

特集
Special

レポート
Report

インタビュー
Interview

エッセイ
Essay

レクチャー
Lecture

オピニオン
Opinion

TOP > [レクチャー](#) > [山下塾第5弾 変わりゆく自衛隊](#) > 山下塾第5弾 第七話「サイバー対策、新たなステージへ」

山下塾 第5弾

山下 輝男

第七話「サイバー対策、新たなステージへ」

我が国の防衛産業や官公庁に対して執拗なサイバー攻撃が繰り返され、

我が国の企業や官公庁に対するサイバー攻撃も頻発しており、安全保障上の重大な脅威となっている。クリック一つで国家の基幹インフラすらも麻痺させ得る可能性すら囁かれている。第4又は第5の戦場とも云われるサイバー空間の安全確保は国家にとっての緊急の課題である。我が国も遅ればせながら、対策に乗り出し、防衛省・自衛隊においても、所要の対策を取りつつある。そして、念願であった「サイバーセキュリティ基本法」が、平成26(2014)年11月6日の衆議院本会議で成立した。

明けて、1月9日、政府のサイバー攻撃対応の司令塔の役割を果たす「サイバーセキュリティ戦略本部」と「内閣サイバーセキュリティセンター」が発足した。

色々な課題はあるものの、自衛隊に期待される役割によっては、自衛隊は大変革を迫られるかも知れない、そんな予感がする。

1 サイバー空間を巡る動向

(1) 安全保障上の重要な課題

重要インフラの情報通信ネットワークに対するサイバー攻撃は、人々の生活に深刻な影響をもたらすものである。インターネット関連技術は日進月歩であり、サイバー攻撃も日に日に高度化、複雑化している。サイバー攻撃の特徴としては、次のようなものがあげられる。

- ① 多様性：実行者、手法、目的、状況などが多様
- ② 匿名性：実行者の隠いん ぺい蔽・偽装が容易
- ③ 隠密性：攻撃の存在を察知し難いものや、被害発生の認識すら困難なもの
- ④ 攻撃側の優位性：手法によっては攻撃手段の入手が容易であることや、ソフトウェアのぜい弱性を完全に排除することが困難であることなど
- ⑤ 抑止の困難性：報復攻撃や防御側の対策による抑止効果が小さいことなど

軍隊にとって情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、ICTの発展によって情報通信ネットワークへの軍隊の依存度が一層増大している。

このような情報通信ネットワークへの軍隊の依存を受け、サイバー攻撃は敵の軍隊の弱点につけこんで、敵の強みを低減できる非対称的な戦略として位置づけられつつあり、多くの外国軍隊がサイバー空間における攻撃能力を開発しているとされている。また、情報収集目的のために他国の情報通信ネットワークへの侵入が行われているとの指摘がある。こうしたことから、今やサイバーセキュリティは、各国にとっての安全保障上の重要な課題の一つとなっている。

(2) サイバー空間における脅威の動向

- ① 中国

頻発するサイバー攻撃の一部は、中国の人民解放軍、情報機関、治安機関、民間ハッカー集団や企業など様々な組織の関与が指摘されている。中国はサイバー空間に強い関心を有しているとみられ、軍がサイバー部隊を編成し、訓練を行っているとの指摘や、軍および治安機関が、IT企業などの人材やハッカーを採用しているとの指摘がある。たとえば13（平成25）年2月、米国情報セキュリティ企業が発表した報告書では、06（同18）年以降、中国人民解放軍所属部隊が米国をはじめとする企業などへサイバー攻撃を行っていたと結論づけている6。また14（同26）年5月、米国司法省は、米国企業にサイバー攻撃を行ったとして、中国人民解放軍のサイバー攻撃部隊「61398部隊」の将校らを起訴したと発表した。

②ロシア

08（同20）年、米中央軍の秘密情報などを取り扱うネットワークに、可搬記憶媒体を介してコンピュータ・ウィルスが侵入し、外部に情報が転送される可能性がある深刻な事態に陥った。この事案については、ロシアの関与が指摘されている。ロシアについては、軍や情報機関、治安機関などがサイバー攻撃に関与しているとの指摘があり、また、軍によるサイバーコマンド創設の検討やハッカーの募集を行っているともみられる。

③北朝鮮

13（同25）年3月には、韓国の放送局、金融機関などに対するサイバー攻撃が、また、同年6月から7月にかけて、韓国大統領府、政府機関、放送局、新聞社などに対するサイバー攻撃が発生した。これらの事案について韓国政府は、過去の北朝鮮によるサイバー攻撃の手口と一致したとしている。北朝鮮については、サイバー攻撃への政府機関などの関与や国家規模で人材育成を行っているとの指摘もある。

④高度化、国家の関与

10（同22）年6月、「スタックスネット」と呼ばれる高度に複雑な構造を有するコンピュータ・ウィルスが発見され、その後もたびたび高度なウィルスが発見されている。

また、意図的に不正改造されたプログラムが埋め込まれた製品が企業から納入されるなどのサプライチェーンリスクも指摘されている。

政府や軍隊の情報通信ネットワークおよび重要インフラに対するサイバー攻撃は、国家の安全保障に重大な影響を及ぼし得るものであり、政府機関の関与も指摘されていることから、サイバー空間における脅威の動向を引き続き注視していく必要がある。

⑤日本へのサイバー攻撃

わが国においても、11（同23）年9月には、防衛装備品などを製造する民間企業のコンピュータが不正なプログラムに感染するという事態が発覚したほか、警察庁によると、12（同24）年9月のわが国政府による尖閣三島取得の閣議決定を行った日以降、数日の間に裁判所や行政機関、大学病院など少なくとも19のウェブサイトに対して攻撃が行われ、被害が発生した。

2 列国の取組状況

（1）米国

①「サイバー空間のための国際戦略」策定（平成23(2011)年5月）

優先的の取り組むべき7つの分野：経済、ネットワーク防護、法執行、軍事、インターネット・ガバナンス、国際的な能力構築、インターネットの自由

②連邦政府のネットワークや重要インフラの防護責任：国土安全保障省の国家サイバーセキュリティ部が全体調整

③米軍のサイバー戦能力＝本土防衛上保持すべき重要な分野、人材確保・育成&サイバー任務部隊の拡充

④米国防省サイバー空間における作戦のための戦略(平成23(2011)年7月)

- ・サイバー空間を陸海空と同じ作戦領域に位置付け
- ・防衛のための新たな作戦概念の採用
- ・他省庁、民間部門と協力
- ・同盟国およびパートナー国との強固な関係構築
- ・人材及び急速な技術革新

⑤組織体制

戦略軍隷下のサイバーコマンド：各サイバー部隊及び作戦を統括

サイバー国家任務部隊の保持、サイバー戦闘任務部隊創設予定

ドクトリンの策定

(2) NATO、英国、豪、韓等

政府全体のサイバーセキュリティの統括組織の設置

3 我が国のサイバーセキュリティ

(1) 我が国に対する脅威

NISCによれば、政府機関を標的にしたサイバー攻撃は2013年度、感知できたものだけで、約508万件に上った。

- ・ 標的型メールも増加

(機密情報などの窃取を目的としたサイバー攻撃、年々増加し、手口も巧妙化(組織的な攻撃の可能性、感染後の通信の接続先は、ほとんどが海外。))

- ・ 水飲み場攻撃による特定の攻撃対象への攻撃(攻撃対象組織を限定(例: 政府機関等、 ウェブサイトを閲覧しただけで不正プログラムに感染、 未発表、未修正の脆弱性(ゼロデイ)を攻撃に利用))



(2) ネットワークセキュリティ政策の推移

年々深刻化甚大化するサイバー空間の脅威に対する我が国の現在までの対応状況は以下の通りである。

我が国は、2006年以降サイバーセキュリティにかかる基本計画を策定してきた。

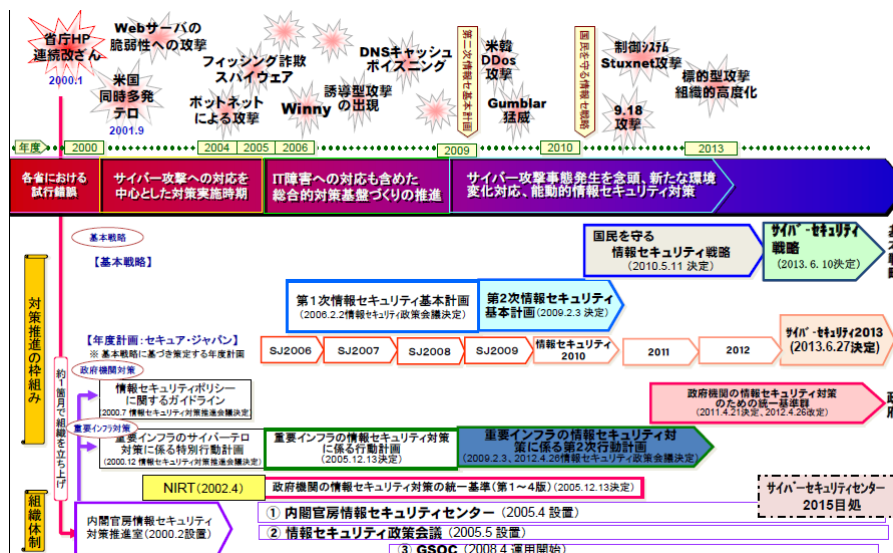
第一次情報セキュリティ基本計画 (2006/2)

第二次情報セキュリティ基本計画 (2009/2)

情報セキュリティ戦略 (2010/5)

サイバーセキュリティ戦略(2013/6)(対象期間: ~2015年)

それぞれの基本計画や戦略に基づき年度計画を策定して、着実な実行を目指した。



(3) サイバーセキュリティ戦略の概要

基本的考え

- ①サイバーセキュリティ立国を目指す
- ②情報の自由な流通の確保

サイバーセキュリティ戦略（13年6月情報セキュリティ政策会議決定）			
	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
①	「強靱な」サイバー空間（守り強化） ● 機微情報を守るためのリスク評価手法の確立・統一基準の見直し【14年5月】 ● GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ● 対処訓練の実施、警察・自衛隊等の関係機関の役割整理 ● SNS・グループメールを含む新サービスに伴う新たな脅威への対応	● 重要インフラの範囲拡大や安全基準見直し等行動計画の見直し【14年5月】 ● 政府機関やシステムベンダー等との情報共有の強化 ● 事業継続確保のための分野横断的な演習	● スマートフォン不正アプリへの対応 ● 情報セキュリティ月間【毎年2月】・“サイバーセキュリティの日”創設 ● 普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【今年度】 ● 税制など中小企業のセキュリティ投資の促進 ● ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ● ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
④	「活力ある」サイバー空間（基礎体力） ● 人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【14年5月】 ● 研究開発戦略（2011年情報セキュリティ政策会議）の見直し【14年夏】		
⑥	「世界を率先する」サイバー空間（国際戦略）【13年10月】 ● 日米 ● 日英 ● 日印 ● 日露 ● 日EU ● 日ASEAN ● サイバー空間の国際規範づくり等に関する会議【平成24年10月：ソウル会議】 ● IWWN注1 ● MERIDIAN注2		
⑦	組織体制 ● NISCの機能強化（サイバーセキュリティセンター（仮称）への改組【2015年度目標】）【方針決定：14年夏】		

(4) サイバーセキュリティ基本法案の概要

平成26(2014)年11月6日の衆院本会議で「サイバーセキュリティ基本法」が可決、成立した。

2020年の東京五輪・パラリンピック開催を見据え、サイバー攻撃への防御体制を強化する狙いがある。

基本法の柱は、官房長官をトップとする「サイバーセキュリティ戦略本部」の設置だ。基本法では、各省庁が攻撃を受けた際、サイバーセキュリティ戦略本部に情報提供することを義務化した。同戦略本部には、改善策の実施を各省庁に勧告したり、対応を報告させたりする権限も与えた。

同法はまた、サイバー攻撃への対策を国と地方自治体の責務としたことに加え、重要インフラ（社会基盤）事業者も対策に協力する努力義務があると明記した



・施策の推進 にあたっての基本理念

- ① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
- ② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築
- ③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築
- ④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
- ⑤ IT基本法の基本理念に配慮して実施
- ⑥ 国民の権利を不当に侵害しないよう留意

(5) サイバーセキュリティ戦略本部とサイバーセキュリティセンターの発足

政府のサイバー攻撃対応の司令塔の役割を果たす「サイバーセキュリティ戦略本部」とその事務局となる「内閣サイバーセキュリティセンター（NISC）」が9日、発足した。

サイバーセキュリティ基本法が同日施行したのを受け、内閣官房情報セキュリティセンターを改名して権限を強めた。約80人いる職員は年内に100人以上に増やし、政府の「防衛能力」を高める狙いだ。

NISCは同日設置したサイバーセキュリティ戦略本部（本部長・菅義偉官房長官）の事務局として、各省庁の情報システムを調べたり改善策を勧告したりする権限を持つ。各省庁にはサイバー攻撃の被害の報告を義務付け、NISCが認知した事案に対処する「司令塔役」を担う。センター長には高見沢将林官房副長官補が就いた。

NISCは監視や分析の力を身につけるため、専門的な知識を持つ人材を集める。任期付きの職員所謂ホワイトハッカーを採用するなどして体制を拡充させる考えである。

4 安全保障とサイバー

(1) 国家安全保障戦略におけるサイバー関連

我が国を取り巻く安全保障環境と国家安全保障上の課題

1 グローバルな安全保障環境と課題

(4) 国際公共財（グローバル・コモンズ）に関するリスク

近年、海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。（中略）

情報システムや情報通信ネットワーク等により構成されるグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

一方、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化しつつある。

我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とする観点から、不可欠である。

（２）サイバー攻撃の特徴

- ①非対称性（高価な兵器を必要とせず、費用がかからない）
- ②攻撃側の優位性（インターネットは拡張性があり、新技術の導入も容易）
- ③従来の抑止モデルが適用されず（攻撃者の特定が困難かつ時間を要する）
- ④ソフトウェア及びハードウェア自体が脅威を内在（サプライチェーンリスク）
- ⑤予測の困難性（国家及び非国家主体の両方が実行者になり得る）

参考

- ① 2007年以降 米国防省、ホワイトハウス等へのアクセス
- ② コソボ紛争（1999年）、イスラエル軍のシリア空爆（2007年）
防空システムにサイバー攻撃レーダー網の無力化
- ③ 米国とイスラエル7年前からイランの核施設にスタックスネット一部の遠心分離器を破壊し核開発を1年半遅らせた。
- ④ 2012年12月：米軍ステルス無人偵察機イラン軍に撃墜された。
- ⑤ 米：シリアへのサイバー攻撃も計画していた（2013/9/7報道）

（３）サイバーと安全保障

- ①サイバー攻撃は大きな脅威・リスク。対象は国家、企業、個人を超えて重層化・融合化。
- ②世界のどこで発生する事象であっても、直ちに我が国の平和と安全に影響を及ぼし得る。国境の内側と外側を明確に区別することは難しい。
- ③サイバー空間は、インターネットの発達により形成された仮想空間。安全保障上も陸・海・空・宇宙に続く新しい領域だが、法的側面については議論が続いている。
- ④サイバー攻撃が行われれば、政府機関から企業に至る社会の隅々にまで深刻な影響を及ぼす。この問題の重要性が認識されるに至っている。
- ⑤日進月歩の技術進歩を背景とするサイバー攻撃は、攻撃の予測や攻撃者の特定が困難、攻撃の手法が多様、といった特徴あり、従来の典型的な武力攻撃と異なる点も少なくない。そのため、サイバー攻撃の法的位置付けについて一概に述べるのは困難。
- ⑥これまでのところ、サイバー攻撃が「武力攻撃」に該当しないと位置付けられている事例が多いように見受けられる。
- ⑦外部からのサイバー攻撃に対処するための制度的な枠組みの必要性等について、国際社会における議論にも留意しつつ、引き続き、検討が必要。

５ 防衛省・自衛隊の取組等

（１）防衛省におけるサイバー攻撃対処の基本方針

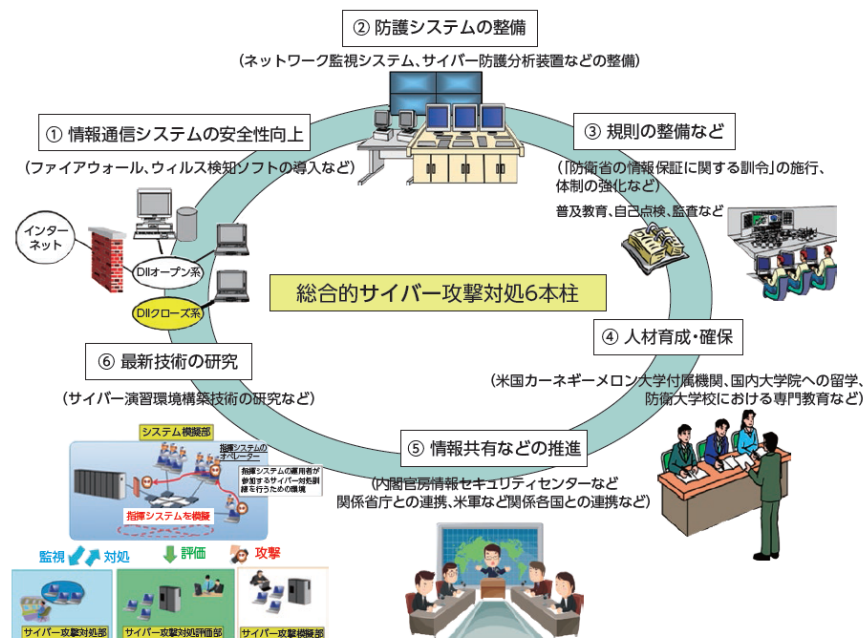
サイバー空間の安定的利用を確保するとともに、サイバー空間という陸・海・空・宇宙に並ぶ新たな「領域」において活動するための能力などを充実・強化する。

- ① 防衛省・自衛隊の能力・態勢強化
- ② 民間も含めた国全体の取組への寄与
- ③ 同盟国を含む国際社会との協力 を基本方針として取組を進める。

（２）具体的取組

「自衛隊指揮通信システム隊」が24時間態勢で通信ネットワークを監視

情報通信システムの安全性向上を図るための侵入防止システムなどの導入、サイバー防護分析装置などの防護システムの整備のほか、サイバー攻撃対処に関する態勢や要領を定めた規則の整備、人的・技術的基盤の整備や最新技術の研究なども含めた総合的な施策を実施



(3) サイバー防衛隊

平成26(2014)年3月26日、サイバー攻撃に対処する自衛隊の専門部隊「サイバー防衛隊」が発足した。防衛隊は、陸海空3自衛隊の自衛隊員ら約90人で編成し、東京・市谷の防衛省内に設置する。

24時間態勢で、防衛省・自衛隊のネットワークの監視やサイバー攻撃が発生した際の対応を担う。当面は防衛省・自衛隊のネットワーク防衛が任務だが、政府は他の政府機関への対応も検討している。

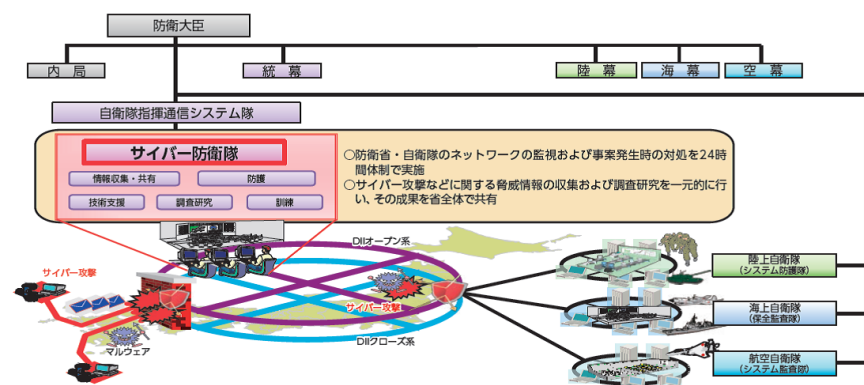
○メリット・必要性等

サイバー防衛隊の新編により、これまで各自衛隊に分散していたサイバー攻撃に関する脅威情報の収集や調査研究を一元的に行うことが可能となることから、その成果を防衛省全体で共有することができるようになる。同時に、政府全体でのセキュリティ向上に向けた取組や民間との協力などが一層強化されるようになる。現在、内閣官房情報セキュリティセンター（NISC）への要員派遣などによって政府全体のセキュリティレベルの向上に貢献しているが、今後、サイバー防衛隊の活動により得られた成果も活用することにより、より積極的に貢献していくことができる。

○防衛産業や重要インフラの防護等

現時点では、防衛関連企業、重要インフラ事業者などの民間企業が保有するシステムやネットワークそのものを直接防護することは想定していない。

防衛省として防衛産業などとの協力は重要であると認識。民間との協力については、13（同25）年から防衛省と防衛産業との間にサイバーディフェンス連携協議会（CDC）を設置して情報共有などについて検討しており、今後、このような場も活用して、将来的な体制に関する検討もなされていく。



(4) サイバー防衛にかかる課題

①サイバー攻撃は安全保障上の脅威だが、我が国に対する武力攻撃事態と認定できるか？ どの時点で認定でき

る？自衛権の発動要件との関係は？

（外国からの組織的・計画的武力行使か？）

②防衛：防衛の対象は自衛隊のみで良いのか？装備機材は、国家的対応・連携は？

*サイバー防衛隊の編成と能力は十分か？

③対抗策は、カウンター攻撃が出来るか

他国からサイバー攻撃を受けた際、発信源を特定しウイルスを送り込むなどの反撃能力を保有すべきかどうかの検討がされている。が、専守防衛との整合性もあり、方針は決まっていない。

*米国は通常兵器での報復も可としているが・・・（米国の「サイバー戦略」）

④攻撃者を特定し得るか、民間であった場合 対応できるのか？

（５）日米サイバー防衛協力等

ア 日米

「日米サイバー防衛政策ワーキンググループ」の設置(平成25（2013）年5月)と会合

「日米サイバー対話への参加」

「日米ITフォーラム」

近々に取りまとめられる日米防衛協力のための指針(ガイドライン)に所要の記述がなされる。

イ その他

・シンガポール、ベトナム、インドネシアとのフォーラム開催

・英国、NATO、エストニア、韓国 防衛当局間のサイバー協議

6 本話の結びに

画期的なサイバーセキュリティ基本法の成立と体制整備がなされ、我が国のサイバー防衛も新たなステージに入った。目に見えぬ空間での熾烈な戦いには日本人は無頓着であるが、臍を噛むことのないようにしっかり態勢を整えなければならない。その一環としての自衛隊の役割は未だ判然とはしないが、より大きな役割が期待されよう。

(了)

キーワード▶ [サイバーセキュリティ基本法](#)・[サイバーセキュリティ戦略本部](#)・[サイバー攻撃](#)・[サイバー空間](#)・[サイバー防衛](#)・[内閣サイバーセキュリティセンター](#)・[変わりゆく自衛隊](#)・[山下塾](#)・[山下塾第5弾](#)・[日米サイバー防衛協力](#)・[自衛隊](#)・[自衛隊の任務](#)・[自衛隊の活動](#)・[自衛隊の行動](#)・[防衛省](#)・[防衛計画の大綱](#)

いいね！ 0

 INDEXへ戻る

次の記事 [山下塾第5弾 第八話「益々増大する国際平和協力活動」](#)

前の記事 [山下塾第5弾 第六話「宇宙の安全保障分野での活用の更なる推進」](#)

[ページの先頭へ](#)

関連サイト

[防衛省](#)

[統合幕僚監部](#)

[陸上自衛隊](#)

[海上自衛隊](#)

[航空自衛隊](#)