第５章

豪日防衛協力の将来の道筋 ── オーストラリアの視点

アンドリュー・デイビス

要旨

オーストラリアと日本は非常に多くの安全保障上の利益を共有している。なかでも特筆されるのは、両国がともに有する「ハブ・アンド・スポーク」モデルに基づく米国との同盟関係である。したがって、豪日両国がパートナーとして協力し合うのは多くの意味で自然な成り行きといえよう。しかしながら、理由は様々だが、可能性のある防衛協力のメカニズムを両国が探り始めたのはごく最近のことである。模索できそうな道筋はいくつかある。共同作業が考えられる分野は、複雑性（complexity）や敏感性（sensitivity）が低い順に、以下のように大まかに分類できる。

敏感性が低い

- 人道支援・災害救援の能力
- 海賊対策や対テロ対策などの「二級（second order）」の安全保障活動
- サイバー防衛に関する協力

敏感度が中程度

- 軍事演習
- 軍事能力開発に関する協力（たとえば潜水艦技術や弾道ミサイル防衛など）

敏感度が高い

- 対外情報収集に関する協力
- 米国の「エアシーバトル（Air Sea Battle）」モデルに対する共通対応の立案
- サイバー戦争や電子攻撃など、敏感性の高い「非対称」能力に関する協力

敏感性の低い活動は、容易に正当化し遂行できる。敏感性が中程度の問題は取り組み可能であるし、現状以上の活動を実施できる分野である。敏感性の高い活動についてはさらなる議論が必要だが、米国のアジア太平洋リバランスにより、豪日両国はこれらの問題の検討を否応なく迫られることになる。

協力すべき理由

オーストラリアと日本はサンフランシスコ平和条約に基づく米国の同盟国であり、民主主義国家であり、経済協力開発機構（OECD）加盟国であり、安定した国際秩序における利害関係国である。両国はともに、過去半世紀にわたり米国のリーダーシップに大きな恩恵を受けてきた。その結果として両国は、両国の繁栄と安全保障を可能にしてきた国際規範の維持に共通の利益を有している。

これが、豪日両国が2007年3月に「安全保障に関する日豪共同宣言」に署名した主たる理由である。同宣言の目的は、「新たな安全保障上の課題と脅威に対応」し、両国間の「安全保障協力の強化のための包括的な枠組みを策定する」ために両国が協力できるメカニズムを創出することであった。それ以後、安全保障情勢は一層複雑になったと言っていいだろう――「悪化した」と言うのは控えたい。なぜなら、当時両国の念頭にあったのと同じ要因が現在も引き続き存在しているからだ。なかには、国際テロの脅威など、低減したように見える要因もある。しかし一方、大量破壊兵器（WMD）拡散の脅威はまだ残っているほか、アジア太平洋地域のパワーバランスは望ましくない方向にシフトしつつある。また、サイバーセキュリティ上の脅威は2007年以降に急速に高まっている。

「共同宣言」以降の5年間には、両国間の協力のあり方についての共通概念の構築に着実な進歩があったものの、どちらの側も、両国関係における最大限の可能性の実現にはまだ遠く及ばないと考えているように思われる。そろそろ次のステップを検討してよい時期だ。

なぜ今なのか

豪日間の安全保障協力の取り組みがこれまであまり進まなかった主な理由は、おそらく特にそうするべき差し迫った理由がなかったからだろう。上述のような利益を共有しているとはいえ、両国の首都は 8,000 キロも隔たっているため、定例的な協力を行うとなれば実際的な諸問題が生じる。また、20 世紀後半を通じ、両国は長きに渡る（ほぼ）平和な時代を享受し、各々の国家の構築を進めるのに忙殺されていた。要するに、協力の費用がその効果に対して高すぎたのである。

しかし今日では、費用対効果の比率を変えるような、以下に挙げるいくつかの外的動因がある。

- 人口動態の傾向により、自然災害が発生しやすい地域に住む人口が増えているため、人道支援・災害救援活動への要求が高まっている。将来の気候変動による潜在的影響により、この傾向はさらに激化すると予想される。
- グローバル化により、距離がかつてのような意味を持たなくなった。非伝統的安全保障の分野では、多国籍の集団がほぼあらゆる場所から脅威を呈しうる。海洋の分野では、世界の主要な貿易ルートが事実上すべての国からの輸出入輸送を担っている。
- （上記のグローバル化に関連して）地理的に大きく隔たった国々も、特に通信とコンピュータシステムの統合により、サイバー空間における共通のインフラを共有している。
- 軍事システムのコストと複雑性の高まりから、防衛産業各社の合併の動きが進んでいるのに加え、同じ目的を持つ国同士が研究開発負担を分担できる分野を探さざるを得なくなっている。
- アジアにおける軍近代化と、その結果として生じる接近阻止・領域拒否（A2AD）システムなどの高水準能力の拡散。
- 北朝鮮、イランなどの各国が、近隣地域を直接的に威嚇でき、万一輸出されればさらに広範な重大性をもたらす核・ミサイル能力の開発を進めている。

- 中国の台頭。なかでも西太平洋地域における勢力関係の変化と、米中間の共通の世界観の欠如。
- （上記 2 点に関連して）米国は敵対国が接近を阻止しようとする環境での作戦行動に関する新たな戦略を立案している。統合作戦アクセス構想とそれに付随するエアシーバトル構想は、基地および／または軍事的貢献の形での同盟国による支援提供を奨励している。

以上のように、豪日両国（および両国と利益が一致する他の諸国）には安全保障問題に関する協力を深めるべき理由が数多くある。

上に挙げた要因の中には、豪日およびその他の国がすでに協力プログラムを実施中もしくは策定中の分野もある。例として、海賊対策における多国間取り組みがあり、これには豪日ともに艦艇を参加させている。ほかに、域内各軍間での信頼と経験の構築を目的とした軍事演習、多数の国が参加する人道支援・災害救援活動などがある。また、サイバーセキュリティとネットワーク防衛の分野でも関係が発展しつつある。これらはすべて前向きな進展であり、この種の活動が今後ますますみられるようになるのは疑いない。ただし、これらはある意味では「二級」の安全保障問題であり（サイバーセキュリティは例外だが）、最上位の軍事能力と、アジア太平洋地域およびその周辺の地理的・政治的要因から生じるさらに困難な問題とがかかわる「一級（first order）」の安全保障問題に比べれば、進展させるのは難しくない。本稿の主題はより深い協力への将来の道筋であるので、ここから先はこうした「一級」の分野に、それらが困難であると同時に重要でもあることが明らかになるものと認識しつつ、焦点を絞っていくことにする。

しかしながら、豪日両国が必ずしもすべての安全保障問題について深い協力を模索すべきだということではない。両国の利益がさほど大きく一致しない事例もあるだろう。どの場合に際しても、両国政府は費用と（即時または潜在的な）効果を比較検討し、どうすれば自国の利益に最も効果的かについての判断に基づいて意思決定を行うはずである。たとえば、ソロモン諸島や東ティモールの安定に関しては、日本はオーストラリアほど大きな利害関係を持たない。同様に、オーストラリアが北

アジアの安全保障にどこまでなら巻き込まれていいと考えるかは、現在もなお国内議論の注目テーマである。上述の共同宣言に際し、当時のオーストラリア野党党首（後に首相）のケビン・ラッドは、日本との安全保障協力の強化は支持しながら、相互防衛条約については「北東アジアにおける安全保障政策の先行きが不透明な今の段階では、その今後の変化にわが国の安全保障上の利益が不必要に縛られることになりかねない」として反対した。また、ヒュー・ホワイトなど影響力のあるオーストラリアの識者らは、米中に対してより中立的な政策路線を積極的に擁護している。

日豪米およびその他諸国の間での協力の程度は、各当事国の将来の政府により決定され、その際各国政府は多くの要因を慎重に考慮することになる。豪日にとって最も重要な要因のひとつは、米国が実行しようとしている幅広い安全保障の枠組みへの豪日両国の貢献に対する米国の期待である。率直に言えば、ここで問題にしているのは中国の台頭に対する地域大国の対応だ。米中間ではすでに戦略的競争が始まっている。これまでのところは当たり障りなく来ているが、事がもっと複雑化する可能性があり、危険も孕んでいることを示す兆候がある。米国は、豪日両国に軍事安全保障の分野でより一層の貢献を望むと公言している。豪日両国が米国の大局観の中でどのような位置を占め、どのようなスタンスをとりうるかを自ら検討しないのは、賢明ではないだろう。

エアシーバトルと米同盟国

現在のところ、豪日（および域内の他の諸国）の主要な政策課題のひとつは、進行中の米国のピボット／リバランスとそれに伴う戦略的・軍事的構想の進展に（個別に、ならびに集団的に）どのように対応するかという点である。そうした構想のうち最も重要なのは「エアシーバトル」構想で、増大しつつある A2/AD の脅威に対処すべく軍事ドクトリンを再調整しようとする米軍の取り組みが、ここに最も顕著に表れている。これまでのところ、米国における「エアシーバトル」に関する議論では、この構想についてのアジアの米同盟国の見解や役割には比較的関心が向け

られていない。しかし、戦略予算評価センター（CSBA）の報告書には、「エアシーバトルは米国のみの構想ではない。日本やオーストラリアなどの同盟国、および場合によってはその他の諸国も、安定した軍事バランスにおいて重要な実効ある役割を果たさなければならない」との指摘がある。この一節は、豪日両国の防衛計画策定にいくつかの重要な戦略上の検討事項を浮上させるとともに、安全保障同盟国としての米国と主要貿易相手国としての中国との間で微妙なバランスをとる必要がある立場 ── この点は豪日両国に当てはまる ── をさらに複雑にする可能性がある。

エアシーバトルに関する情報は、少なくとも公になっているものとしては、比較的少ない。ただし、米国の構想には A2/AD を打破するための多層的アプローチが含まれていることと、豪日両国の軍構造とドクトリン策定に影響を与えうる点がいくつかあることはわかっている。あるいは、豪日のどちらか、または両国ともが、想定外の決断を迫られることもありうる。この意味できわめて重大なエアシーバトルの要素として、以下のものがある。

- 北アジア（特に韓国、日本、グアム）の基地強化
- より広範な地域に米軍を分散させる「多層防衛」のアプローチ
- 中国人民解放軍の指揮統制および情報・監視・偵察（ISR）能力を破綻させるための戦術と技術
- 遠距離目標に対する深部攻撃能力
- 中国に出入りする船舶交通に対する遠距離封鎖作戦

上記の活動のうち初めの 2 つは実施が比較的容易で、米国との二国間ベースで実行が可能である。基地強化や米軍駐留受け入れに関する合意は、基本的に米国とその同盟国やパートナーの間でそれぞれ協議すべき問題だ。たとえば、シンガポールは米海軍軍艦 4 隻の受け入れに合意し、一方オーストラリアは米海兵隊員 2,500 名の駐留と追加の米艦の寄港を受け入れることになっている。しかしながら、上記の残り 3 つの項目は実に重大な作業であり、豪日両国が参加するとすれば、米同

盟国を代表してきわめて大きな責務を負うことが必要になる。

だが少なくとも、参加する場合に必要になる能力については、たとえ結果的にそこまではとても到達できないと判断することになるとしても、考えてみるべきだろう。また、これらの問題についての協議が必要になる経緯は、豪日いずれの場合も物議を醸すであろうことは予想できるが、両国で同じではないだろう。オーストラリアは多数の戦争参加も含めて、主要な有力同盟国を支援する遠征軍事作戦に長く関与してきた。したがってエアシーバトルへの参加は、従来の国の政策とある程度は一貫性があることになる。しかし上述のように、オーストラリアは現在、米国との協力をどこまで深め、中国との対立をどこまで回避するか――要するに、わが国の安全保障と経済的利益のバランスをどうとるか――について議論している最中である。日本も同じ問題に直面しており、加えて未解決の領土紛争も抱えているが、憲法第 9 条の問題によりエアシーバトルへの参加はさらに込み入った問題になると考えられる。たとえば、日本が深部攻撃能力の開発を検討することになるとは考えにくい。

また、空海戦闘のすべての要素が、我々が支持したいと望むようなものであるかどうかは不明確である。たとえば、重大な対立の最中に核大国の指揮統制や ISR ネットワークを広範囲に破綻させることは、エスカレーション管理の助けにはならない。将来紛争が起これば、これが主要な懸念のひとつになる。これらは重大な問題であり、この構想が進展するにつれて、米国がその考え方をより詳細に開示することが望まれる。

いずれにせよ、豪日両国にとって、全面参加は論外としても、段階的な関与（将来必要な状況になれば、どちらかの方向に軌道修正できる）や米国の構想に対する支持と支援ならば可能なことはある。そのような活動としては大まかに 2 種類、すなわち米海軍と相互運用可能な海軍力の育成と、コンピュータネットワーク作戦に関する能力開発における協力が挙げられる。いずれも豪日をエアシーバトルにコミットさせるものではないが、米国独自の能力に厚みを加えるものとして米国に歓迎されると見込まれるほか、豪日にとっては様々なコミットメントレベルで米国の諸活動に参加する選択肢を与えられることになろう。

潜水艦 ── 豪日の協力分野？

豪日はともに高度な海軍能力を有し、両国とも P3 オライオン、イージス戦闘システム、シーホーク・ヘリコプターなどの米国製システムを採用している。両国海軍とも米海軍と統合演習を行い、米海軍との相互運用性の程度もかなり高い。海上での米軍との協力を可能にするうえで、残る課題はあまりないと言える。しかしながら、相互運用性の目的をさらに進めうる日豪米 3 国間協力の機会がひとつある。それは、オーストラリアの将来潜水艦（FSM）計画である。

FSM はオーストラリア国内で盛んに議論されているテーマであり、現在、今後の最善の道筋を決めるための情報収集を行っているところである。検討されている選択肢は 4 つある（すべてディーゼル電気式）が、確定的な要件は、耐久性が高く十分な有効搭載量のある長距離潜水艦であることだ。また、米海軍との相互運用性と、可能な限り最良の能力を確保したいとの希望を考えれば、米国製の戦闘システムと兵器を搭載したコリンズ級潜水艦が保持される可能性が高いだろう。現行のコリンズ級は多数の望ましい特性を有するが、信頼性の問題を抱えており、特に推進システムに懸念がある。このことから、将来の道筋は次の 2 通りの可能性のどちらかになるであろうことが強く示唆されている。

- 現行のコリンズ級潜水艦の更新。戦闘システムおよび兵器を保持 ── または次世代の同等システムを導入 ── しつつ、推進システム（ディーゼルエンジン、ジェネレーター、電動モーター、バッテリー）を大幅に刷新する。
- オーストラリアおよび他国の通常型潜水艦の設計技能を利用し、米国製の戦闘・兵器システムを組み込んだ潜水艦を新たに設計する。

当然ながら、日本は太平洋地域での運用に適した、非常に優れた通常型大型潜水艦を建造している。北ヨーロッパの狭い低水温の海での運用向けに設計された欧州製潜水艦では、この地域には必ずしも適応できない。日本の潜水艦システムはオーストラリアにとって非常に興味深いものと考えられ、これまでに何度か FMS

計画の責任者と日本の代表者との間で協議が行われている。日本側の代表者が誰であったかについては確信がないが、防衛省が協力の可能性に関心を持っていることは確かである。

達成できる成果についてはまだわからないが、少なくとも、オーストラリアは上述のいずれかの方式をとるにあたっての選択肢として、日本の潜水艦推進技術に大いに関心を持っていると考えるのが妥当であろう。非公式にではあるが、日本の設計をオーストラリアでライセンス製造するという形はまずありえないと聞いている。同様に、オーストラリアが自国の潜水艦を日本で製造させようとするとも考えにくい。どちらの場合も産業上の問題に対応する必要が生じるし、いずれにしても、オーストラリアが米国製の戦闘システムと兵器を指向していることを考えれば、結果として船体と運用システムは欧州と米国の技術の混合になることはほぼ確実である。オーストラリア政府は潜水艦推進テストベッド施設の開発を約束している。試験されるシステムの中に、日本の技術を多く取り入れたものがあれば有用であろう。率直に言って、日本の潜水艦のほうがオーストラリアのものより信頼性は高いと考えられる。オーストラリアが日本から学べる点は多いはずである。

ネットワーク作戦

本節では、より広範な同盟国間のコンピュータネットワーク作戦に関する取り組みに豪日が寄与する可能性について論じる。議論の前提として、この種の作戦は、やはり敏感性と複雑性が低い順に、次の 3 種類に分類できる。

- コンピュータネットワーク防衛：自国のデータおよびネットワークのセキュリティ維持と、有効な対応策の実施に向けた、データおよびネットワークへの脅威に対する理解の増進。
- コンピュータ諜報活動：情報収集のためのネットワーク・エクスプロイテーション技術の利用。

- 攻撃的サイバー作戦：スタクスネット（Stuxnet）ワームと同種の「サイバー兵器」の使用、またはネットワーク侵入や切断（ネットワーク性能を低下あるいは無力化させることによる）、もしくは偽データ注入や保存情報の破壊などの手法による。

コンピュータネットワーク防衛は容易に正当化できる活動であり、重要システムの搾取を目的としたスパイ行為や妨害行為などの敵対的活動に対するまったく合理的な対応である。豪日両国（およびその他の諸国）のシステムに対する脅威の多くは発生源が同じであることを考えれば、サイバー防衛に関する協力は大いに理にかなうことであり、一部ではすでに始まっている。効果的な協力を妨げている最大の要因は、おそらく各国政府の組織構成の問題だろう。オーストラリアでは（日本も同様と思われるが）、あらゆる種類のサイバー脅威 ── 個人や企業に対する犯罪リスクから、極秘の政府データの保護にいたるまで ── に対する適切な政策決定を可能にする理想的な解決策はまだ見つかっていない。しかしながら、効果的なサイバー防衛には、ある領域の脆弱性が利用されて他の領域への侵入を許す事態を避けるための「連携」が必要である。たとえば、防衛省に接続されている政府部局からの、自衛隊に接続されているシステムへのアクセスを許してしまうというようなことがありうる。これらのシステムを利用する人々も潜在的な脆弱性となる。こうした様々な要因の結果として、一国の政府全体のサイバーセキュリティ対策を調整することは容易ではなく、異なる二国間での調整となるとさらに難しい。しかしいずれにせよ、サイバー防衛は協力の拡大が予想できる分野である。これは国際的な問題であり、したがって国際的な解決策が必要であるからだ。

もうひとつ上の段階のサイバー活動であるコンピュータ諜報活動の実施は、事実上すべての国にとって諜報活動の一環としての重要性が増しつつある。豪日間には ── また、それぞれ米国との間においても ── すでに一定の情報共有・協調の仕組みがある。ネットワーク・エクスプロイテーションを通じて収集されたデータについても、少なくとも一部は共有されるのが理の当然であろう。しかし、画像諜報や信号諜報などの他の諜報形態とは異なり、ネットワーク・エクスプロイテーションは受動的な活動ではなく、必然的に情報収集対象のインフラに侵入することになる。

この他にはない煩瑣な問題があるため、実施手順は法的・政治的な考慮事項を念頭に置いて立案しなければならない。協力活動を頭から否定する理論上の理由はないが、異なる法的管轄領域間で協働するには、これらの活動を 2 通りの国内法ならびに国際法に準拠させることが必要になる。

攻撃的サイバー作戦はさらに問題が多い。前段落と同じ法的問題がすべて当てはまるうえに、組織上の複雑性の問題が加わる。オーストラリアは信号諜報機関の管轄下にサイバー作戦センターを設置することを選んだ。この信号諜報機関は国防省に属するが、オーストラリア国防軍とは別の組織である。一方、米国のサイバー軍は戦略軍の下に設置され、陸海空軍の命令系統に属する部隊から構成されている。

最近の発表に関する筆者の理解が正しいとすれば、日本は米国モデルに近い方を選択し、防衛省の管轄下に自衛隊の一部門としてサイバー部隊を設置することになった。オーストラリアとは異なり、諜報活動との明示的な関連性はないようである。同盟諸国との協力の必要性が公言されており、報道では「米国と共同歩調をとる」ことの重要性が強調されている。オーストラリアとしては、日米両国と協力できれば理にかなうだろう。

上述のような理由により、豪日米の三国間でネットワーク作戦へのシームレスなアプローチを策定することは難しいだろう。ただし、不可能ではない。また、我々にはその方向に向けて行動を起こすべき動機もある。多くの技術的、組織的、法的問題に遭遇しながらも可能ではあると思われる早期の行動としては、図上演習や、敵対的サイバー活動に対する「ウォーゲーミング」による防衛対応などがある。これらの活動を実施すれば、関係各国が互いの方針を理解し、サイバー脅威の性質やその対応策の選択肢についてのパートナー各国の見識を聞くことができるはずである。

計画演習や作戦演習より先へ話を進めるならば、標的となるネットワークおよびその防衛策や潜在的脆弱性を含めた特性に関する情報を共有することで、サイバースペースにおける一定の「責任分担」が可能になる。参加各国は、サイバースペース内の「ランドスケープ」や活動を、自国のリソース経由で収集可能な範囲よりも多

くカバーできるようになる。また、突発的に優先度が高まった標的に対する「サージ（大量動員）能力」を獲得できる可能性もある。これは、信号諜報などの他の諜報活動分野における同盟諸国間の既存の仕組みと同様のモデルである。

最後に、「サイバー兵器」（スタクスネット型ソフトウェアパッケージなど）のソフトウェア開発は、協力の可能性のある分野である。共通ソフトウェアの生成ではなくとも、少なくともネットワークの脆弱性に関する情報共有による協力は可能であろう。この分野は、前段で述べた「標的開発」作業から派生する可能性のある活動のひとつである。

結論

アジア太平洋地域の安全保障情勢は、確立された大国と新興大国である中国との間の戦略的競争が深まるなかで、複雑化する方向へ――ある意味ではより危険な方向へ変化しつつある。直面する課題に対する米国の対応は、多くの面でいまだ「作業中」の段階にあり、「アジアの世紀」に対するより含みのあるアプローチが現れてくるにつれて、公の場でみられる攻撃的な色合いの強い見解が脇へ追いやられる可能性がある。

しかしながら、域内における米国の緊密な同盟国であるオーストラリアと日本は、米国が両国に寄せるであろう期待についてよく考える必要がある。そして、同盟国である米国を協力して支援するにはどうすればよいか、また、米国の戦略を支援するためにどこまでの行動をとる覚悟を持つかを判断しなければならない。本稿では、豪日両国が全体の利益のために地域の安全保障において役割を果たす能力を高めるために、両国が協力しうる方策を広範に論じてきた。ここで述べた選択肢の中には、「容易」なもの――難なく正当化でき、さほどマイナス面のリスクがないもの――もあれば、危険性が高まるおそれがあり、中国に歓迎されないのは確実なものもある。豪日両国にとって鍵となるのは、費用対効果を慎重に検討し、今後どの分野を推進したいかを判断することだろう。