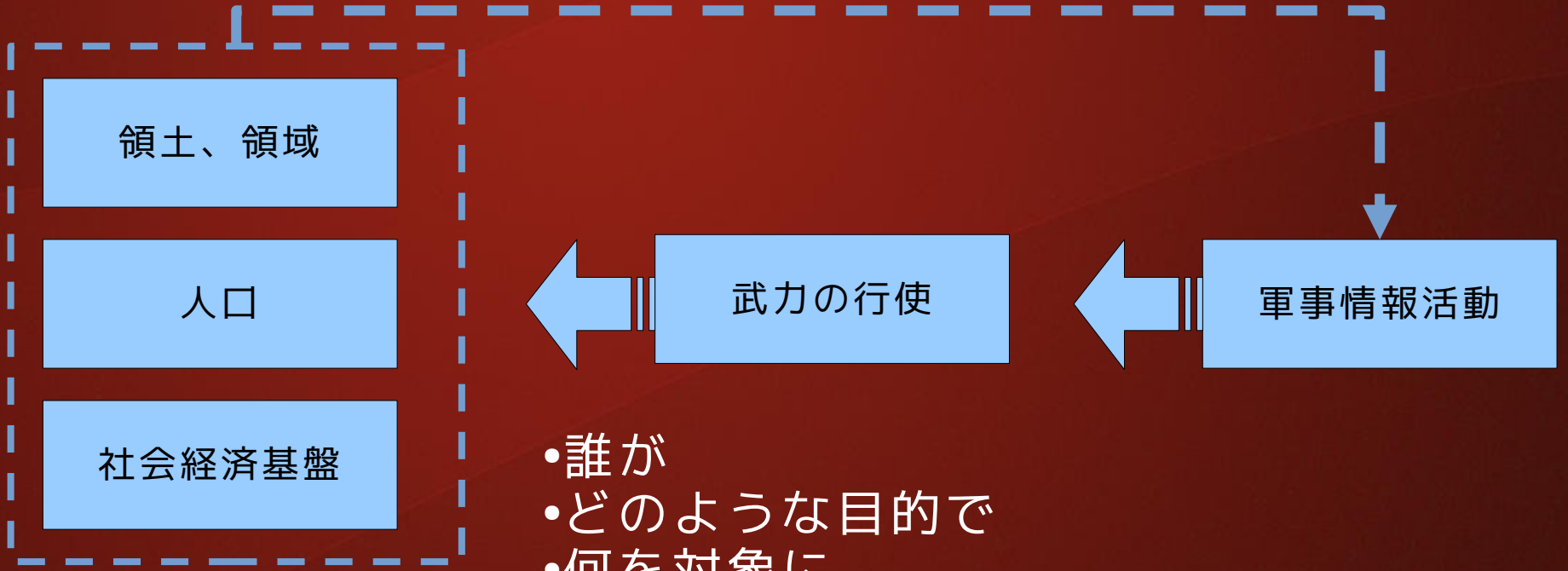
分　野		前回の計画（2019～2023年度）	今回の計画（2023～2027年度）
スタンド・オフ防衛能力		0.2兆円	５兆円
統合防空ミサイル防衛能力		１兆円	３兆円
無人アセット防衛能力		0.1兆円	１兆円
領域横断作戦能力（宇宙・サイバー・陸海空自衛隊の装備品）		３兆円	８兆円
指揮統制・情報関連機能		0.3兆円	１兆円
機動展開能力・国民保護		0.3兆円	２兆円
持続性・強靱性	弾薬・誘導弾	１兆円	２兆円
	装備品の修理等	４兆円	９兆円
	施設の強靱化	１兆円	４兆円
防衛生産基盤の強化		１兆円	0．４兆円
研究開発			１兆円
その他		4.4兆円	６．６兆円

2019～2023年度の計画額 17.2兆円（契約額） → 今後５年間で必要な経費 43.5兆円（契約額）

21

サイバー戦争は「戦争」なのか？

従来の「戦争」の基本的な枠組



•誰が
•どのような目的で
•何を対象に
•どのような手段を用いて
•物理的な破壊を行使するのか

建前上は、国際法上の制約があるため、どこでも、誰に対しても、いかなる破壊行為をしてもよいわけではないが、実際には何でもアリ。

サイバー戦争は「戦争」なのか？

- そもそも「戦争」なのか、単なる犯罪行為なのかの判断の基準が、実空間でも不明瞭に。「対テロ戦争」という概念が「常識化」してからますます曖昧に。
- サイバー戦争に「領土」「領域」をめぐる争奪といった軍事目標の設定はなじまない。サイバー空間には「領土」に該当するものが存在しないから。
- インターネットはサイバー攻撃の対象であるだけでなく、「手段」でもある。
- 実空間とサイバーとは相互補完的な関係をもち、陸海空いずれの領域でも相互に関連し、かつ、諜報活動にも利用されるので、「統合的」な運用が必要だとみなされるようになる。

サイバー戦争は「戦争」なのか？

対テロ戦争がもたらした「戦争」状態の転換

- 2004年、ブッシュ大統領が議会で「ボーダレスな戦争戦略」に言及。「合衆国の自衛権および国民と国益を守る権利を行使するために必要であれば…特殊作戦軍およびその他の戦力を緊急展開させ、世界中のあらゆる地域で秘密作戦を遂行させることである。」
- 2004年春、ラムズフェルド国防長官が「アルカーイダ・ネットワーク破壊遂行命令」の命令書。アルカーイダが活動、潜伏している可能性のある地域であれば、世界中どこでも、暗殺を含む作戦を展開することを可能とした。

この世界の戦場化はオバマにも継承される。

ジェレミー・スケイヒル『アメリカの卑劣な戦争』（上）、第16章「世界が戦場」、横山啓明訳、柏書房）

サイバー戦争は「戦争」なのか？

戦争とは何なのか、サイバー戦争とは何なのか、これらの定義を明確にする必要があるが、現状ではあいまいなままだ。以下の表は、とりあえず、あいまいなままの概念を前提としつつ、実空間とサイバー空間での「戦争」の違いを表にした。

	主体（誰が）	標的	目的	手段	法的枠組
実空間での戦争	ほぼ明確 代理戦争の可能性がある	明確	明確	武力	あり ただし遵守されていない
サイバー戦争	あいまい アトリビューションという問題が生じる	直接の標的が本来の目的かどうかは不明な場合がある	戦争行為の一環であることが不明瞭なケースが多い 犯罪目的に偽装することがある	武力の定義がない ネットワークへの侵入、マルウェアの使用など	なし いくつかの国際的な宣言などがある。 タリンマニュアル。パリコールなど

武器が用いられれば戦争である、というわけではない。戦争なのか、刑事事件なのか、テロなのか … は上の表では表現できない。

論点をどのように整理するか？

9条との関連では

- 日本国民は、正義と秩序を基調とする国際平和を誠実に希求し、国権の発動たる戦争と、武力による威嚇又は武力の行使は、国際紛争を解決する手段としては、永久にこれを放棄する。
- ② 前項の目的を達するため、陸海空軍その他の戦力は、これを保持しない。国の交戦権は、これを認めない。

従来の戦争	サイバー戦争
国権の発動たる戦争	国権の発動たるサイバー戦争
武力による威嚇	サイバーにおける「武力による威嚇」とは
武力の行使	サイバーにおける「武力の行使」とは
陸海空軍その他の戦力	サイバーにおける「戦力」とは
国の交戦権	サイバーにおける「交戦権」とは

論点をどのように整理するか？

9条で再度確認すべき論点

- 「戦争」と「武力による威嚇又は武力の行使」は同じ事態を指していない。
  - 戦争に至らない武力の威嚇や行使も放棄の対象とされている
  - 国内の犯罪行為に対する警察の武力による威嚇や行使は対象外。これが抜け穴になる可能性もある。
- 「国権の発動」ではない場合は対象になるのか？

放棄の対象は「国権の発動」としての武力の威嚇、行使に限定されている。サイバー戦争の場合、民間や個人が主体になる可能性がかなり高い。（銃器や戦車は保有できなくてもパソコンがあれば「参戦」できる）

- 「戦争」の行為主体は自衛隊（あるいは国の軍事組織）に限定できない

論点をどのように整理するか？

「サイバー」領域における概念の定義が極めてあいまいなままだ。

- 国権の発動たるサイバー戦争とはどんな状態を指すのか
- サイバーにおける「武力」「戦力」「交戦」とは何なのか。これらがはっきりしない限り９条との関係がグレーゾンになる。
- 戦争は、領土と人口への暴力による支配を実現する行為だと定義すると、サイバー戦争はこの定義に該当しない。
- しかし、サイバー戦争は戦争ではない？では、なぜ自衛隊が？どこの国でも軍隊がが関与していることに意味は何なのか。

定義のあいまいさと私たちの戦争観がもたらす先入観の問題

- 定義を不明確なままにしているのは、サイバー戦争を「戦争」の概念から外して政府にフリーハンドを与えようとする傾向があるのではないか？
- 戦争＝自衛隊という等式を前提に、私たちひとりひとりは、この戦争の枠内にはいないという実感が支配的。しかしサイバー領域では、この実感を過信できない。

論点をどのように整理するか？

自衛隊をどのような存在として捉えるか

- 自衛隊を違憲とする場合

あらゆる自衛隊の取り組みを容認しない。シンプルでわかりやすいが、落とし穴がある。

- 自衛隊が専守防衛であれば合憲であるとする場合

サイバー領域での専守防衛を定義しなければならない。能動的サイバー防御は専守防衛を逸脱するのかどうかは定義次第。敵基地攻撃とリンクすれば逸脱だが、それ以外の場合は容認する？どのようなサイバー事案が自衛隊の任務になりうるのか、とも関連。

- 政権与党の立場を追認する場合

サイバー戦争と従来型戦争の関連がはっきりしていない。戦争観が未成熟。

論点をどのように整理するか？

自衛隊を違憲とする場合

あらゆる自衛隊の取り組みを容認しない。シンプルでわかりやすいが、落とし穴がある。

- サイバー戦争は自衛隊以外の組織もその担い手になる。

（例）NATOのサイバー戦争の演習「ロックドシールズ」には総務省、警察庁、情報処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）、NTTデーグループ(NTTドコモ、NTTコミュニケーションズ、NTTデータ、ならびに NTTセキュリティ・ジャパン)、Splunk、Red Hat、株式会社ラック、ESET、中部電力カパワーグリッド、レッドハット ジャパンなどが参加。

（例）ウクライナ戦争。Googleは脅威分析グループが協力。検索結果からRTとスプートニクを削除。ウクライナ外務省と直接連携して約150の海外の広告会社が情報戦。ウクライナのIT軍にClearview社が顔認識を提供。ロシアは西側SNSなどを遮断。「情報戦」の戦場は私たちの日常必需品でもあるネットのコミュニーションそのもの。

- 殺傷兵器ではないが、戦争遂行の一環として利用される場合をどう判断するか。
- サイバー戦争は従来とは異なる意味での総力戦の構造を不可欠にする

論点をどのように整理するか？

現に起きている武力紛争を前提にした場合

- 国家の正規軍だけを行為主体とみなすことはできない。
- 「宣戦布告」はほとんど意味をなさない。
- 「戦争」という概念で武力の行使を位置づけるかどうかは、政治的な判断による。
  - ロシアは戦争ではなく「特殊軍事作戦」と呼んだ。
  - 911 以後米国は「テロとの戦争」を宣言した（しかし、どの武力行使がこの戦争行為に該当するのかは不明）
  - テロリズムを戦争の範疇に入れることが多くなる→テロリズムに対して軍がテロ支援国家に対して直接武力行使を行なうことが当たり前になった
- 武力の行使には、「暗殺」のような行為が含まれるようになった。（正規軍による標的へのピンポイントの攻撃）
- ブッシュ「世界が戦場」発言→戦場の概念があいまいに。

論点をどのように整理するか？

問題

- 基本的な概念の定義が明確になっていないなかで「サイバー」領域の軍事安全保障の制度が先行し、既成事実化が進んでいる。
- 諸外国のサイバーに関する軍事安全保障の考え方が導入され、「９条」の制約が機能していない。
- 政府の考え方は、「サイバー戦争」を足がかりに、政府と民間を包摂する新しい総動員体制の構築を模索している。
- サイバー戦争の放棄は、従来の戦争放棄の主張の延長線上では捉えきれない、より広範な領域を含む。私たちひとりひとりが「サイバー戦争」とどう関わりあいがあるのかを確認することが必要。