第Ⅱ部 わが国の安全保障・防衛政策

第1章 安全保障と防衛の基本的考え方

▶ P.237

安全保障を確保する方策

▶ P.237

- 国民の命や暮らしを守り抜くうえで、まず優先されるべきは、積極的な外交の展開である。日米同盟を基軸とし、同志国との連携、多国間協力を推進していくことが不可欠である。
- 同時に、外交には、裏付けとなる防衛力が必要であり、戦略的なアプローチとして、自由で開かれたインド太平洋（FOIP）の実現に向けた外交を展開するとともに、反撃能力の保有を含む防衛力の抜本的強化などを推進する。
- 憲法のもと、専守防衛に徹し、他国に脅威を与えるような軍事大国とならないとの基本方針に従い、文民統制を確保し、非核三原則を政策上の方針として堅持している。

着任にあたり特別儀仗隊を巡閲する小泉防衛大臣

「三文書」の改定について

▶ P.242

- 現行の国家安全保障戦略、国家防衛戦略、防衛力整備計画（「三文書」）を策定した2022年と比べ、安全保障環境の変化が様々な分野で加速度的に生じている。
- 第１に、法の支配に基づく自由で開かれた国際秩序への挑戦が勢いを増していること、第２に、インド太平洋では、中国・北朝鮮の更なる軍事力の増強や、中露や露朝の連携強化などがみられること、第３に、各国等は、ロシアによるウクライナ侵略を教訓に、無人アセット機の大量運用を含む新しい戦い方や長期戦への備えを急いでいることがあげられる。
- このように、安全保障環境の変化が様々な分野で加速度的に生じているなか、まずは、現行の国家安全保障戦略に定める「対GDP比２％水準」を、2025年度中に、当初予算および補正予算を合わせて前倒して措置するとともに、「三文書」の2026年中の改定に向けて政府内で検討を行っている。
- 具体的には、2025年10月、防衛大臣のもとに、現行の「三文書」に基づく取組の進捗管理とその加速化のための検討を行うこと、また、新たな「三文書」の検討を行っていくことを目的とした防衛力変革推進本部が置かれ、改定に向けた議論が進められている。

防衛力変革推進本部

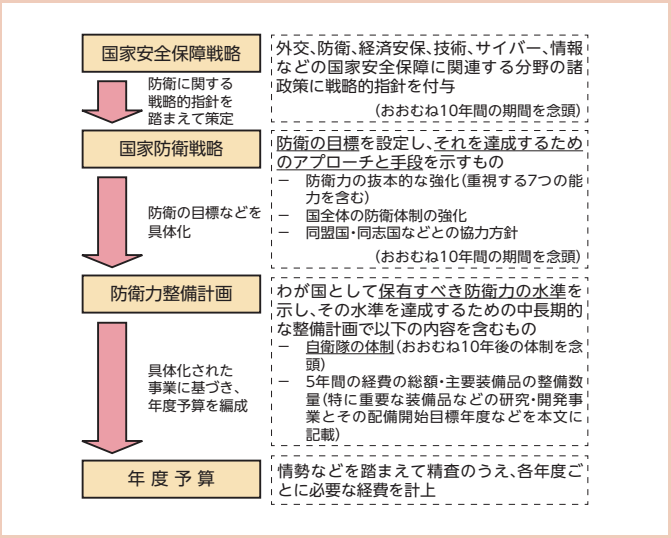
第2章 国家安全保障戦略などの「三文書」と防衛関係費 ▶ P.244

国家安全保障戦略 ▶ P.244

- わが国の安全保障に関する最上位の政策文書であり、外交・防衛分野のみならず、経済安全保障、技術、情報も含む幅広い分野の政策に戦略的な指針を与えるもの。

国家防衛戦略 ▶ P.244

- わが国の防衛目標、この防衛目標を達成するためのアプローチやその手段を包括的に示すもの。
- わが国政府の最も重大な責務は、国民の命と平和な暮らし、そして、わが国の領土・領海・領空を断固として守り抜くことであり、それこそが安全保障の根幹である。わが国を含む国際社会は、深刻な挑戦を受け、新たな危機に突入しており、厳しい現実に正面から向き合って、相手の能力に着目した防衛力の抜本的強化が必要である。
- 防衛力の抜本的強化にあたって、①スタンド・オフ防衛能力、②統合防空ミサイル防衛能力、③無人アセット防衛能力、④領域横断作戦能力、⑤指揮統制・情報関連機能、⑥機動展開能力・国民保護、⑦持続性・強靱性、の７つの機能・能力を重視する。
- わが国への侵攻を抑止する上で鍵となる、①などを活用した反撃能力を保有する。



国家安全保障戦略・国家防衛戦略・防衛力整備計画・年度予算の関係

防衛力整備計画 ▶ P.250

- 国家防衛戦略に従って防衛力を抜本的に強化するにあたって、わが国として保有すべき防衛力の水準や、それを達成するための経費総額、主要装備品の整備数量などを示すもの。
- 2027年度までに、わが国への侵攻が生起する場合には、わが国が主たる責任をもって対処し、同盟国などの支援を受けつつ、これを阻止・排除できるように防衛力を強化する。策定からおおむね10年後までに、防衛力の目標をより確実にするためさらなる努力を行い、より早期かつ遠方で侵攻を阻止・排除できるように防衛力を強化する。

第3章 安全保障と防衛を担う組織 ▶ P.260

- 防衛省・自衛隊は、内閣に設置された国家安全保障会議で議論された基本的な方針のもとで、政策を立案・遂行している。
- 防衛省・自衛隊は、平素から有事まであらゆる段階においてシームレスに領域横断作戦を実現するため、統合作戦司令官を長とする「統合作戦司令部」のもと、陸・海・空自を一体的に運用する統合運用体制を採用している。
- あらゆる事態への対処に万全を期しつつ、増大する政策課題にもしっかり対応しうる体制を構築するため、2026年度に防衛副大臣を１人体制から２人体制へ強化した。

第4章 自衛隊の行動に関する枠組み ▶ P.268

- 2026年10月、一定の重要な電子計算機に対するサイバー攻撃について、特別の必要があるときには、自衛隊の部隊等が、被害を防止するため、サイバー攻撃に使用されている電子計算機へのアクセス・無害化措置（通信防護措置）を講じることが可能となる。