

研究ノート

安全保障としての情報政策に取り組む リーダーの責任：

バイデン・スナク・岸田政権における取り組みに注目して

井 田 浩 之

要 旨

本研究ノートでは、情報政策を安全保障の枠組みに位置付けるために、バイデン（アメリカ）、スナク（イギリス）、そして岸田文雄（日本）政権時代に発表された安全保障関連のドキュメントを対象に、AIや新興技術がどのように位置付けられているかを検討した。いずれも政治的信条は異なるが、国家戦略として情報政策をリスクの観点から対策・戦略を講じていることが明らかになった。

キーワード：安全保障、情報政策、リーダーシップ

1 章 はじめに

本研究ノートでは、アメリカのバイデン元大統領、イギリスの元首相スナク、そして岸田元首相の政権下で実施された情報政策が、安全保障政策の中でどのように位置づけられてきたのかを、公開されている政府文書等をもとに検討することを目的とする。

これら三者を取り上げる理由は、一言で言えば、日本国内におけるメディアの偏向的な報道によって、彼らの政策の本質的な取り組みが見えづらくなっていると考えためである。2025年現在、世界情勢は極めて不安定であり、ウクライナ戦争、アメリカによる対中関税措置、台湾有事など、枚挙に暇がないほど多くの危機的事象が同時進行している。

これらの国際的な安全保障上の課題と密接に関係しているのが情報政策である。その代表的な事例が「ハイブリッド戦争」である。ハイブリッド戦争とは、正規戦、非正規戦、サイバー戦、情報戦、心理戦、認知戦など、複数の戦術を組み合わせで展開される軍事戦略であり、とりわけ情報戦の重要性は、ウクライナ戦争におけるドローンの活用などからも明らかである。

こうした状況を踏まえ、日本政府も対応を進めている。内閣官房は「武力攻撃やテロなどから身を守るために」というパンフレットを作成し、国民に向けた啓発を行っている⁽¹⁾。

また、台湾有事に関連する情報政策においても、着実な連携が進められている。たとえば、NTTと台湾の中華電信は、次世代通信基盤であるIOWNにおいて国際接続を進めており、高市早苗・内閣府特命担当大臣は記者会見で「我が国が強みを有する光技術を基に、海外の通信事業者との相互接続が実現しますと、双方の地域の経済や産業の更なる発展につながるものだと考えております」と述べている⁽²⁾。この発言からも、情報基盤の強化を通じた国際連携が日本の情報政策の中核に据えられていることが読み取れる。

台湾有事や、中国の覇権的動向も、日本の情報政策を考える上で無視できない要素である。たとえば、正式には台湾有事が政府により明言されていないにもかかわらず、岸田文雄元首相は2024年8月、中国による情報収集を目的とした領空侵犯や軍事的威圧に対抗する措置として、護衛艦「さざなみ」の派遣を指示している⁽³⁾。また、情報政策の観点からは、海底ケーブルの安全保障上の脆弱性も看過できない。2025年1月、台湾海峡付近において中国船による海底ケーブルの断線が疑われる事案が発生し、*New York Times* はこれを正面から取り上げ、すでに台湾有事が情報インフラを標的とする形で進行している可能性を指摘している⁽⁴⁾。

さらに、バルト海地域でも同様の事例が相次いでいる。2024年11月には、スウェーデン、フィンランド、リトアニアなどで海底ケーブルが断線し、通信網の遮断という重大な事態が報告されている⁽⁵⁾。これらの事例は、領土・領空・宇宙空間に加え、サイバー空間の安全保障が今や不可欠な要素となっていることを強く示している。

このような現状を踏まえると、情報政策を安全保障の一環として再構築していく必要がある。AI技術の発展、特にOpenAIのような先端技術の進展により、情報の生成・拡散・操作の在り方が根本的に変化しつつある現在、この問題の重要性は今後さらに増していくだろう。

今後も、同様の事象は頻発する可能性が高い。それゆえに重要なのは、個別の事象の分析にとどまらず、安全保障の枠組みの中で情報政策を位置づけ、理論的かつ実践的な検討を行っていくことである。本稿では以下において、そのための手がかりと枠組みの提示を試みる。

2 章 理論的な枠組みの提示：安全保障としての情報政策

本章では、情報政策を安全保障の枠組みに位置づけるための理論的な枠組みの可能性を提示することを目的とする。

2.1 国際政治学の立場から

国際政治学の中でも、スーザン・ストレンジの定義は本論を進めるうえで有益である⁽⁶⁾。その理由として、安全保障の範囲と対象について、「誰が誰に対して安全を保障するのかという問題であり、またどのような（一つのまたは複数の）脅威を認知して安全を守ろうとするのか」と述べていることから（p.109）、情報政策を安全保障の観点から捉える際の基本的な問いを構成する。

たとえば、前章で言及した海底ケーブルの問題においても、事件が表面化していない、あるいは意図的に表面化されていない事例が見受けられる。実際、これらの事案に対しては、明確な抗議や対抗措置よりも、回避的・黙認的な姿勢が取られる傾向にある。これは、地上戦に比べて証拠の隠蔽が可能であるという海底ケーブルの特性とも無関係ではない。

しかしながら、「安全保障」の観点からすれば、情報網への攻撃に対して明示的に同意する国家は存在しない以上、海底ケーブルの破壊は明確に国家の安全を脅かす行為として位置づけるべきである。ストレンジが述べるように、「二つの権威が、暗黙のうちにであれ表立ってであれ、対等な立場で共存することに同意しないがゆえに争っている状況、または、相対的に弱い立場にある権威が、より強い権威によって認められた支配領域を越えようと努めている状況」も考慮する必要がある（p.116）。

台湾有事の文脈では、中国が台湾のインフラ、特に情報インフラを一方的に攻撃している現状がある。これは単なる軍事的威圧にとどまらず、領土の実効支配や搾取を企図するものであり、しかも情報網という海底という曖昧な空間を介して行われる攻撃である点に特徴がある。この点についてストレンジは、「安全保障構造が脅かされるのは、対抗的社会集団の存在自体に原因があるのではなく、ある権威が他の権威の支配領域や権限に挑戦し、その挑戦が後者によって認知された場合に限られる」とも指摘しており（p.118-119）、まさに今日の台湾海峡やバルト海で生じている海底ケーブルの問題はこの構造的脅威と密接に関係しているといえる。

2.2 技術進展が拓く安全保障の新局面

次に、技術の進展に応じた安全保障政策の変化について概観しておきたい。内閣官房『国家安

全保障戦略2022』によれば、「サイバー空間、海洋、宇宙空間、電磁波領域等におけるリスクの深刻化」が指摘されており⁽⁷⁾ (p.5)、サイバー空間は現代の安全保障上の最重要課題の一つと位置づけられている。さらに『国家安全保障戦略(概要)』においても、サイバーセキュリティは繰り返し強調されており、「能動的サイバー防御の導入及びその実施のために必要な措置」や、「新たな調整組織の設置、法制度の整備、運用の強化」が具体的な戦略として示されている (p.7)。このように、サイバー空間の安全保障はもはや技術の領域にとどまらず、政治・法制度・行政運用を含む包括的な枠組みで対応すべき課題であるとされている。

安全保障研究の理論的視点からも、この問題は重視されている。宮岡は、サイバー空間の特徴として「技術や我々の認識とともに発展しており、その実態は常に流動的である」(p.212)ことを指摘している⁽⁸⁾。注目すべきは、技術そのものの変化に加えて、私たちの「認識」の変化もまた、安全保障上の課題に直結しているという点である。また、伊東は「サイバー戦争はすでに始まっている」と述べ、「この戦争では守っているだけでは必ず敗北する。攻防両面からの国際的な防衛戦略の構築が急務である」(p.225)と主張している⁽⁹⁾。ここでは、サイバー攻撃に対する受動的な対応の限界と、能動的・積極的な戦略の必要性が強調されている。

このような認識を踏まえて、内閣官房は2025年に『「サイバー対処能力強化法」および「同整備法」』(令和7年5月16日成立、同年5月23日公布)を整備した⁽¹⁰⁾。公開資料によれば、サイバー攻撃の質・量の両面で脅威が高まっている現状と、欧米諸国の先行的取り組みを背景として、能動的サイバー防御の必要性が体系的に位置づけられている。このように、サイバーを取り巻く環境は日々変化しており、そうした変化に対応した政策決定のプロセスや、意思決定の論理を明らかにすることが、今後の研究にとって極めて重要な課題となる。

2.3 ま と め

情報政策は、それ単独で議論されるべき対象というよりも、研究や政策との強い連関を持ちながら、安全保障の枠組みの中に組み込まれて初めて、その意義が明確になる。したがって、国家のリーダーである大統領や首相がどのような問題意識を持ち、どのように国家を導こうとしているのかを把握することは、情報政策と安全保障の具体的な関係を明らかにするうえでも重要である。

さらに言えば、これは単なる安全保障の問題にとどまらず、広義の政治の問題と密接に関連している。以下では、アメリカ、イギリス、日本において安全保障上重要な政策文書を発表したジョー・バイデン、リシ・スナク、岸田文雄の各政権における取り組みを検討する。これにより、表層的には見えにくい安全保障政策の実態を浮かび上がらせ、私たちが見逃している可能性のある「政治と安全保障の相互作用」を可視化することを目指す。

3 章 情報政策の安全保障的定位に関する諸条件の検討

3.1 リーダーシップとは？

先に示したとおり、本稿では「リーダーシップ」という概念を用いて議論を展開してきたが、ここでその定義を確認しておきたい。リーダーシップは多分野において用いられる汎用的な概念であるが、本稿においては品田の定義を援用する⁽¹¹⁾。品田は、リーダーシップを多層的性格を有するものと捉え、すなわち①構造的要因に基づく理論的広がり、②指導者側の戦略に基づく合理的説明、③手法の多様性といった側面から分析可能であると指摘している。この分類に依拠するならば、本研究は「指導者側の戦略に基づく合理的説明」に焦点をあてた事例研究として位置づけることができるであろう。また、収集したドキュメントを一つの社会現象として把握することも可能である。加えて、自伝的要素を導入することで、対象人物の内的要因と社会的影響との関係を描出することも考えられるが、自伝的アプローチについては本稿においては扱わず、別稿においてその方法論を包括的に検討する予定である。

3.2 対象とする人物

以上の問題意識を踏まえ、本稿ではアメリカ、イギリス、日本におけるリーダー（主に大統領・首相）が提示してきた国防政策を対象とし、その具体的内容を分析する。分析対象は、ジョー・バイデン（アメリカ）、リシ・スナク（イギリス）、岸田文雄（日本）の三名である。

バイデン元大統領は、大統領令において DEI（Diversity, Equity, Inclusion：多様性・公平性・包摂性）を強調し、アメリカ社会における多様性を重視するリベラルな政治家としての側面が広く認識されている。しかし注目すべきは、それに加えて国家防衛を重視した数多くの安全保障政策を打ち出した点である。この側面は、日本国内においては必ずしも十分に認識されていない可能性がある。

スナク元首相は、40代前半で保守党から首相に就任し、インド系の出自を有する点でも注目を集めた。大学院修了後は金融機関に勤務し、その後財務大臣を歴任しており、経済・社会動向に敏感な政治家であるといえる。加えて、安全保障分野においても重要な役割を果たした。具体的には、海底ケーブルの戦略的重要性を論じた報告書を公表するとともに、サイバー攻撃対策および半導体分野での協力を目的としたデジタル・パートナーシップを主導した。また、岸田首相との首脳会談においては、自衛隊と英軍の共同訓練を可能とする「日英円滑化協定」に署名し、これを「1902年の日英同盟以来、最も重要な安全保障協定」と位置付けた点からも、日本との安全保障協力を重視する姿勢が明確に示された⁽¹²⁾。

岸田文雄元首相についても言及しておきたい。氏は台湾有事への対応策を提示したほか、『国家安全保障戦略 2022』において国力の構成要素を外交力、防衛力、経済力、技術力、情報力と明確に定義し、そのうち防衛力については「反撃能力」の保有を通じ抑止力の強化を打ち出した⁽¹³⁾。さらに、AI のリスクを国際的課題の一つとして取り上げ、将来的な安全保障上の懸念を先取りした視点を提示した点も特筆に値する⁽¹⁴⁾。岸田政権期における国内での評価については本稿では分析対象としないが、少なくとも国力要素を構造的に整理し、AI というグローバル課題への対応を言及した先見性については評価されるべきである。

以上の三名を対象として、本研究は第4章において情報政策と安全保障に関するドキュメントの分析を行う。

4章 事例

4.1 ジョー・バイデン

(1) National Security Strategy (October 2022)

まず検討すべき資料は、2022年10月にバイデン大統領およびハリス副大統領の政権が発表した『国家安全保障戦略 (National Security Strategy)』⁽¹⁵⁾である。この文書においては、主として二つの課題が強調されている。第一に、世界的規模で大国間の勢力争いが続き、その帰趨が依然として不透明である点である。第二に、国家を超えて共有される共通課題、すなわち気候変動、食糧不足、テロリズムなどに各国が直面し、その影響への対応に苦慮している点が指摘されている。アメリカは、世界秩序を牽引する立場にありながら、過去に例を見ないほどのリスクにさらされているとの認識を示している。

さらに同文書においては、テクノロジーが安全保障および経済をはじめとする国家戦略の中核を構成することが強調されている。すなわち、経済的繁栄および軍事的優位を支える基盤としてイノベーションが不可欠であり、特にAIをはじめとする先端技術は、経済の再構築、軍の再編成、さらには国際秩序の変革に寄与するものとして位置付けられている。また、同盟国との共同開発を通じて強固な供給網を構築し、各国にとって利益をもたらすことも示されている。

加えて、本戦略は、半導体、AI、誤情報対策、安全保障と人権の保護、輸出規制の遵守といった分野において、同盟国との協力を推進することにより、国際的なテクノロジー・エコシステムを形成していく方針を明確にしている。

(2) White House Council on Supply Chain Resilience (Executive Order 14123 of June 14, 2024)

バイデン政権の終盤に発表された大統領令(2)⁽¹⁶⁾においては、冒頭で「本政権は、アメリカの強靱な供給網の構築を政策の柱とする」と明言されている。その上で、経済的繁栄、公衆衛生、安全保障の三領域を優先課題として位置付けている。また、サイバーテロリズムが重要インフラや製造・加工能力、さらには重要物資・材料・サービスの供給を低下させる潜在的脅威であることが指摘されている。

同文書はさらに、経済活動の基盤を強化するためには、国内製造能力の増強、研究開発における国際的競争力の維持、イノベーションの促進、重要インフラの強靱化、ならびに高水準の雇用創出が不可欠であると論じている。このような取り組みは、国家の繁栄を支えるのみならず、気候変動への対応を前進させ、国家的緊急事態への備えを強化し、全国的な経済成長を促進する基盤を形成するものと位置付けられている。

以上を踏まえると、バイデン政権は多様性や民主主義の推進といった側面が前面に注目されがちであるものの、実際には国力維持の戦略として供給網の強化や脅威への対応を重視していたことが明らかである。

4.2 リシ・スナク

(1) Undersea Cables: Indispensable, Insecure (2017)

次に取り上げるのはリシ・スナクである。意外に思われるかもしれないが、スナクは首相に就任する以前からシンクタンクとの共同研究を通じて安全保障に関する報告をまとめていた。その代表的成果が *Undersea Cables: Indispensable, Insecure* (2017) であり⁽¹⁷⁾、海底ケーブルに焦点を当てた包括的な報告書である。

同報告書によれば、イギリスは海底通信ケーブルに大きく依存しているが、世界全体で存在するケーブルはおよそ 213 本に過ぎず、現在の国際ネットワークにおける代替手段は事実上存在しない。これらのケーブルは国際送金を含む経済活動に不可欠の役割を果たすと同時に、政府間の通信にも深く関与している。したがって、仮にこれらのケーブルがテロの標的となれば、国家間の意思疎通に深刻な支障をもたらす危険がある。加えて、「海底」という地理的に限定された場所に設置されているため、標的となりやすい脆弱性を抱えていることが指摘されている。

さらに、サイバー空間においても海底ケーブルや地上施設が標的となりやすいこと、そして高度に相互接続された現代社会においては、一部が破壊されただけで世界的規模の分断を引き起こす可能性が示唆されている。そのため、とりわけ一箇所に依存する構造をいかに改善するかが、今後の課題として提示されている。

(2) A Guide to RFA Proteus — the UK's New Seabed Warfare Vessel,” Navy

Lookout⁽¹⁸⁾, Oct 10, 2023

スナクは、海底ケーブルを安全保障上の重要課題として早期から指摘していたが、その後も関連する施策を実施している。特に、ノルドストリーム爆破事件直後には、2億5千万ポンド（約460億円）規模の費用を要する国有迎賓船（National Flagship）の建造計画を取りやめ、その代替として高性能無人潜水艇の運用を可能とする多用途海洋観測船（Multi-Role Ocean Surveillance Ship, MROSS）の取得・前倒し就役を決定したことが報告されている。これらの対応は、スナクの危機対応における迅速性を示す事例と評価できる。

本稿では情報インフラとしての海底ケーブルに焦点を当てたが、スナクの政策対応はそれを超えて、国家戦略の策定において一貫して安全保障を最優先に位置付けていたことを窺わせる。実際、スナクはイギリスの地政学的特性を踏まえ、安全保障上のリスクを強調してきた一方で、その後に顕在化したウクライナ戦争の危険性を十分に予見できなかったことについては、自らの見通しの不十分さを認め謝罪していることが明らかにされている。

4.3 岸田文雄

(1) 国家保障安全戦略 2022

岸田政権の最大の功績の一つと評価し得る取り組みが、『国家安全保障戦略 2022』⁽¹⁹⁾の策定と、G7 広島サミットにおいて「広島 AI プロセス」を発表し、生成 AI のリスクに関する包括的政策枠組みを提示した点である。広島 AI プロセスでは、次のような方針が示されている。すなわち、「広島 AI プロセスを通じた我々の共同の取組が、デジタルデバイドの解消およびデジタル包摂性の達成の観点から、開発途上国および新興エコノミーを含む世界共通の利益のために、リスクを軽減しつつ技術の利益を最大化するため、安全・安心で信頼できる AI システムの設計、開発、導入および利用を可能とする開かれた環境を促進する」⁽²⁰⁾ことが明記された。

さらに、この取り組みは各国政府の政策に留まらず、学術界、市民社会、民間部門、公共部門に対しても実施指針を提示している。特に、高度な AI システムの設計、開発、導入においては、法の支配、人権の尊重、適正手続、多様性、公平性、無差別、民主主義、そして人間中心主義を基本原則として遵守すべきことが強調された。

(2) AI セーフティ・インスティテュート

2023 年 12 月 21 日に開催された AI 戦略会議において、岸田総理大臣は「AI セーフティ・インスティテュート（AI Safety Institute: AISI）」の設立を表明し、これを受けて 2024 年 2 月 14 日に同機関が正式に発足した。同機関の公式ウェブサイトによれば、その趣旨は「安全・安心で

信頼できる AI の実現に向けて、AI の安全性に関する評価手法や基準の検討・推進を行うための機関」⁽²¹⁾と定義されている。

AISI の活動は、日本国内の各省庁や関連研究機関にとどまらず、国際的な連携業務をも包含している点に特徴を有する。とりわけ、その任務の一つに「AI の安全性評価の枠組みを策定すること」が明示されていることから、AISI は AI の適合性と信頼性の確立において中核的役割を担う組織として機能することが期待されている。

4.4 ま と め

2025 年 8 月時点においては、いずれの人物もすでに大統領や首相の地位を退いている。しながら、彼らが国家の安全保障に資する具体的な指針を提示してきた事実は十分に確認できる。無論、各人物の意図が政策文書にどの程度反映されているかについては判然としない部分もある。しかし、現存するドキュメントを検討する限り、情報政策を安全保障の枠組みの中で位置付ける試みはすでに始まっていることが明らかである。したがって、情報政策は今日、安全保障に内包される要素の一つとして位置付けられつつあるといえる。

5 章 ま と め と 今 後 の 課 題

以上の検討から明らかになるのは、情報政策、特に AI をめぐる議論においては、テロリズムを含む安全保障の文脈で取り上げなければ、基盤となるコミュニケーションそのものが成立しなくなるという危機意識が前提にあるという点である。そのうえで、現状において顕在化している問題を可視化し、次なる取り組みに向けて迅速に対応するか否かこそが、リーダーシップの具体的表れであると位置付けられる。

スナクに関しては、金融分野での経験を有していたこともあり、民間シンクタンクと連携しながら実証的な報告書を作成し、その中で指摘された課題に対して政策的対応を進めてきた点が注目される。バイデンの場合、一般にリベラルな政治家として認識されているものの、実際には安全保障関連の諸組織と連携しつつ、リスクへの対応を進めてきた事実は広く知られており、アメリカの戦略的特色を示しているといえる。日本の場合、対応の開始が相対的に遅れた印象を与える一方で、単なる AI イノベーションの推進にとどまらず、安全性や適合性を評価する制度的枠組みを構築しようとするなど、むしろリスク管理を重視した政策的姿勢が見て取れる。

これらの動向の背後に存在するのは、それぞれの国家を取り巻く地政学的リスクであり、リスク＝安全保障として捉えられている点にある。その認識が当事者によって明示的に共有されているかは必ずしも判然としないものの、少なくとも各国の議論はこの枠組みの中で展開されている

と解釈できる。

今後の課題としては、各種政策文書を対象にテキストマイニング等の手法を用い、その全体的傾向を探索することが考えられる。また、それ以上に重要な方向性としては、各リーダーの自伝的 (autobiographical) 側面と実際の政策対応との関係を明らかにすることであり、この点については今後の検討課題としたい。

《注》

- (1) 内閣官房「武力攻撃やテロなどから身を守るために」https://www.kokuminhogo.go.jp/pdf/hogo_manual.pdf
- (2) 高市早苗記者会見 2024 年 8 月 30 日 https://www.sanae.gr.jp/kaiken_detail708.html
- (3) 海自護衛艦「さざなみ」が台湾海峡を初通過、岸田首相が派遣指示…軍事的威圧強める中国をけん制『読売新聞』2024 年 9 月 26 日 <https://www.yomiuri.co.jp/politics/20240925-OYT1T50170/>
- (4) Anderson, C., & Nierenberg, A. (2025 January 27). Damage to a cable in the Baltic Sea heightens tensions with Russia. The New York Times. <https://www.nytimes.com/2025/01/27/world/europe/cable-baltic-sea-sweden-damage.html>
- (5) CNN. (2024, December 25). Finland investigates outage of undersea power link to Estonia, Finnish PM says. <https://edition.cnn.com/2024/12/25/europe/finland-estonia-power-under-sea-intl>
- (6) Strange, S. (2020).『国家と市場：国際政治経済学入門』（西川 潤・佐藤 元彦（訳））筑摩書房
- (7) 内閣官房『国家安全保障戦略 2022』https://www.cas.go.jp/jp/siryoku/221216anzenhoshou/national_security_strategy_2022_pamphlet-ja.pdf
- (8) 宮岡勲 (2023).『入門講義 安全保障論 第2版』慶応義塾大学出版会
- (9) 伊東寛 (2016).『サイバー戦争論:ナショナルセキュリティの現在』原書房
- (10) 内閣官房 (2025).『サイバー対処能力強化法及び同整備法』令和7年5月16日成立、同年5月23日公布 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html
- (11) 品田 裕 (2008). リーダーシップの比較政治学 はじめに、日本比較政治学会年報、10 巻, p.i-vi, <https://doi.org/10.11193/hikakuseiji1999.10.i>
- (12) 外務省の HP を参照のこと https://www.mofa.go.jp/mofaj/erp/we/gb/page1_001466.html
- (13) 注(7)を参照。
- (14) 同上。
- (15) *National Security Strategy* (October, 2022) <https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>
- (16) White House Council on Supply Chain Resilience. Executive Order 14123 of June 14, 2024 <https://www.federalregister.gov/documents/2024/06/21/2024-13810/white-house-council-on-supply-chain-resilience>
- (17) Snack, R. (2017). Undersea Cables: Indispensable, insecure. Policy Exchange. <https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/>
- (18) A Guide to RFA Proteus — the UK's New Seabed Warfare Vessel,” Navy Lookout, Oct 10, 2023
- (19) 注(7)を参照。
- (20) 内閣府「広島 AI プロセス」<https://www.soumu.go.jp/hiroshimaaiprocess/>

(21) AI セーフティ・インスティテュート (AISI) の HP <https://aisi.go.jp/about/>

(注) なお URL については、全て 2025 年 9 月 26 日に確認した。

Intersection of information policy and security:
Strategic approaches under
the Biden, Sunak, and Kishida administrations

Hiroyuki Ida

Abstract

This research note investigates the integration of information policy within the domain of national security by examining key security documents issued under the administrations of Biden (United States), Sunak (United Kingdom), and Kishida (Japan). Particular attention is given to the treatment of artificial intelligence and other emerging technologies within these strategic frameworks. While the three administrations differ significantly in their political orientations, the analysis demonstrates a shared recognition of information policy as a security concern that demands proactive, risk-oriented measures. The findings suggest that information policy has become a critical component of contemporary national security strategies across advanced democracies.

Keywords: security, information policy, leadership