基調講演

シグナル・インテリジェンスと日本の安全保障

ジョン・フェリス

本稿では、過去100年間の戦争とパワー・ポリティクスにおけるシグナル・インテリジェンス（シギント）の役割について検討する。本稿では、英国、特にそのシギント機関である政府通信本部（GCHQ）の経験について焦点を当てるが、筆者のナラティブと分析においては、現代日本の関心事項についても取り上げる。2022年時点では、インテリジェンスの専門家は、シギントの歴史の多くを把握しているが、これらは僅か10年前には謎に包まれていた。それでも、専門家たちは、シギントの歴史について連続的なナラティブを提示することも、把握している多くの詳細を発表することもしていない。戦略や国際関係を研究する歴史家たちはこうした動向をほとんど把握していない。日本の歴史家や国民は、1904-45年におけるシギントの経験については多くを把握しているものの、その後の経験については把握していない。日本のシギント担当官と当局者は、米国のシギントとの現代的関係を理解しているものの、こうした問題が日本国内で議論されることはほとんどない。日本がパワー・ポリティクス、場合によっては戦争をめぐる競争に足を踏み入れようとしているにもかかわらずである。今後の競争においては、二度の世界大戦や冷戦同様、インテリジェンスが活躍するだろう。こうしたシギントをめぐる全般的な経験は、現在の日本の状況、ニーズと機会を明らかにしている。

シギントと二度の世界大戦

日本は、大国のなかでも独自のシギント経験を有している。1900-45年にかけて、日本はシギントを通じてある程度の恩恵を受けてきたものの、その後は一方的かつ多大な損害を被った。最終的にはシギント機関を改めて整備したが、それは外国シギント機関の補助的な役割を果たしてきた。

日本は、戦時中に無線傍受によるシギントをいち早く経験した国の1つである。1905年、日本海海戦の直前に、ロシアのジノヴィー・ロジェストヴェンスキー提督は、日本艦隊の動向を無線信号の強度や位置で判断するとともに、海上のもや、戦場の霧のなかを前進しつつ、自艦隊については無線封止を行うことで、日本艦隊の陣形を突破しようとしていた。東郷平八郎提督は、無線を最大限に活用して自艦隊を指揮し、敵を探知した。これには犠牲が伴ったものの、勝利に欠かせないものであった。こうした知識を基に、ロシア艦隊

は勇敢にも日本艦隊の突破を図ったが、最終的には失敗した。無線封止により、日本側がロシア軍の位置を把握する能力が制約された一方で、日本側の平文信号を傍受したことで、ロジェトヴェンスキー提督は、自艦隊が探知され、戦闘が迫っていることをついに悟った[1]。こうしたシギント面での失敗はあったものの、東郷平八郎提督は劇的な勝利を収めた。

シギント革命は、第一次世界大戦中に起きた。そのなかで、メッセージ本文の送信から得られる資料であるコミント（コミュニケーション・インテリジェンス）と、通信と指揮の結節点同士の関連を観測するトラフィック分析が結び付いた。英国はシギントで世界をリードし、連合国に知られざる貢献を行った。英国はドイツとのシギント競争に勝利したが、この勝利は重要であった。シーパワーの物理的支配を強化し、英国王立海軍（RN）がそれまでに直面したなかで最も戦いやすい大戦となるとともに、封鎖の適用が通常より効果的で痛手の少ないものとなった。さらに、英国が米国と共に危険を回避し、それどころか米国の支援を無償で獲得する上で役に立った。軍事シギントにおいては、フランスは英国を上回り、米国も成果を挙げていた。英国の同盟国によるコミントでの最大の成功は、英国の外交暗号や、英国の国益を標的にしたものだったかもしれない。しかし、こうした英国（および協商国）の勝利は、オーストリア=ハンガリー帝国やドイツによるシギントの勝利により相殺された。後者のシギントは、より小規模な部隊でより大規模なロシア陸軍を打ち負かす上で役立った。協商国と同盟国によるシギントでの成功は同時期に起き、そうした成功が利用される前に、お互いに相手方の効果にすぐさま対抗した。第一次世界大戦におけるシギントでの最大の成功は、第二次世界大戦のそれを上回り、1916-18年における総合的な質は、恐らく1942-45年のそれに匹敵した。しかし、戦略レベルでは双方の成功が互いに大方打ち消し合っていたため、インテリジェンスが第一次世界大戦に及ぼした影響は、第二次世界大戦よりも少なかった。作戦で劇的な結果を生むためにインテリジェンスを利用するのは第二次世界大戦よりも困難であった。他方、第二次世界大戦では、部隊はより激しく、素早く攻撃を行い、1942-45年には、インテリジェンスは一方を組織的に強化し、他方を不利にした。それでも、数十万人の兵士を動員し、数百万トンの鉄鋼を生産する能力によって戦力が測られる戦争において、シギントは、それまでのどの紛争よりも重要な役割を果たした[2]。

日本はこのシギント革命を逃したものの、日本軍は速やかに能力を整備した。その能力は一流とまではいわないまでも、相当なものであった。日本軍は市場に流入したありとあ

1 Julian Corbett, *Maritime Operations in the Russo-Japanese War, 1904-1905, Volume II*, (Naval Institute Press, Annapolis, MD, 1994), pp. 216, 231.

2 John Ferris, *Behind the Enigma, The Authorised History of GCHQ, Britain's Secret Cyber-Intelligence Agency*, (Bloomsbury, London, 2020), pp. 29-64.

らゆる暗号装置の模造品を購入し、独自のシステムを設計した。日本の暗号システムは優れていたが、米英のシギント担当官は往々にしてこれらの軍事・海軍暗号を解読しており、ドイツ、ソ連と並んで日本の外交暗号を定期的に解読していた。日本軍は小規模ながら優秀な無線傍受・暗号解読部隊を編成し、敵方の暗号システムを秘密裏に窃取することでそれを強化した。こうした活動により、日本軍は中国軍に対し有利に立ち、ソ連軍のシギントとほぼ肩を並べた。米英の暗号システムから得られたインテリジェンスにより、1941年12月の日本軍による奇襲が可能になった[3]。しかし、その瞬間から、シギントは日本にとって常に致命的な弱点となった。日本のシギント機関が停滞した一方で、英米の機関は質・量ともに爆発的成長を遂げた。英国の支援を受けて、米国は日本の主要な暗号システムについて素早く習得し、太平洋各地における作戦の指針となった。戦いのなかで、シギントは米国を利する一方で、日本に対しては、第二次世界大戦のほかのどの交戦国よりも多くの損害を与えた。

第二次世界大戦の情報戦は、全当事者に成功と失敗を伴う競争であった。1942年以前は、インテリジェンスは枢軸国の大規模で優秀な部隊の価値を高めることにより、枢軸国に僅かに有利に働いた。一方、1942年以降、インテリジェンスと戦力のバランスは、同時かつ体系的に連合国に有利に働いた。その影響は、長期間にわたって一方的であった。インテリジェンスが枢軸国の敗北に寄与することはほとんどなかったが、連合国の勝利には大いに貢献した。

「ウルトラ」は、特にブレッチリー・パークが「エニグマ」装置などのドイツの暗号システムから入手したものなど、高度なコミントから得られた資料に対する連合国のコード名である。第二次世界大戦期間中、ウルトラは最良の情報源であったが、決して完璧ではなかった。ウルトラは敵から直接情報を手に入れていたが、内容が単純明快であることはほとんどなかった。ウルトラの価値は時期と戦域によって異なった。時間とともに、ウルトラはより多くの成功を収めるようになったが、その歴史は運命の逆転にあふれていた。連合国が敵の重要なメッセージを全て解読できたということは決してなく、その大半を解読できたということもなかった。ウルトラは、全てについて最良の情報源ということはなく、暗号解析の技術的な成果がそのまま戦場での成功につながることもなかった。アフリカ戦域では、作戦状況により、ウルトラが技術的に最も成熟した時期ではなく、最も未熟だった時期が最も有用であった。最も未熟だった時期は、戦力空間比が低く、双方の戦力も低かった。したがって、決定的な結果をもたらす勝利が可能であった。ウルトラが成熟した頃には、

3 Ken Kotani, *Japanese Intelligence in World War II*, (Osprey Press, 2009); John Ferris, "'Consistent with an Intention': The Far East Combined Bureau and the Outbreak of the Pacific War", *Intelligence and National Security*, 27/1, January 2012, pp. 5-26.

大規模で優秀な陸軍が、第一次世界大戦よりは流動的ではあったものの、第一次世界大戦のように、狭い前線で長期かつ高烈度の消耗戦によるこう着状態にあった。それでも、知識は強者の能力を高めることから、インテリジェンスは消耗戦のバランスを連合国有利に傾けた。主導権を握っているときは、枢軸国のインテリジェンスの弱点は重要ではなく、戦術的収集における強みが重要であった。守勢に回ると、強みは重要ではなくなり、弱点が危険となった。ドイツの戦力が低下すると、成功の可能性はエリート部隊を敵が攻撃する区域に展開できるかにかかっていた。そうすれば、足手まといとなる部隊と共に、突破を制止し、犠牲が大きく一方的な消耗戦に敵を追い込み、戦略的こう着状態に持ち込める可能性があった。この目標を達成するには、ドイツは敵の攻撃の時間と場所を推測しなければならなかったのだが、実際に推測することはなかった。それどころか、1942 年以降、ドイツは西側連合国から立て続けに虚を突かれる形となった。北アフリカ、シチリア、ノルマンディーに対する上陸作戦は、雷のようにドイツの弱点を突き、奇襲で前線を一変させた。これは、ドイツのインテリジェンスは能力が不足しており、指揮は英国に操作されていたからである。ウルトラが敵に損害を与えた形態としては、欺瞞が最も精確かつ破壊的であった。1943 年のシチリア侵攻前、1944 年のノルマンディー侵攻前に、英国は、ヒトラーをだまして連合国は別の場所を攻撃すると信じ込ませた。これが奏功し、侵攻前のドイツ軍展開を妨げ、部隊の 33% が誤った場所に展開されるようにした。欺瞞により、多くのドイツ軍部隊は、ノルマンディーの戦いに影響を及ぼすことができなかった。インテリジェンスと欺瞞は、これらの作戦における連合国の成功に欠かせなかった。ドイツのインテリジェンスは、ナチスの戦略上、成功を最も必要としていた正にその時に機能しなかったのである[4]。

太平洋戦争では、欧州よりも質の低いウルトラが、欧州よりも大きな勝利を可能にした。これは、戦場での状況が、インテリジェンスにより劇的な効果をもたらしたからである。太平洋戦争は、インテリジェンスが史上最も影響を与えた戦争であった。数百万平方マイルの空間に分散した小規模な部隊にとって、通信の中心は無線であった。捕虜や工作員の情報源としての有用性が通常よりも低かった一方で、シギント、レーダー、画像、ろ獲した文書は通常よりも有用性が高かった。これらの分野では日本の能力は低く、日本の敵国が優れていた。戦力空間比が低く、どちらの部隊も相手方に接触することはまれであり、配備は掩蔽されていた。主導権がそれほどの力を持つことはめったになかった。奇襲は扱いが困難であった。海軍・空軍部隊をある基地から別の基地へと再展開させるのには数週間

4 Ferris, *Enigma*, pp. 223-66; Ferris, J.R., "Intelligence", in J.R. Ferris and Ewan Mawdsley (eds), *The Cambridge History of the Second World War, Volume I, Fighting the War*, (Cambridge University Press, Cambridge, 2015), pp. 637-63; Stephen Budiansky, *Battle of Wits, The Complete Story of Codebreaking in World War II*, (Free Press, New York, 2000).

を要する可能性があり、新たな地域で大規模な部隊を維持するのに必要なインフラの構築や、海路・陸路で兵士を移動させるのには数か月を要することもあり得た。兵士2万人を粉砕し、航空機200機を破壊し、基地1か所を占領し、2個師団の裏をかくことで、地中海と同じ広さの戦域であるニューギニアでの作戦を一変させた。敵の弱点を標的にし、不意打ちを食らわせ、敵の意図を知りそれに付け込む能力は、特にそのような最も複雑な作戦や上陸攻撃においては、非常に高かった。こうした分野での失敗は、非常に大きな犠牲を伴った。ウルトラは、一連の戦略をどのように実施すべきか、どこから作戦を開始すべきか、どのように敵軍に誤りを犯させるべきか、そしてどのように敵軍の報復を防ぐかを示すことにより、米国の能力に「かみそり」を与えた。通信保全、インテリジェンス、画像、レーダー能力が低かったため、日本は奇襲や各個撃破を受けやすく、主導権を失いやすくなっていた。インテリジェンスは、1942年5-12月の戦闘に不可欠であったが、戦闘を通じて日本海軍は弱体化し、その勢いが食い止められた。インテリジェンスのおかげで、1942年8月 -44年2月の消耗戦において、米国は大きな勝利を収めた。それはガダルカナル占領に始まり、18か月にわたるソロモン諸島での作戦、最終的には小規模な航空機部隊や潜水艦部隊を広大な海域に点在する日本軍艦船に精確に誘導するという恐ろしい海上阻止作戦に発展した。1944年に、犠牲の少ない形で日本の防衛を破ったアイランド・ホッピング（飛び石）戦略が可能だったのは、専ら敵が最も弱点とするところを攻撃する方法を、インテリジェンスが明らかにしたからであった。1945年、九州における日本軍の戦力と、日本の戦う決意に関するウルトラを受け、米国は原子爆弾で戦争を終結させることを決断した。米国が太平洋戦争に勝利したのは、部隊や指揮官の質や資源の規模が要因ではあったが、インテリジェンスは、インテリジェンスがない場合に起き得た展開よりも、早期かつ損害が少ない形での勝利を可能にした。ここでも、1942年以降の戦争全般同様、インテリジェンスが強者の味方となったのである[5]。

冷戦期のシギント

シギントは、強者が一切戦闘をせずに済むようにすることにより、冷戦を大方形作った。人々のイメージでは、冷戦期のインテリジェンスは東西のスパイ間の争いが中心であり、そのなかでは国家保安委員会（KGB）が一人勝ちしていた。実際には、その争いの中心にあったのは軍事情報であり、シギントが最良の情報源であった。冷戦期の諜報活動の象徴

5 John Prados, *Combined Fleet Decoded, The Secret History of American Intelligence and the Japanese Navy in World War Two*, (Naval Institute Press, Annapolis, MD, 2001); Edward Drea, *MacArthur's Ultra, Codebreaking and the War Against Japan, 1942-1945*, (University Press of Kansas, 1991).

的な中心地であったベルリンは、スパイの戦場というよりも、西側の対ソ連のシギントの拠点として重要であった。この争いの中心地は、フィクションで重んじられるチェックポイント・チャーリーではなく、英国王立空軍（RAF）ガトー基地や、米仏の基地などの軍事施設であった。ガトーは、地上最大の通常戦力であったドイツ駐留ソ連軍の中心地であり、「シギントの金鉱、共産圏の軍事システムの中心をのぞく窓」にある、とりわけ音声通信の傍受によるシギント収集を行う上で理想的な場所であった[6]。この争いは、1946-92年におけるGCHQの主要任務であった。低級システムを忍耐強く徹底的に活用することで、GCHQ、国家安全保障局（NSA）と欧州におけるそのパートナーは、ソ連軍の意図と能力を見通していた。GCHQは、インテリジェンス面で「主敵」と互角に持ち込み、西側の勝利に貢献した[7]。

冷戦期の情報機関は、それまでで最も大規模で、最も洗練され、技術的に進んでいた。需要と供給はかつてない形で増加した。最も広範な形態の技術、最も狭義の兵器の性質、最も機密性の高い計画に関するインテリジェンスの価値が飛躍的に高まった。暗号学とコンピューターが互いを革命へとつなげるなか、シギントは工業化、機械化、数式化が進んだ。年々暗号解読のためのブルートフォース（総当たり攻撃）は強力になり、「のみ」は鋭くなった。かつてない形で、インテリジェンス同盟は、冷戦のあらゆる連合を結び付け、日常的に最も緊密な要素になった。特に「ファイブ・アイズ」である豪州、英国、カナダ、ニュージーランド、米国間の暗号をめぐる連携であるUKUSA協定はそうであった[8]。こうした同盟の特徴は、競争的協力と政治的緊張であった。ファイブ・アイズが欧州同盟国のシギント機関に技術や収集情報を共有しようとしなかったことが主因となって、北大西洋条約機構（NATO）のインテリジェンス協調は不十分で、平時には無駄が多く、戦時にはぜい弱であった。その他の西側のシギント機関は、UKUSAや米国のジュニア・パートナーか、そうでなければ独自の同盟を形成した。UKUSAと、西側の第三国のより緩やかな関係は、東側の機関と比べれば平等主義的であったが、これらの機関の職員は、自国の他部局との連携よりも、機関間同士の連携の方が緊密であった。各パートナーは、共有プールを強

6 Tom Johnson, *American Cryptology during the Cold War,1945-1989, Book One, The Struggle for Centralization, 1945-1960*, p. 118, (Center for Cryptologic History, Fort Meade, MD, 1995).

7 Johnson., op. cit., and Volumes Two to Four; Ferris, *Enigma*, pp. 502-51; Matthew Aid, *Secret Sentry, The Untold History of the National Security Agency*, (Bloomsbury, London, 2010); Richard Aldrich, *GCHQ, The uncensored story of the Britain's most secret intelligence agency*, (Harper Press, London, 2010); Stephen Budiansky, *Code Warriors, NSA's Codebreakers and the Secret Intelligence War Against the Soviet Union*, (Vintage, New York, 2017).

8 Ferris, *Enigma*, pp. 324-89; Michael Smith, *The Real Special Relationship, The True Story of How the British and U.S. Secret Services Work Together*, (Simon & Schuster, New York, 2022).

化し、取引材料を得るための能力を構築した。これらの連合において優越的なパートナーは、同盟国よりも強力であったが、英国や東ドイツなど、後者のなかで最も優れていた国々は、質の面で劣ることはなく、ノルウェーやハンガリーなどの国々のシギント機関は、1939年以前のどの時期よりも大規模であった。イスラエルは世界有数の情報・シギント機関を創設した。インドやイラクなどの国々の機関は、地域競争には有効であった。

シギントは、冷戦期における秘密情報としては圧倒的に主流であった。シギントに関して分かっていることは限定的であるが、一部のことは分かっており、ほかのことは分からない、ということは理解している[9]。したがって、既知の事実を保守的に分析してみても、外交暗号解析の規模の大きさが浮き彫りになる。1945年以降の主要な暗号システムは、適切に使用し、かつ物理的に侵入されていなければ、エニグマのように、解読は不可能なはずであった。しかし、暗号ハードウェアやソフトウェアを秘密裏に複製するといった「不法侵入」や、電子機器からの漏えいの傍受にはぜい弱であった。多くの国々は、特に利用者のあずかり知らぬところでシギント担当官が利用できるようなバックドアを組み込んでいたため、暗号解析で解読できるシステムを使用していた[10]。コミントは、電子的漏出や暗号化されていないトラフィック、特に大量の公用・私用電話のトラフィックを傍受するなどの付随的スキルにより入手していた。米国が自らの手の届くあらゆる外国公館の暗号室を盗聴していたように、KGBは在モスクワの全大使館を盗聴していた。大使館は、外国の首都においてマイクロ波と電話のトラフィックを傍受する拠点であった。

この努力は実を結んだ。冷戦期のどの時点においても、UKUSAは世界の大半の国々による多くの重要なメッセージを解読した。しかし、スパイがシギントに勝ったことで、主敵に対する成功は限定的であった。1946-48年、米国はソ連の情報トラフィックに対する攻撃により、当時のソ連のスパイの巨大ネットワークに侵入したが、英国の裏切り者であるキム・フィルビーによって、そのアクセスは断たれた。一方、米国の裏切り者であるウィリアム・ワイスバンドは、英国の暗号解析官がソ連の暗号装置に対して展開していた第二のウルトラを破綻させた。UKUSAがワルシャワ条約機構の最高軍事暗号システムを解読できたことはめったになかったが、中程度までの軍事暗号システムの一部の解読には成功し、時には暗号化されていない重要なトラフィックの一部を傍受することができた。1945-60年、UKUSAは

9 GCHQから許可を受けた歴史家として、2015-20年の間、筆者は今日も秘密指定を受けている資料を閲覧する権限を得たが、本稿はそうした資料の影響は受けていない。本稿は公開資料のみを参照している。非公式の資料を引用しているからといって、現在も秘密指定を受けている資料がその結論を裏付けているということではなく、公知の事実に基づき、その根拠と議論について筆者が妥当と判断しているということにすぎない。

10 Greg Miller, "'The Intelligence Coup of the Century': For decades, the CIA read the encrypted communications of allies and adversaries", *The Washington Post*, 11.2.2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

ソ連機関のメッセージを約1.5億件傍受した。これらのメッセージは平文だったが、特に経済問題については貴重な情報が含まれていた[11]。UKUSAは、欧州や海上で、平文の軍事トラフィックを伝送するソ連の電信を頻繁に盗聴し、二次的な問題に関する資料を大量に得た。UKUSAは、ソ連の音声通信暗号化システムの欠陥を利用していたが、実は一部の中・高レベル軍事回線を含む多くのチャンネルに対応できていなかった[12]。エリント（電子情報）とトラフィック分析中心のシギントは、引き続き西側にとってソ連のシステムに関する最良の情報源であった。この問題は依然秘密に包まれているが、ソ連のシギントは恐るべきものであった。それまでと変わらず、純粋な暗号解析では西側の競合国には恐らく及ばなかったものの、第一級の諜報活動が、とりわけ米国海軍（USN）の暗号システムを解読することによって、シギントを支援した。1950年代、恐らく盗聴や電子的漏出の傍受を通じて、在モスクワ米国大使館を含め、ソ連は世界の外交トラフィックの半分を解読していた[13]。

1945年以降、最も優れた暗号システムが解読されたことはほとんどなかったが、引き続き諜報活動にはぜい弱であったため、諜報活動は暗号システムに対する最大の武器となった。相手方は、海底ケーブル、音声無線、マイクロ波や携帯電話など、国内通信で保全度が相対的に低いシステムで伝送される重要なトラフィックを傍受した。コミントから得られる外交情報は以前より増加したが、主要国の主要システムから得られる頻度は減少した。強国同士が相手方を打ち負かすようなことはあり得たとしても、実際に起きることはなかった。フランスや日本の暗号はぜい弱だった一方で、1970年代後半から1980年代前半にかけて、米国のコミントはソ連の一部の高度なシステムに侵入した。恐らく他の事例も今後明らかになるだろう。それでも、防御形態が強化されたことから、戦間期と比べて、大国間の情報源としてのコミントの効果は低下していた。

外交コミントには主に2つの形態が存在した。1つ目は、強国による弱小国に対する攻撃である。こうして得た資料はそれ自体が有用である一方、暗号がぜい弱だが情報に通じた閣僚がいる二流国家では、不注意にもあらゆる大国の政策をほかの国々に明らかにしてしまう。2つ目の形態はより独特である。冷戦状態は安定していた。国家間のシギント競争は戦略的問題が中心であった。シギント機関の職員は、外交活動を行った相手、同盟国、競争関係にある問題、外交政策や経済の基本的問題に外交コミントの焦点を当てていた。そのような資料は、電話の傍受などの単純な手段で入手できることが多いが、大いなる分

11 Carol B. Davis, *Candle in the Dark, COMINT and Soviet Industrial Secrets, 1946-56*, (Center for Cryptologic History, Fort Meade, MD, 2017); Ferris, Enigma, pp. 522-25. Ferris, *Enigma*, pp. 525-49.

12 Ferris, *Enigma*, pp. 525-49.

13 Desmond Ball, *Soviet Signals Intelligence*, (ANU Strategic and Defence Studies Centre, Canberra Papers on Strategy and Defence, No 47, 1989); David Easter, “Nikita Khrushchev and the Compromise of Soviet Secret Intelligence Sources”, *Journal of Intelligence and Counter-Intelligence History*, 35/3, April 2021.

断の向こう側から高度な外交インテリジェンスを入手するよりは簡単に入手できた。コミントが利用者にとって最も役に立ったのは、恐らく通商問題をめぐる二国間・多国間交渉に関する競合国（通常は友好国や中立国）の交渉上の立場を明らかにしたことだった。このような条件下で、外交暗号の解読が小さな競争関係を形成するとともに、そのような問題について最も責任があり、かつそうした問題について精通する大国による同盟管理が形成された。暗号解読の天秤が攻撃者側に劇的に傾いた、サイバー諜報活動の最初の10年も同様で、外交資料が交渉相手（同盟国や中立国）から収集され、貿易・経済問題に焦点が当てられた。貿易・経済問題では、各国に友人はおらず、競争相手しかいない。外交コミントに関する公表文書が少ないことは、少なくとも1980年代、UKUSAが日本の暗号システムを解読し、政治問題や、特に関税及び貿易に関する一般協定（GATT）などの経済問題に関するインテリジェンスを大量に入手していたことを示唆している。米国は一方で、日本政府にクリプトAG社の装置の使用を認めており、それを米国は解読していた。したがって、日本はイタリアやトルコと並んで、世界の同盟国のなかでも二流国に位置付けられていた[14]。

冷戦期の軍事競争のなかで、インテリジェンスの重点は、相手方に対するパワー・ポリティクスの世界的競争において、数百万人の兵士と数千発の核弾頭を支援することに置かれていた。この競争が熱い戦争に発展することはなかったが、いつ発展してもおかしくはなかった。米国、そしてその後を追う形でソ連は、競争相手の現在の核戦力を特定する技術的手段を開発したが、拡張計画や質的発展は常に不明なままであった。1939-45年にはコミント戦争があった。トラフィック分析と画像が冷戦を支配した。毎日、東西を問わず、数十万人の要員が、相手方の能力と意図を監視していた。彼らの主任務は「第三次世界大戦が今日起きることはない」と報告することであった。これはよい知らせであった。各機関は、核戦力に関する知識不足、不透明性と不安を払拭し、恐怖の均衡を安定化させた。二度の世界大戦同様、インテリジェンスが従来の作戦を形成した。冷戦期の戦略インテリジェンスについては、勝利は軍事分野にあった。核兵器とその効果については誤りようがなく、それらに関するインテリジェンスも十分であった。核による絶滅が確実であることにより、双方の最終的な推測が一致した。そのため、誰もがリスクを伴う戦略を最小化し、ゲームの大半において同じように行動せざるを得なかった。このような状況下では、通常戦力の価値は損なわれ、競争の中心は、西側にとって切り札である、経済成長と政治の安定に移った。インテリジェンスは、こうした競争の出現と終えんにおいて、さほど重要ではなかった。ソ連が冷戦に負けたのは、敵や自らについて把握していなかったからである。西側は自ら

14 Aldrich, *GCHQ*, pp. 445-6; Greg Miller, "Intelligence Coup", op. cit.

を把握し、敵についても多少は把握していたが、把握している事実も把握した方法もはっきりとは知らずに勝利したのだった。

シギントの技術

シギントは不確定要素の多いプロセスである。シギント担当者は、最先端の通信やデータ処理に取り組んでおり、どちらの分野のいかなる動向についても敏感である。変化がシギントの特徴ではあるが、革命が起きることはめったにない。1939-92年の期間は、シギントの第一期にあたり、無線通信、アナログ的な収集・処理、目視や電気機械データ処理装置による暗号解析が主役であった。1992年までは、コンピューターは、組織変革の装置というよりも、実質的には暗号解析の支援装置であった。しかし、その後は急速に組織変革の装置としての役割を果たすことになる。衛星による収集や衛星を標的にした収集が増加したように、自動化されたシステムを通じて、計算能力は着実に向上した。エニグマを粉砕するために利用された部屋一面に広がるデータ処理装置は消え去り、別の標的に対応するための別のシステムが立ち上がった。1992年まで、GCHQ は様々な装置、アプローチや体制を利用しており、これは1945年、あるいは1918年の英国のシギントを特徴付けるものであった。オペレーターのチームは依然として音声、短波（HF）、超短波（VHF）のモールス無線を傍受していた。データ処理はカード索引やパンチカード、タイプ課や通信センターで勤務するチームに頼っていた。GCHQ は情報を生み出す装置であったが、蒸気の代わりに紙の流れで稼働していた。GCHQ の職員は圧倒的に、熟練の職人技を必要とする傍受、データ処理、原始的な紙の複写、再複写と移動という労働集約型の作業に従事していた[15]。

通信と傍受の手段は常に変化した。収集拠点は大量にあり、常設のものもあれば、航空機や潜水艦など、移動プラットフォームによるものもあった。耳、手、テープレコーダーで収集した音声は、重要度においてテキストに匹敵した。かつて通信の主流であった海洋ケーブルによる電信は衰退した。2000年頃、海底光ファイバーケーブルがその地位を回復した。モールス信号はなくなるだろうという予測が立てられていたが、HF と VHF は軍事信号の主流であった。「アンテナ・ファーム」（傍受に適した場所に集中的に設置されたアンテナ群）が、そのような通信を最も収集した。これらの通信は、周波数を複雑に変更することで保護されていた。かつてないほど高度な傍受・データ処理システムだけが、衛星からの膨大なトラフィックを処理することができた。1915-45年の英国と比較すると、シギン

15 Ferris, *Enigma*, pp. 480-500.

トの収集量はかつてないほど増加したが、全体の割合からいえば大きく減少した。任意の時期に最良の資料を伝達するチャンネルを把握することの重要性は爆発的に高まり、より多くの要員が割かれた。衛星上のトラフィックについては、モールス信号、キーワードや電話番号に関するメッセージのタイミングや周波数を学習することで、単に傍受能力を高めるよりも、収集量を増やすことができるようになった。

傍受の英雄時代には、ヘッドフォンを装着したオペレーターが、扱いにくい装置に前屈みになって、変動する周波数を追跡し、鉛筆でメッセージを殴り書きしていた。オペレーターが侵入したネットワークに関する知識により、個人のスキルと自律性は依然高かった。次第に、技術的・組織的発展が労働環境を変えていった。新機材により周波数ずれがなくなり、高周波帯の傍受が改善された。オペレーターはそれまでよりも多くの機材を管理し、より多くの周波数帯を監視するようになった。引き続き職人技は非常に重要であったが、改良された傍受装置、チューニング補助装置、マイクロコンピューター、テープレコーダーなどの工業化を通じて、傍受量が増大した。1974年までに、初の完全コンピューター管理による通信所が衛星通信の収集を扱うようになった。この通信所は、人間と事務机ではなく、アンテナと機械を中心に設計され、コンピューターの数が運営要員の人数を上回っていた[16]。

全ての信号が言葉を伝達しているわけではない。電子的放射による非通信信号を分析するエリントは、シギントの最初期の形態の1つであり、日本海海戦で初めて活用された。1940-45年には、エリントはレーダーなどの電子機器からの放射を収集・分析した。エリントは、戦術航空情報と電子戦（EW）の中心となった。1945年以降、エリントはシギントと電子戦、そして軍隊に不可欠となった。エリントは、空軍・海軍に戦術情報と状況把握を提供し、電子戦を可能にする一方で、シギント担当官の運用評価を大幅に改善した[17]。

冷戦中に、コミント、エリントとトラフィック分析が融合され、シギントは国家情報の中核となった。シギント担当官は、圧倒的な量の資料を提供したが、これらの資料は様々な分析を必要とした。こうした分析は常に技術的で、通常、多くの費用がかかるものであった。ワルシャワ条約機構を対象にした業務は、たとえ高度なコミントが機能しなくとも、複数の低度のシステムが合わさると有用なインテリジェンスを生み出すときは、フュージョン（情報の融合）を活用した。これは一回きりの例外ではなく、シギント全体の特徴であった。フュージョンにより、産業規模の収集、評価、報告が必要になった。トラフィック分析の1つ1つが、ウルトラのメッセージとほぼ同じ程度の関心を集め、作成者と利用者のなかで分析要

16 Ferris, *Enigma*, pp. 483-8.

17 Alfred Price, *The History of US Electronic Warfare*, Volumes One (Association of Old Crows, Westford, MA, 1984), Two (*The Renaissance Years, 1946 to 1968*) (1989) and Three, *Rolling Thunder Through the Allied Forces, 1964 to 2000* (2000).

員の増員が必要になった。フュージョンは、ウルトラには及ばないものの、目的にはかなったプロダクトを作成するために、ウルトラと同規模の人的資源を必要とした。毎日、数万人のオペレーターが、自分の家族のように見知った通信ネットワークを監視し、変化や危険の兆候がないか確認した。大規模なソ連の作戦に関するトラフィック分析報告は、冷戦中の軍事情報のなかでも指折りのものであり、ワルシャワ条約機構軍の戦闘計画を明らかにするものであったが、1年半もの作業、数千時間もの分析の末、文字がぎっしりとタイプされた200ページにも及ぶプロダクトになることもあった。他の手段や機関では、この目的を達成することはできなかった[18]。正確な評価は、断片情報からデータセットを生成したり、単語が複数形なのか単数形なのかを検討したりするなど、大量の細部に関する骨の折れる分析と比較にかかっていた。

シギントの第二期

1945-89年の間、シギント担当官は2種類の通信ターゲットを攻撃していた。主として、専門要員と暗号で保護された軍事無線網と、もう1つは電信、マイクロ波、衛星などの民間通信システム上の（大半は国家に関するものであるが、時に外国人に関する）少量のトラフィックであった。その後、冷戦の終結と技術の変化により、コンピューター、インターネット、デジタル化された収集・分析の活用を特徴とする、シギントの第二期の幕開けとなった。HF・VHF無線や、それらを収集していた拠点は、通信とシギントにとって重要度が低くなったが、通常兵力（特に航空機や軍艦）が交戦するときはその価値が高まった。衛星、地上・海洋ケーブルが、国家・民間通信やシギントの主流となった。外交官、スパイ、テロリストなどの標的は、独自の通信システムの利用をやめ、民間システムを利用するようになった。自国民を含む民間人のトラフィックに触れることなく標的のトラフィックを傍受することはできなくなった。これは、メッセージの外形的特徴を確認しなければその送信元と送信先が特定できないためである。民間システムも変化を遂げた。情報通信はデジタル化され、インターネットに融合した。インターネット上にいる人は誰でも、インターネット上にいる全員とつながっている。インターネットの一般的な特徴は、開示と監視が、セキュリティやプライバシーより優先されるということである。電子メールは音声・文字メッセージを伝送した。携帯無線機器により、傍受の対象となる私的通信の量が増加した。無差別に国境を越える信号を通じて、オンラインや無線電話により伝送される通信は、インターネットに接続するあらゆるコンピューターに保管されているあらゆるデータに接続しており、同時に

18 Ferris, *Enigma*, pp. 543-5.

全ての来訪者による傍受を受けやすい。資料は電子と同じくらい容易に複製が可能であるが、検索と分析は引き続き不満がつのる作業であった。

国境を越える通信の特徴の変化は、自由主義国家による国内外での自国民のトラフィックや、自国の空間を通過する外国のメッセージを傍受する方法に影響を与えた。アナログ時代には、弁護士やシギント担当官が国内で発信されたトラフィックと国外で発信されたもの、違法な傍受と合法的な傍受を区別することができた。法律により、国内での傍受は制限されていたが、海外での傍受は制限されていなかった。デジタル時代には、国内のトラフィックが海外に移動し、外国のメッセージが自国を通過する。東京にあるオフィス間のメッセージが北京を経由する可能性もあれば、モスクワとサンクトペテルブルクにあるロシア情報機関間のトラフィックがロンドンを経由する可能性もある。外国の標的に対する攻撃は、通信が自国内を通過する際に行うのが最善かもしれないが、これは従来の法律の概念に挑戦するものである。合法的に容認される海外での傍受を通じて国内のトラフィックが取得されることは避けられない。第一、インターネット・トラフィックの大量収集においては、確実に自国民が含まれる。大量収集をしないということは、コミントを断念するということであるが、競合国がそうすることはないだろう。しかし、傍受場所が国内であろうと海外であろうと、そのような資料の分析においては、令状なく自国民の電子メールの封筒にあたるメタデータに触れざるを得ない。こうした手続きは合法的ではあるが、不快に感じられる。

インターネットは、無秩序な国際秩序の台頭を可能にした。「サイバー空間」はメタファー、領域や場所ではなく、多くの物事の一部であり、多くの物事の間の接点の一部である。すなわち、通信と情報の共有地（コモンズ）である。市場や海洋などほかの共有地同様、国家か否かを問わず、多くのプレイヤーの間の争いが、国家主体と非国家主体との間の重複する競争における慣行を規定する。こうした慣行は条件、利害、能力、時間の変化とともに変わるものであり、常に争点になっている。サイバーをめぐって浮上したこうした慣行は、これまでに共有地にあったのと同じぐらい多くのアクターや利害が関与していた。国家にとってはインテリジェンスとセキュリティが、個人にとってはプライバシーと監視であった。こうした展開が、信号の傍受や伝送を緩和し、国家と社会、対内関係と対外関係、戦争と平和、民生と軍事、安全と不安定、国家主体と非国家主体との間の確立した境界を解体した。シギント機関が国内で傍受したトラフィックと国外で傍受したトラフィックを区別できるようになると、自由主義国家は市民的自由と暗号解析を両立できるようになった。国内外のサーバー間のメッセージが自動的に急増すると、この状態はもはや正しくはなくなり、シギント機関は、外国に対するのと同様、これまでにないほど私人のメールを解読できる能力を備えるようになった。史上初めて、非国家主体が各国政府と同じコミント技術を使用し、外国や人々に対して用いるようになった。市民は、同じ市民や、外国政府、企業、犯罪者

からの攻撃という脅威にさらされるようになった。個人はほかのどの共有地よりも多くの略奪者や外国政府からの攻撃にさらされることになった。国家は、かつての平時とは比べものならないほど、外国の個人と企業の通信に攻撃し、こうした脅威から自国民を守るのは容易ではなくなった。

このサイバー・コモンズ上の英国の未開拓分野に要員を配置するため、GCHQ は新規に独自の大量収集形態を採用し、毎日世界中で起きている何十億もの通信事象から僅かなサンプルを収集し、このトラフィックを数日間分析した後に削除することで、ほかのサンプルを保有するスペースを確保した。世界中のインターネット・トラフィック全てをビリヤード台に例えると、GCHQ はビアマット大のメッセージを拭い取って、トラフィック分析でほんのピリオド大のデータについて処理を行う。これは、攻撃や解読の対象となった量よりはるかに少ない。こうした資料は全て、何らかの暗号化処理が行われている。低水準の初歩的なものもあれば、高水準の強固なものも多い。慣習として、トラフィック分析は、HF 無線受信機間の信号の外的特徴を評価することから、ネットワーク内のコンピューターのインターネット・プロトコル（IP）アドレス間のリンクの評価へと、体系的に変化した。こうした変化により、異なるスキルセットを備えたオペレーターが必要になったが、彼らは、通信の外形的特徴を分析する創造力と忍耐力を保持しており、そのため GCHQ は冷戦期にフュージョンで成功した。このトラフィック分析は、内容を解読するはるか前に潜在的脅威や問題を明らかにするため、大量のトラフィックを対象にした成功の主要部分を成していた。暗号解析は添え物にすぎなかった。処理の第一段階では、IP アドレスのメタデータを匿名化し、個人に関する詳細をすべてそぎ落とすことでシギントを簡略化するとともに、英国民が関与している可能性のある通信を標的にする GCHQ の法的立場を強化した。トラフィック分析では、どの IP アドレスが既に不審な IP アドレスと通信を行っているかを特定し、それによりさらなる不審者を特定する。暗号解析は、不審なアドレスからのメッセージのみを攻撃の対象としている。これらのアドレスが、UKUSA 以外のアドレスから発信された非ファイブ・アイズ国市民のアドレスと関係があった場合は、攻撃の決定は純粋に技術的なものであり、分析官や暗号解析官が決定を行う。ファイブ・アイズ国市民や場所、アドレスが関わるときは、メッセージの内容に対する攻撃を正当化するために必要な令状が必要になる。

イアン・ロバン GCHQ 長官が2013年に述べたように、「インターネットを広大な干し草畑とするなら、我々がしようとしていることは、入ることが可能であり、かつ我々が関心を持ち、我々の任務に資する可能性のある針や針の破片を含んでいるという点で見返りの良い可能性がある干し草畑の一部から干し草を回収することである。そうした干し草の山を集めても、これは畑全体の干し草の山ではなく、その畑のごく一部から回収した干し草の

山なのだが、この干し草の山のなかに、英国国民だけでなく、外国人を含めた無害な人々による無害な通信である多くの干し草が含まれているということを我々は重々承知している。したがって、そのデータに対するクエリーを設計して針を引き抜き、言ってみれば、周囲の干し草に踏み込まないようにしている。非常に具体的な法的基準があり、要件が満たされた場合のみ、通信の内容を見ることができる。それが事実だ。我々は無害な電子メールや電話を詮索することは望んでいない（中略）。私がその干し草の山を持っていたら、針と針の破片を探す。私のクエリーで引き抜くのはそうしたものである。周りの干し草は見ない。傍受されるかもしれないし、そのごく一部が英国市民を対象にしているかもしれないが、我々は具体的な許可がなければ見ることはない」[19]。

トラフィック分析、暗号解析、様々な言語によるテキストの解読と翻訳の対象となる僅かなリソースと比較して、圧倒的な数の潜在的標的の存在がこのプロセスを推し進めている。国家が引き続き主要な標的ではあるが、GCHQ は、テロリスト、反政府勢力、略奪者から英国市民や英国軍人の生命を守らなければならない。国内外の脅威は融合しており、GCHQ はそれまでめったにしなかったような形で、いわば外国に派遣された兵士というよりも英国国内の警察官のように活動するようになった。そのような行為は対外的脅威に対するGCHQ の法的権限を拡大解釈するものであるが、GCHQ がその業務を引き受けなければ、他に誰がその業務に必要な技術力を備えているというのだろうか。外国に拠点を置く工作員がグラスゴーの企業から秘密を窃取し、ブラッドフォードで英国国民にテロリズムを奨励し、全国の選挙を妨害することを、ほかにどのようにしてGCHQ が防げるというのだろうか。

GCHQ には、優先順位が高くないメッセージを攻撃する手段がない。毎日、数十億件ものメッセージのメタデータを評価する能力はあるが、恐らく取り扱うのはそのうち僅か数万件であり、解読するのは数百の新たな標的のトラフィックのごく一部であった。それでも後者は多くの成功を可能にした。GCHQ は、膨大な量のトラフィックからサンプルを抽出する効率的な手段を考案した。それは、トラフィックを確保し、分析し、必要に応じて保持する。そして、データベースをフラッシュして、このプロセスを繰り返す、というものである。後に記されるように、「GCHQ は、大量の能力を活用して大規模な形でインターネットにアクセスし、外科手術のような極めて高い精度で詳細に分析している。インテリジェンスの断片を引き出し（中略）、ジグソーパズルのように組み合わせることで」、GCHQ は「新たな脅威を発見」し、「現在の標的の計画と意図に関する独自のインテリジェンス」を提供し、「最も抜け目ない相手からのサイバー攻撃から英国を守り、インターネットの広大な泥沼で彼ら

19 “Intelligence and Security Committee of Parliament, Uncorrected Transcript of Evidence”, 7.11.2013, http://isc.independent.gov.uk/public-evidence/7november2013

を追い詰める」ことができた[20]。

GCHQ とサイバーセキュリティ

サイバー・コモンズの治安を維持する必要性が高まるにつれて、シギント担当官にとって組織的問題が生じた。サイバー犯罪が大企業や、英国のように大規模な金融セクターを抱える国々を危険にさらすようになった。各国は、軍組織や内部組織との新たな関係に直面するなか、シギントと通信秘密保全を組織化しようと苦慮した。デジタルの手段と物理的手段が融合するサイバー戦争において、攻勢を指揮すべきなのはシギント担当官か、それとも兵士か。サイバー犯罪に対処すべきなのはシギント担当官か、それとも警察官か。こうした問題は、組織と法律に関する複雑な問題を提起した。場所を問わず、各国の内部構造が解答につながる。イスラエルやシンガポールなど、一部の中小国は、英米より何年も前からサイバーセキュリティでの連携を行っており、多数の機関が、こうした問題のなかでも、より大規模かつより複雑な問題に対処している。

米国やイスラエルの水準に届いていなかった2007年から10年以上が経過し、様々な出来事が重なったことで、英国は一貫したサイバーセキュリティ政策を推進することになった。政治家は、GCHQ や他省庁からの助言ではなく、自身の観察により、サイバーセキュリティは重大な問題であり、解決策を必要としていると認識するようになった。常に互いの成果を覆すのではなく、超党派でこの問題に対処した。ゴードン・ブラウン首相は、サイバーセキュリティ戦略を策定した。戦略では、以下のような刺激的な文言が記載されている。「19世紀に国家の安全と繁栄のために海洋を確保しなければならなかったように、20世紀に空域を確保しなければならなかったように、21世紀には、サイバー空間における優位を確保しなければならない」。そして、国家主体と民間主体の協調の必要性などの基本原則が記載された。しかし、実際の変化はほとんどなかった。中央の小規模なユニットが、サイバー・コモンズでの動向を監視し、GCHQ の別のユニットが脅威に対応した。GCHQ は密かに企業に対しサイバーセキュリティに関する助言を行った。15の省庁は、依然として共有地のなかで好き放題に活動していた[21]。

2010-15年の保守党・自由民主党連立政権は、ブラウン首相の成果を足掛かりとした。

20 David Anderson, Q.C., Report of the Bulk Powers Review, CM 9326, 8.2016, pp. 152-6, 159-62, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

21 Cabinet Office, *Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space*, (CM 7642, 25.6.2009.

デイビッド・キャメロン首相などの主要閣僚は、サイバーセキュリティを国家の優先事項とした。ロバート・ハニガン GCHQ 長官が記したように、閣僚たちは、英国を「『オンラインで生活し、事業を行うのに一番安全な場所』」にしようとしていた。「無論、これは相対的な野心であり、英国が100% 安全になり得るということではない。サイバー犯罪の対象が他の場所のより簡単な標的に移る程度まで守りを強化することができるという主要な評価に基づいている。斜に構えているように聞こえるかもしれないが、ベースラインを国際的に上げていくことで、全ての経済がより困難な標的になり、他者に対して一層技能を向上させるよう促すことができる。長期的な方策として、強固な強靱性とセキュリティは、英国企業にとって市場の差別化要因となり、対内投資家にとって魅力的に映る」[22]。サイバーセキュリティは、厳格な国家安全保障戦略のなかで、英国が直面する4つの「第一級の脅威」のなかで主要な優先事項となった。同戦略は、多くの聖域にメスを入れている[23]。政府は、省庁間や民間企業との協調など、政策と行動の戦略的な橋渡しの成功に関する明確な基準を設定した。また、4年間で6.5億ポンドの計画が、サイバーセキュリティの予算に充てられた[24]。GCHQ はその予算の約60% を獲得し、「最も高度な国民国家による攻撃」に対応する責任を負った。内閣府所管の公開組織である CERT が、企業に対する大半の攻撃に対応するようになった[25]。

GCHQ の歴代長官は、危険が存在し、解決されなければならないことを認識し、報奨金を提供していたが、サイバーセキュリティの専門的側面については把握しておらず、部下に対応させていた。こうした目標を達成するために、サイバーセキュリティに関する新たな体制を構築した。GCHQ での経験はないが、インテリジェンスを含め、英国政府での業務経験が豊富な当局者であるキアラン・マーティンが、サイバーセキュリティと通信保全を監督することになった。マーティンは、GCHQ の通信保全部署内の急進的な近代化推進者と協力してサイバーセキュリティに対応し、そこで自身のアイデアを追求するとともに、米国やイスラエルのモデルを研究した。2011-15年にかけて、GCHQ は政府機関や企業と緊密に協力し、サイバー脅威を評価する部署を設置した。ハニガンが記したように、サイバー・コモンズの脅威とリスクの評価は「特に困難である。これは、比較的新たな分野であるからだけではなく、他の情報源の評価だけでなく詳細な技術的理解を必要とするからである

22 Robert Hannigan, *Organising a Government for Cyber, The Creation of the UK's National Cyber Security Centre*, RUSI Occasional Paper, February 2019, pp. 7-10.

23 *Securing Britain in an Age of Uncertainty, The Strategic Defence and Security Review*, CM 7948, October 2010, pp. 47-9.

24 Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011.

25 Hannigan, *Organising*, p. 14.

（中略）。閣僚たちにテロの脅威やテロ事件の深刻度を評価する枠組みがあっても、サイバー脅威を評価する枠組みはなかった。インターネット上では、あらゆる数字が大きいことから数字が常に大きく、何が100% なのかは誰も分からない。インターネットのデータは測定が難しく、静的ではない。由緒ある英国合同情報委員会（JIC）など、従来の評価機関は、有用な評価を実施するどころか、他機関が行った評価を後から批判するにふさわしい技術的スキルを入手できていなかった」。さらに、「誰もふさわしい専門家は誰かという明白な問いを提起しなかったため」政策がつまずいた。「特に英国の公務員は、経験の長さや豊富さよりもゼネラリストを優遇する傾向があるため、創造的で技術的な助言を提供し、あるいは他者による提案を実際に評価できる人材が純粋にいなかった」[26]。こうした批判の一部は、当時の GCHQ にも当てはまる。

各機関が企業に矛盾する助言を行い、企業側は負わされた負担に対応できなかったため、こうした成功は霧散してしまった。GCHQ はインテリジェンスを提供し、サイバー・コモンズで敵と戦ったが、企業は基本的に援助ではなく助言を受け取るだけで、共同歩調をとらせることができなかった。企業の防御に関する国の方針は混乱していた。ハッキング攻撃は高度になり、時には外国シギント機関との関連もあった。イングランド銀行は、こうした混乱が英国経済に損害を与え、セキュリティを弱体化させ、サイバー犯罪者を引きつけたと警鐘を鳴らした。協調に基づく国の政策は限界を迎えており、リーダーシップが必要であった。2015 年の選挙後、保守党政権は、単一のサイバーセキュリティに関するパブリックセンターの指導を受け、GCHQ の指揮下にある、国家戦略を必要としていた。キャメロン首相はハニガン長官に対し、「サイバーインシデントが発生すると、多くの省庁の代表が席に着いたが、質問のほとんどは GCHQ に集中していた」と語った。ジョージ・オズボーン財務大臣は、GCHQ は「世界最高に匹敵する機関として知られているのは当然だ（中略）。英国政府にとって深い専門知識の拠点であり、インターネットや情報保全の方法に関しては、ほかに類を見ないほど理解している」[27]。

他の省庁はサイバーセキュリティに関する権限がなくなることに抵抗した。抵抗は、保安局（MI5）が権限を手放し、行き詰まりを打開するまで続いた。各種サイバー犯罪への対応を担当する法執行機関だけが独立していたが、それでも GCHQ と緊密に協力することになった。GCHQ の職員の多くは、世間に知れ渡ることやサイバーセキュリティを担当することを好ましく思っていなかった。上級閣外大臣たちがこうした懸念を克服し、責任を「GCHQ の一機関である国家サイバーセキュリティセンター（NCSC）」に割り当てた。

26 Ibid., pp. 10, 39.

27 Ibid., pp. 14.

NCSCには独自の名称と組織が与えられた。マーティンがNCSCの初代センター長となり、イアン・レヴィがテクニカル・ディレクター（本人によれば、政府内の「最高サイバーセキュリティおたく責任者」）に就任した[28]。NCSCの幹部5人が宣誓し、公の場での発言や名前の公表ができる。5人はGCHQの他部署で公にできる人数よりも多い。2019年春までに、NCSCの職員は740人となり、GCHQの総職員数の10%に達した。NCSCの職員は、チェルトナムのGCHQ本部「ドーナツ」では、サイバー諜報活動とシギントの世界的リーダーたちと共に働いているほか、ロンドンの事務所では民間人と共に働いている。NCSCは政府保安区域内にあり、閣僚にも近い。緊急事態の際には、NCSCとGCHQが各省庁にサイバー脅威に関する知識をリアルタイムで提供し、可能な場合は、脅威が出現し次第排除する。NCSCは、公のサイバーセキュリティ・コミュニティーと協力する部門と、秘密機関と協力する部門の2つの部門から成る。NCSCは、ブレッチリー・パーク同様多くの要素からなり、自由に行動していた。NCSCは、企業のサイバーセキュリティ監査官、監察目的のために民間リソースを動員する組織、デジタル面で心を痛めた人々にとっての「人生相談の回答者」、英国の社会・教育に変化をもたらす伝道者となった。

NCSCが設立されると、速やかに英国のサイバーセキュリティ政策の指揮をとり、英国の社会・経済を保護しようとした。マーティン・センター長が述べたように、「我々はこのデジタル革命の成功を願っている。我々の任務は、組織的サイバー攻撃の3つの動機に対し、デジタル経済とデジタル政府をより安全にすることで、機能させることにある（中略）。1つは力である。これはデジタル時代に展開されている従来的な『ステイトクラフト』である。秘密を窃取したり、緊迫している時期に破壊的攻撃を行うための事前展開を行ったりすることで優位に立とうとしている国々やならず者が当てはまる。別の動機は金銭であり、知的財産の高度な窃取から、銀行口座からの現金の単純な窃取に至るまでのあらゆることである。もう1つがプロパガンダである」。敵性国家のなかには、「サイバー攻撃を利用してスパイ活動を行い、商業的・経済的に大きな優位を獲得し、破壊的攻撃のための事前展開を行う大国」が含まれる。中小国は、「サイバー空間内の比較的未発達な道路規則」を悪用して、「従来の軍事的手段では考えも及ばなかった方法で、自国より大国とみなす国々の鼻を明かそうとした」。犯罪者のなかには、「非協力的な国家の庇護や黙認を受けて活動しており、これはサイバーに関する新たな事態である。というのも、彼らは、我々に損害を与えるために我が国や同盟国の法域に足を踏み入れる必要がないため、法の裁きを受けさせることがはるかに困難だからである。こうした犯罪集団の一部は非常に高度である。我々は、

28 “Dr. Ian Levy”, Enigma 2017, https://www.usenix.org/conference/enigma2017/speaker-or-organizer/dr-ian-levy-national-cyber-security-centre-uk

どの攻撃目標が利益をもたらし、どの目標がもたらさないかについて詳細に情報を提供する非常に高度な MBA 級の管理情報システムを目撃してきた。しかし、我々が目撃する犯罪の大半が MBA 級なわけではなく、余りに多くの犯罪が行われてきた。世界の主要なテロ組織には、破壊的なサイバー攻撃を行う意図はあるが、能力がない。今、そうした状況が変わるかもしれない」。一方で、英国は「プロパガンダや過激化目的で世界中のテロリストがインターネットを恐ろしく悪用」することを抑制しなければならない[29]。

NCSC は GCHQ や軍のサイバー部隊と協力し、サイバー・コモンズへの定期的な襲撃などのハッカーや国民国家による攻撃に対処しているほか、脅威を発見し、無力化・迎撃している。NCSC はまた、より深い戦略を追求し、「サイバー空間で英国をより安全にし（中略）、インターネットに組み込まれたセキュリティ上の欠陥を修正し、サイバー犯罪者の経済方程式を変更し、攻撃者―防御者環境を変える」ことを目指した。政府は「ユーザーを責め、個人にセキュリティに関するあらゆる負担に耐えるよう期待する」ことから脱却した[30]。レヴィがその戦略――「能動的サイバー防衛」プログラムを策定し、この戦略は NCSC が公開している。同氏は、「サイバーセキュリティに関する産業から政府に対するよくある不満」について強調した。「一般的に、それは産業側の対策が不十分であり、さらなる措置を講じなければならないと政府から言われるが、そうした要求が現実にもたらす影響や、商業的含意について実際に理解していないことが多い、というものである。ところで、我々の戦略は、全国規模で実施してほしいあらゆる措置の実験台として政府を利用するというものである。我々が求める措置の有効性（あるいは非有効性）を証明し、誰かに何らかの措置の実施を求める前に、分別のある形で規模の拡大が可能であることを証明するために、我々がドッグフードを食べるというものである」。

NCSC は、監視ではなくセキュリティを基礎とすることで、インターネットの基本原則に挑戦した。NCSC は、民間企業と協力して、電子メールの基準や、インターネットプロバイダーがメッセージを転送するインフラプロトコルを改良するなど、インターネット内の技術的ぜい弱性に対処した。NCSC は、政府ウェブサイトと通信を行う英国の団体に対し、ソフトウェアのぜい弱性について警告することで、「英国のソフトウェア・エコシステムをより良いものにしよう」とした。レヴィはまた、「『お前たちは愚かすぎてこれを理解できない。助けられるのは私だけだ。この魔法のお守りを買えば問題ない』と基本的に言っている」ような

29 “A new Approach for cyber security in the UK”, 13.9.2016, https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

30 Hannigan, *Organising*, pp. 40-42.

売り口上を用いる企業を批判した。「それは中世の魔法だ。まさに中世の魔法だ」[31]。NCSCはまた、「悪を探して倒し」、英国の標的を攻撃したインターネット上のウェブサイトを無効にした。「我々は引き続き、GCHQだけができる方法で相手方の意欲をそぐために行動する」。この声明は「わざと遠回しな表現を用いている。こうした措置はいずれも発展する。成功するものもあれば、失敗するものもある。相手方が我々の防御に対応する間、我々は相手方に対応しなければならない。それがニューノーマル（新たな日常）となるだろう（中略）。今こそ翼のある忍者のサイバーモンキーに何ができるのかについて語るのをやめ、毎日のように市民にも企業にも同じように実害を及ぼしている大規模な問題に自動的に対抗する時だ」[32]。

大規模な不祥事が公になったにもかかわらず、こうした成功は起きた。2013年、NSAの契約職員兼システム管理者のエドワード・スノーデンが、UKUSAの仕組みに関する大量の記録を複製し、ジャーナリストや活動家に漏えいした。突如として、人々と技術専門家は、サイバー・コモンズにおける軍事化とコミントの現実に直面し、純粋に衝撃を受けた。当初、暴露は理解し難いものであった。メタデータ（時には単に収集し匿名化したメッセージの件数）に対するトラフィック分析の各事例が電子メールの解読を意味すると受け止められるようになると、人々はファイブ・アイズが実際よりもはるかに多くのメッセージを解読していると思い込み、「ピリオド」を「ビアマット」と、場合によっては「ビリヤード台」と混同するようになった。ガーディアン紙は、当局は「オーウェルの想像以上」の権限を得ていると報じた。人権団体「プライバシー・インターナショナル」は、「シュタージは東ドイツ人の3人に1人に関するファイルを保有していた」が、GCHQは「英国のほぼ全国民の通信を傍受し保管していた」と抗議した[33]。こうした暴露は誤っており、一方的で甘い認識に基づいていた。反対派は、そのようなことをするなど検討することもないという、紳士としての言葉に懸けて報道官が誓った、中国やロシアなどの「善良な」国家とは異なり、サイバー・コモンズでコミントを実施している西側諸国はほんの数か国であると想定した。反対派は、こうした慣行は専ら英米市民の生活を監視することを目的としており、戦争、テロ、サイバー犯罪や敵性国家の活動を無視していると考えた。シギントを批判する立場からは、優秀であるか否か、信念に基づいたものか敵意を抱いたものかを問わず、暴露を推進した。ビーヴァーブルック男爵による帝国自由貿易十字軍と同様、古典的な報道キャンペーンは販

31 Iain Thompson, 3.2.2017, “GCHQ cyber-chief slams security outfits peddling ‘medieval witchcraft’”, *The Register*, https://www.theregister.co.uk/2017/02/03/security_threat_solutions/

32 Ian Levy, Blog Post, 1.11.2016, “Active Cyber Defence—tackling cyber attacks on the UK, https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

33 “UK Debate Grows over ‘Orwellian’ NSA and GCHQ Surveillance”, The Guardian, 9.10.2013, https://www.theguardian.com/world/2013/oct/09/debate-grows-orwellian-nsa-technology

売部数拡大を目的としていた。インターネット・リバタリアンたちは、国家によるインテリジェンスや秘密を悪とみなしており、安全の追求により引き起こされた隷属からの自由を守ると主張した。こうした意見には一定の勢いもあったが、よりメロドラマ的要素が強かった。反対派は共有地での競争の問題や、敵の存在を無視しており、自分の国から攻撃を受けている人々のことのみを念頭に置き、外国政府に攻撃されたり、犯罪者に搾取されたりした人々のことを考慮していなかった。西側諸国では、ほとんどの人々は自国から攻撃を受けることはなかった。それより多くの人々が、外国政府や民間当事者から攻撃を受けていた。ビッグ・ブラザーの支援を必要としたり、求めたりする人よりも、ビッグ・ブラザーを恐れている人の方が少なかったかもしれない。

この危機は GCHQ に衝撃を与えた。どの資料が公表されるか把握しておらず、GCHQ の代表は当初、公の場で法的・技術的問題や、GCHQ がいかに英国人の生命を守ってきたかについて、明確に説明できなかった。しかし、GCHQ の記録と神話が GCHQ を救った。保守党・労働党の有力政治家は、GCHQ はその活動について適切に報告していたという点で一致していた。関連する技術的問題や、情報は常に小出しになっていたため、人々は混乱し、飽きるようになった。能力がある国はどこもシギントを実施している一方で、サイバー犯罪者やテロリストが英国民の情報搾取・攻撃を計画している証拠が間もなく表れた。シギントの敵は、立証できないことが明らかな発言や、大量収集がテロ攻撃を減らした事実はないなど、虚偽の発言をしたり、GCHQ が解読した英国市民のメッセージの件数を誇張したりして、強く出過ぎてしまった。議論は神話の様相を呈するようになった。反対派は、GCHQ はビッグ・ブラザー、あるいはサウロンであると当てこすった。人々はブレッチリー・パークの後継組織がオークであるとは容易には想像できなかった。英国の国民は、生存に関わる脅威を認識し、脅威に立ち向かう GCHQ をガンダルフとして、自身を助けが必要なホビットとしてみなすようになった。次第に、議論は情報に基づいて、公の場で行われるようになった。客観的な専門家によるバランスの取れた報道が、杞憂を払拭した。そうでなければ、英国のサイバーセキュリティは成功を収めることができなかっただろう。

NCSC のプログラムには、政府による検閲や監視の疑念を生じさせかねない多くの活動が関わっていた。NCSC は、「信頼性と透明性のある組織」としての評価を確立することでその危険に対処し、人々が NCSC による提案を断る方法を広報した。人々や、筋金入りの GCHQ の批判派でさえ、問題は重大で解決しなければならないと認識していた。彼らは、NCSC を秘密警察官というよりは、「巡回中のお巡りさん」のようにみなしていた。開放性により、シギント担当官は国民の自由を損なうのではなく、国民の安全のために努力しているという信頼を生んだ。NCSC の脅威警報、セキュリティ問題に関する週間・年間予測は、技術専門家、企業、個人や家庭向けに異なるバリエーションを提供しているが、

英国メディアにおいておなじみの存在となり、多くの視聴者に届くようになった。こうした資料は、GCHQ や JIC が冷戦期に公表した秘密報告書の公表版に相当する。NCSC は、一般の人々に対し、定期的に国家情報評価を提供する最初の組織となり、例えば、「ロシアが我が国の重要部門の一部に事前展開している証拠や、我々のネットワークからそれを排除する方法に関する企業向けの詳細な技術ガイダンス」を提供している[34]。これらの報告の大半は公開情報を基にしているが、一部は NCSC 自身の成果物である。昔ながらのサニタイズの慣行により、より秘匿性の高い情報源に基づく資料の拡散を防いでいることは疑いない。NCSC と GCHQ の双方が、国家を対象にした業務を含め、自らの業務についてこれまでよりもはるかに多くの資料を一般向けに公表していることもまた、シギントの第一期と第二期との違いの表れであった。

2022 年の日本とシギント

シギントは2022年の日本にとって主要な問題であり、多くの日本人が認識しているよりもはるかに重大な問題である。どの国においてもシギントは秘密に包まれているが、日本では特にそうである。日本ではシギント担当官が独立性と自律性を驚くほど重視しているが、それを政府が容認し、ほとんどの国民も異議を唱えない。以下の所見は、この問題に関する数少ない公刊資料を分析した結果に基づくものである。包括的ということはできないが、筆者としては内容が正確で有用であることを願っている。

日本はシギントにおける課題とその解決策の必要性に直面している。現代の日本のシギントは、ほかの先進諸国ではみられないほどに、他国のシギントに依存しているかもしれない。日本のシギントは、米国との協力と統合を通じて浮上した。米国はまた、同盟国のほとんど、場合によってはほかのどの同盟国に対してよりも、はるかに多く日本の国防政策を形成してきた。日本は、インテリジェンスを利用した政策の強化については成功も失敗もあり、通信保全については長らく平凡な実績を残してきた。日本はロシアと中国という2つの脅威に直面しており、両国ともインテリジェンスを強力な武器として扱っている。ロシアのヒューミント（人的インテリジェンス）は、外国の海軍の暗号解読に成果を挙げることで、シギント能力を低下させ、一定の情報優位を獲得した。日本はこうした脅威に留意しなければならず、主たる同盟国である米国もまた、通信保全、特に海軍の通信保全については、月並みな実績であることを日本は忘れてはならない。友好国、敵国、中立国を問わず、あらゆる大国が日本の外交トラフィックを攻撃する一方で、ロシアと中国は日本企業、社会や

34 *NCSC Annual Report 2018*, p. 10.

政治に対して、サイバー破壊活動やサイバー諜報活動を実施するだろう。日本は艦艇と航空機との間の衝突に適したシギントを整備し、古典的な収集・分析方法を「エアシー・バトル」とサイバー脅威に適用しなければならない。いずれの場合にも、悪魔は細部に宿ることになる。

日本はサイバーセキュリティを強化するための措置を講じてきた。2014-15年にかけて、内閣官房長官の下にサイバーセキュリティ戦略本部を設置したほか、内閣サイバーセキュリティセンターを設置した。2021年、日本は国家的な「サイバーセキュリティ戦略」を採択し、そのなかでは、ITとセキュリティを協調させるため、同盟国との関係や、国家機関、企業、国民との間の連携を重視している。これらは結構であるが、経験的に、そうした取組みは個々の国に合わせたものでなければならない。英国、イスラエル、シンガポール、米国はそれぞれ、この問題について独自の制度を通じて異なるアプローチを採っている。言葉や形だけではサイバーセキュリティは実現できない。こうした目的には、国家的、公共的リーダーシップ、国家と社会との間における新しく困難な形態の協調、シギントに関するさらなる開放性、シギント担当者の態度の変化を必要とする。例えば、英国によるサイバーセキュリティでの成功には、政府首脳の主導による10年間の努力、組織の抜本的改革を受け入れるGCHQの意思、国の全省庁の積極的関与、この課題に多くのリソースを投入するとともに、王立空軍や秘密情報部（MI6）と同様に、GCHQを公的執行機関にするという国家の決定を必要とした。日本はシギントを民間機関や国民に接触させないようにする傾向があり、またコミントや攻撃的サイバーにおける高度な能力が不足していることから、サイバーセキュリティの構築を制約するだろう。これらの目的を果たすために、中央政府は断固として主導性を発揮し、シギント担当官、一般の公務員、ビジネスマン、オピニオンリーダーが確実に協力するようにしなければならず、そのためには彼らの自発的な協力、国による透明性と人々からの信頼が必要である。筆者は、日本のサイバーセキュリティは、日本人が想像するよりもはるかにぜい弱なのではないかと懸念している。2022年においても、サイバーセキュリティ分野では、2007年の英国と大差ない。カナダのサイバーセキュリティが英国の教訓を得て改善したように、この問題について日本はシンガポールの経験に学べるかもしれない。

日本はまた、シギントと戦略の関係性を再検討してもよいかもしれない。最近の歴史に優れたモデルがある。「海洋戦略」は、冷戦中の西側のインテリジェンスのなかでも最も秘密主義的な要素が関与していた。1975年以降、ソ連海軍は弾道ミサイル搭載原子力潜水艦（SSBN）を世界各地に展開する取組みを、探知・破壊されるおそれがあることから断念し、その代わりに、攻撃型原子力潜水艦（SSN）やその他の部隊による防護が可能な白海に展開した。米国海軍と王立海軍は、これらの部隊、特にSSBNと交戦する準備を

進め、双方による秘密の争いが勃発した[35]。この争いには、多くの情報源が関与した。最も有名なのが「音響監視システム」であるSOSUSであり、これは世界各地の水中聴音機からなるシステムで、ソ連の潜水艦を探知した。そして最も秘密に包まれていたのがシギントである。冷戦を通じて、SSNは戦争に備えた訓練として、探知されずに敵部隊の付近を航行しようとした。こうしたSSNの一部にはシギント集団が乗船しており、ソ連の軍艦を追跡し、近距離で平文の音声を傍受し、探知・通信システムの技術的詳細や、あらゆる軍艦が発する機械やスクリューに特徴的な「音響シグネチャー」を入手した。SSNは敵を理解し、敵と戦うために情報を収集し、シギントを活用して哨戒の指針とした。シギントの活用が緩和されたのは、海洋戦略がファイブ・アイズのうちの三か国である英国、カナダ、米国と、ノルウェーを軸にしていたからである。三か国はあらゆるレベルのインテリジェンスの共有が可能であり、ノルウェーはNATOに加盟する第三国として最も信頼できるパートナーであり、シギントとは分離可能な収集分野である航空偵察を通じて任務に貢献しつつ、目的を果たすことが可能であった。SOSUSとシギントの能力により、ソ連海軍を大西洋のブルーウォーターから白海のグリーンウォーターに追い込み、白海で支援すら提供し、ソ連の決定を米国当局に明らかにすることで、海洋戦略自体に拍車をかけた。しかし、ソ連の諜報活動で多くの裏切り者がリクルートされた。特に、米国のウォーカー・ウィットワース家のスパイだけでなく、英国のジェフリー・プライム（そして一世代後の、カナダのジェフリー・ドリール）は、西側の海洋インテリジェンスとシギント、そして米国海軍の暗号システムについて漏えいした。もし冷戦が熱い戦争に発展したならば、ソ連を有利にしていただろう[36]。

---

35 John B. Hattendorf, *The Evolution of the U.S. Navy's Maritime Strategy, The Newport Papers, No 19*, (2004), https://digital-commons.usnwc.edu/newport-papers/35; John B. Hattendorf and Peter M. Swartz, (eds), *U.S. Naval Strategy in the 1980s: Selected Documents, The Newport Papers, 33*, https://digital-commons.usnwc.edu/newport-papers/21; Cote, Owen R. Jr, *The Third Battle, The Newport Papers, 16*, (2003), https://digital-commons.usnwc.edu/newport-papers/38

36 Aldrich, *GCHQ*, pp. 125-47; John Olav Birkeland, *Maritime airborne intelligence, surveillance and reconnaissance in the High North—The role of anti-submarine warfare—1945 to the present*, (Ph.D. diss., University of Glasgow, 2021); Marcus Faulkner, "Naval Intelligence and Innovation: A Historical Perspective", in Alessio Patalano and James A. Russell (eds), *Maritime Strategy and Naval Innovation, Technology, Bureaucracy, and the Problem of Change in the Age of Competition*, (Naval Institute Press, 2021), pp 90-106; Christopher Ford and David Rosenberg, *The Admiral's Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War*, (Naval Institute Press, Annapolis, MD, 2005); Christopher A. Ford and David Rosenberg, "The Naval Intelligence Underpinnings of Reagan's Maritime Strategy", *The Journal of Strategic Studies*, 28/2, 2005, pp. 379-409; Peter Hennessy and James Jinks, *The Silent Deep, The Royal Navy Submarine Service since 1945*, (Allen Lane, London, 2015); John Schindler, *A Dangerous Business: The USN and National Reconnaissance during the Cold War*, (Center for Cryptologic History, Fort Meade, MD, 2004); Susan Sontag and Christopher Drew, *Blind Man's Bluff: The Untold Story of Cold War Submarine Espionage*, (London, Arrow Books, 2000).

冷戦中の英国海軍による取組みは、相違もあるものの、今日の海上自衛隊の取組みと類似点がある。当時世界第三の海軍であった英国海軍は、ブルーウォーターでの対潜戦と艦隊運用に特化し、世界的な能力を備えていた。英国海軍は、特に海洋戦略において米国海軍と有機的に協力した。それにより、多くの重要な技術的発展を利用できるようになる一方で、英米が共にファイブ・アイズに加盟していたことで、情報交換が緩和された。敵は、数的には対等ではあるが、質的には英米に劣っていたソ連海軍であった。ソ連海軍は、沿岸以遠に戦力投射する上で並々ならぬ困難に直面していたが、それでも攻撃は困難であった。当時、米国海軍がソ連海軍を太平洋のブルーウォーターに進出するのを阻止する上で海上自衛隊が果たした役割はより小さく、防御的かつ従属的ではあるもの、非常に重要であった。海自の戦略は、ソ連の戦艦をアジア沿岸で足止めすることであり、そこではディーゼル電気潜水艦がブラウンウォーター、特に宗谷、津軽、対馬の各海峡に潜んで、太平洋に進出しようとするソ連部隊の位置を特定し、撃沈することで、同時に日本のシーレーンを守り、前方展開している米国海軍の空母戦闘群が、オホーツク海で身動きの取れないソ連部隊を攻撃できるようにしていた。日本の潜水艦は、ウラジオストク近海でソ連部隊を偵察し、海自部隊とシギントは米側のカウンターパートの下で協力関係にあった[37]。運用面での二国間関係のため、日本のシギントは、恐らくNATOのどの欧州加盟国によるファイブ・アイズとの協力よりも緊密な形で米国の機関と協力していた。しかし、米側が技術やトラフィックの交換に関する「交易条件」を統制しており、日本を基礎段階より向上させる支援をする必要性がほとんどなかった。米側は、日本の戦術的シギントやエリントの能力の恩恵を受けていたが、日本が高度なコミントや通信保全を構築する支援を得ることはなかった。日本のシギントは、日本の国益と同じぐらい米国の国益を追求していた。軍事標的に対するトラフィック分析やエリントについては成果を挙げており、恐らくフランスやドイツといったまずまずの二流プレイヤーに肩を並べるほどであったが、一流シギント大国が有する傍受、暗号解析、分析能力が完全に欠けていた。

日本は現在、大規模で先進的な航空部隊と、恐らく三番目か四番目に優れた海上部隊を保有している。日本はあらゆる種類の海上部隊の急激な変化、エアシー・バトルという形態における新たな海洋戦略の構想と、ロシア・中国という2つの国家に直面している。

37 Narushige Michishita, Peter M. Swartz and David F. Winkler, *Lessons of the Cold War in the Pacific: U.S. Maritime Strategy, Crisis Prevention and Japan's Role*, (Woodrow Wilson Center, Washington D.C., 2016); Alessio Patalano, "'The silent fight': submarine rearmament, and the origins of Japan's military engagement with the Cold War, 1955-76", *Cold War History*, 21/1, 2021, pp. 91-111. ; Alessio Patalano, "Shielding the 'Hot Gates': Submarine Warfare and Japanese Naval Strategy in the Cold War and Beyond (1976-2006)", *JSS*, 31/6, 12.2008, pp. 859-95; Alessio Patalano, "Japanese Naval Power", in Robert J. Pekkanen and Saadia M. Pekkanen (eds), *The Oxford Handbook of Japanese Politics*, (OUP, 2021).

ロシア・中国はともにグリーンウォーターへの進出が可能であり、太平洋のブルーウォーターに部隊を展開することを目指している。日本にはブルーウォーター能力があり、東シナ海からオホーツク海にかけてのブラウンウォーターやグリーンウォーターにおいて、中国・ロシアに対抗するコミットメントがある。こうした問題に対処するため、日本には、特にインテリジェンス分野において、冷戦期の英国海軍と同様の海洋能力が必要である。一方で、日本は時に「クアッド」と呼ばれる複数の友好国と共に活動している。クアッドの構成国のうち、米国と豪州の二国はファイブ・アイズに所属しており、事態に影響を及ぼし得る英国とカナダの二国も同様である。「クアッド」の構成国が第四の構成国であるインドに高度なシギントを交換する可能性は低い。このような状況では、日本は最高水準のシギントへのアクセスが容易に遮断される可能性があり、それは日本の国益だけでなく、より広範な利益を害する可能性がある。ちょうどファイブ・アイズがシギントや戦略に関して NATO の利益を損ねたのと同様である。冷戦期の英国の経験から示唆されるのは、日本の立場にある国は、米国からの信頼と、米国への影響力を築くことで、戦略の策定に影響を与え、作戦とインテリジェンスにおいて必要な支援を獲得しなければならない、ということである。日本が同盟国としての価値や、米国政府に対して必要な影響力を獲得するためには、シギント面でより多くの能力と独立性が必要である。

こうした問題に対してはチャンスもある。9.11同時多発テロ以降、先進国は軍隊への支出以上にシギントへの支出を増額してきた。これらの国々はいずれも、シギントを主要な問題、重要性が増しつつある問題として扱っている。日本はこうした分野において大半の先進国に遅れをとらずに進んでいるが、シギントの主要国には追いついていない。例えば、GCHQ は日本のシギント機関の6倍の人員を擁し、最も高度な形態のシギントにおいてはるかに優れた能力を有しており、世界中での英国の影響力に貢献している。一方、ファイブ・アイズは依然として独自の集団であるものの、第三国との技術やプロダクトの共有に関する従来の制限の一部を緩和してきた。日本にとって、シギント能力の拡大は、インテリジェンスを直接提供し、米国により多くの支援を提供させることによって、戦略における主体としてのより大きな役割を支える上で不可欠である。シギントを拡大する場合、高度な軍事標的だけでなく、敵国、中立国、友好国の外交システムも含めるべきである。ここでいう友好国には、シギントについて不満がないほど高度で、自助努力する国々を尊重する米国も含まれる。日本のシギントが強力になればなるほど、米国は日本のシギントとの協力を深める必要が高まり、日本は米国をテコで動かし、その決定や戦略に対する影響力を獲得できるようになる。強力なシギントは、日本の安全保障に不可欠なのである。