警察政策学会資料　第113号
令和２（２０２０）年１１月

テロ対策に見る我が国の課題
国民保護における避難
「クリプト社」とNSA（暗号攻略大作戦）

警察政策学会

テロ・安保問題研究部会

テロ対策に見る我が国の課題
国民保護における避難
「クリプト社」とNSA（暗号攻略大作戦）

本資料は、テロ・安全保障問題研究部会の最近の研究成果を取りまとめたものである。

令和2年10月　テロ・安保研究部会長　茂田忠良

テロ対策に見る我が国の課題～欧米諸国との対比において～

日本大学危機管理学部教授　茂田忠良

＜目次＞

初めに

１　本稿の由来と特徴

筆者は、2019 年 10 月、警察政策学会・テロ安保問題研究部会と中央大学日本比較法研究所共催「テロ対策に関する国際フォーラム」において、「日本のテロ対策の課題～欧米諸国との対比において～」と題して講演を行った。

しかしながら、時間の制約もあり、講演内容はかなり要約したものとせざるを得なかった。また、根拠となる出典・資料等についても提示していない。そこで、講演内容に大幅に加筆補充して、資料の出典も明示して、論述することとした。論述に当たっては、単に我が国のテロ対策それ自体の課題を述べるにとどまらず、その背景にある我が国の安全保障（Security）上の課題についても視野に入れた。

なお、我が国におけるテロ対策の課題については、松本光弘氏（現警察庁長官）が積極的に且つ広汎に論じている[1]。同氏は、欧米諸国、主として英独仏の治安機関の権限を解説した上で、「我が国治安当局に与えられた権限が世界の趨勢から時代錯誤的に取り残されている」[2]現状について問題提起をしている。本稿も、我が国当局の権限が世界標準に遠く及ばず国際テロ対策では全く不十分であるという点において、認識を同じくするものであるが、松本氏の諸論稿と比較して、本稿の特徴と意義は特に次の諸点にあると考える。

（１）　テロ対策を含む国家安全保障のために運用されている一国の情報収集力の全体像を提示しようと試みていること。

松本氏の論文は、英独仏諸国の国際テロ対策関連の個別の法的権限を中心に論述しているのに対し、本稿では、それら諸権限が全体としてどのように一国の情報収集力を構成しているかに力点を置いて論述している。また、単に国際テロ対策のためだけではなく、国家安全保障のために広義の治安機関が有すべき情報収集力の視点から論述している。欧米の諸機関の情報収集力は、20 世紀の「冷戦」下にあって主として国際共産主義からの脅威（自由民主主義国家体制に対する挑戦）に対抗して（即ち、防

---

[1] 松本光弘『イスラム聖戦テロの脅威』（講談社、2015 年）、同「国際テロ対策の手法と組織～テロ攻撃の阻止とテロリストの監視」関根謙一・北村滋他編『講座警察法第三巻』（立花書房、2014 年）、同「国際テロと自由」大沢秀介・小山剛編『自由と安全―各国の理論と実務』（尚学社、2009 年）、同「国際テロリズムとの闘い」安藤忠夫他編『警察の進路』（東京法令出版、2008 年）、同「国際テロ対策とインテリジェンス」『警察政策第 10 巻』（警察政策学会、2008 年）など参照。

なお、松本氏は、「欧州諸国では行政傍受が以前から常識だったのに対し、米国は国内での傍受が（9.11 以前は）司法傍受（犯罪嫌疑なしで傍受できず、可否判断は裁判官）のみだった」（松本『聖戦テロの脅威』206 頁など）とする。しかし現実は、遥か以前から米国内においても行政傍受は行われてきた。茂田忠良『米国における行政傍受の法体系と解釈運用』（警察学会資料第 94 号、2017 年）参照。対外諜報監視法 FISA105 条に基づく通信傍受は、国家安全保障のための行政傍受であって、刑事捜査のための司法傍受ではない。

[2] 松本「国際テロ対策の手法と組織」594 頁

諜 Counter-Intelligence、政府転覆活動対策 Counter-Subversion、テロ対策 Counter-Terrorism のため）構築されてきたものである。近時の国際テロ対策のための情報収集力も、新規に構築されたものではなく、20 世紀に構築された情報収集力の延長線上にある。これは実務経験者にとっては常識であり、この点を前提として論述している。

（２） 欧米の情報収集力がどう運用されているか、具体的事例を示して論述していること。

テロ対策における情報収集力や情報収集権限の実態を理解するには、具体的事例を見るに勝るものはない。しかし、情報収集力の実態を対象勢力に知らせてしまえば、対抗措置を採られてしまう。当局にとっては「手の内」であり、開示したくない秘密事項である。欧米諸国の情報収集力の実態が我が国で広く知られていないのも、そのためである。本稿では、各種開示資料から、参考となる具体的事例を探して、記述している。なお、上述したように、防諜、政府転覆活動対策、テロ対策のための情報収集力は同質であり、テロ対策で適切な具体例を見い出せない場合は、防諜事案における情報収集事例を記述する。

（３） シギント機関とシギント情報力の重要性を強調していること。

21 世紀の特徴は、サイバー空間が主要な情報空間として登場したことである。今や情報活動の中心はサイバー空間であり、その当然の帰結として、国際テロに関連する情報活動もサイバー空間に移行している。従って、サイバー空間における情報収集力の中核としてのシギント機関、その中でも米 NSA と UKUSA シギント同盟の重要性が増大しており、西側民主主義諸国においては、その役割の理解なくして国際テロ対策を効果的に実施に移すことは不可能であろう[3]。本稿では、シギント機関とシギント情報力が国際テロ対策で担う役割について詳述している。

なお、本稿が依拠した資料は、全て公刊資料又は漏洩資料であって誰でも入手可能な資料である。また、参考までに、講演において使用したパワーポイント資料を末尾に添付した[4]。

２　議論の視座（パワーポイント資料スライド 3 頁参照）

我が国におけるテロ対策の課題を議論するに当たっては、先ず、如何なる立場から議論するか、議論しているかという議論の視座を確認することが重要である。この視座をどこに置くかで、議論の射程と在り方が大きく影響を受けるからである。

---

[3] 後述するが、国内に所在するテロ容疑者の容疑解明については、警察機関に対する行政傍受権限の付与によって対処可能であろうが、国内外に所在する国際テロ容疑者の発見については、シギント機関の役割が大きいものと考えられる。

[4] 本講演自体の骨子は、『警察学論集』第 73 巻 10 号（2020 年 10 月号）に「日本のテロ対策の課題」として掲載されている。分量は本稿の約 4 分の 1 である。

（１）実務家の立場

従来の我が国のテロ対策の課題についての議論は、基本的には実務家の立場からなされてきたと言える。テロ対策の実態に詳しいのは実務家である以上、これは当然のことであろう。そのような立場から政府は、今まで必要と目される政策を逐次決定し実施に移してきた。

即ち、2004 年「テロの未然防止に関する行動計画」（国際組織犯罪等・国際テロ対策推進本部《本部長・内閣官房長官》）という当時としては画期的な政策策定を皮切りに、2008 年「犯罪に強い社会の実現のための行動計画 2008」（犯罪対策閣僚会議《主宰・総理大臣》）、2013 年「『世界一安全な日本』創造戦略」（閣議決定）にもテロ対策が盛り込まれた。更に、国際組織犯罪等・国際テロ対策推進本部は 2017 年「2020 年東京オリンピック競技大会・東京パラリンピック競技大会等 を見据えたテロ対策推進要綱」を策定するなどして、各種のテロ対策を策定して幅広く実施してきた[5]。

また、テロ対策の中心官庁である警察庁でも、政府の動きと連動して 2004 年「テロ対策推進要綱」、2015 年「国際テロ対策強化要綱」を策定し、対策を実施してきた。

それでは、このような政府のテロ対策への取組は、十分なものであろうか。このような実務家によるテロ対策の特色は、現状を前提としてこれに何を加えるかという形にならざるを得ない。実務家にとっては実現不可能な政策を掲げても無意味だからである。その結果テロ対策の取組は、どうしても漸進的な、incremental な取組となる。問題はそうして実務家が主導してきた我が国のテロ対策が、十分なものなのかということである。

（２）実務家 OB 研究者の立場

これに対して民間研究者のテロ対策の議論を見ていると、一方では、テロ対策強化は結局テロ対策を担当する諸組織の権限を強化することとなり、これは国民の人権擁護の観点からは問題があるという議論がある[6]。もう一方には、我が国のテロ対策の現状に不安を抱きつつもテロ対策の実態を理解していないと思われる議論がある。テロ対策の詳細を公表することは、テロリストに対して対策の弱点を知らせることにもなるので、各国当局は情報開示に積極的ではなく、テロ対策の実態は必ずしも広く知ら

---

[5] 実施状況は、「主なテロの未然防止対策の現状」（平成 29 年 12 月内閣官房作成）に要領良くまとめられている。

[6] テロ対策において最も重要な視点は、国民の人権の保護である。テロ対策上必要があるからと言って、テロ対策当局の権限を強化すれば、それは国民のプライバシーその他の人権を制約することとなる。そのような人権の制約は成るべく少ないことに越したことはないのである。他方、テロが敢行されてしまえば、これまた国民の生命財産という人権の侵害をもたらす。またテロによる恐怖により、国家の安全保障の毀損、国家体制・国家秩序の動揺を通じて国民の人権侵害を惹起しかねない。国民の人権と国家安全保障とは、共に終局的には国民の人権に係ることなのである。

れている訳ではない。そのためか、欧米諸国で大規模テロ事件が発生した際に出される我が国「有識者」のコメントを見ても、テロ対策の実態を理解した上でのコメントなのか疑わしいものも見受けられる。

筆者は、現在研究者の立場であるが、嘗ては警察庁で国際テロ対策に従事し、諸外国の諸機関とも交流を持った経験がある。そのため我が国のテロ対策の実情と共に諸外国のテロ対策の実態についても知識を有していると考えている。また、既に実務家ではないので、実現可能性を前提とした議論に拘束される必要もない。

そこで、国内外のテロ対策の実態を前提とした上で、当面の実現可能性を離れて、我が国のテロ対策の現状でテロを抑止できるのか、我が国のテロ対策の現状は世界の標準的対策から見てどうか、更には、どのような組織や権限があれば国際テロを抑止できるのかなど、我が国のテロ対策の課題を論じてみたい。

その際の最大の課題は、情報収集力である。テロ抑止のためには、テロ容疑者やテロ準備活動を如何に捕捉探知するかが枢要であるからである。

（３）国際協力上の必要性

議論の視点としてもう一つ重要なのは、国際協力上の必要性である。国際テロに対応するには国際協力が不可欠であるが、他の諸国のテロ対策の実態、テロ対策の国際標準を知らなければ、国際協力も円滑に進めることはできない。例えば、友好国のテロ対策組織に情報収集で協力を依頼するにしても、当該国がどのようにして情報を収集しているのか、どのようなテロ対策手法を採っているのかを知らなければ、効果的な協力を得ることは期待できない。或いは、在京の外国インテリジェンス機関員からテロ関係情報の提供を受けた場合、その情報ソースをヒューミントであると速断するようでは問題である。米国のテロ対策の実態とインテリジェンス諸機関の関係を知っていれば誤解することはないのであるが、知らなければ誤解を生じ、国際協力を円滑に進める上での支障となる。

テロ対策において国際協力を実効あらしめるには、特に欧米諸国のテロ対策、世界標準のテロ対策を念頭に置く必要があるのである。

以下、本稿では、実務家 OB 研究者の立場から、国際協力上の必要性を視野において、我が国のテロ対策の課題について論ずる。

（４）本稿の構成

本稿の構成は次の通りである。先ず、「第１章　思考と認識におけるギャップ」においては、テロ対策に対する我が国と欧米諸国の間での、思考の枠組のギャップ、認識ギャップについて言及した上で、我が国おけるテロ対策における最大の課題「情報収集力の決定的不足」について事例を挙げて指摘する。次に、「第２章　20 世紀以来

の情報収集力の違い」では、テロ対策における情報収集手法と収集力[7]に関して、既に20世紀において欧米諸国と我が国の間では極めて大きな違い・格差があり、それが現在にも引き継がれていることを述べる。次に「第３章　サイバー空間の課題」では、21世紀の枢要な情報空間はサイバー空間であり、テロ関係活動も同空間に移行している。従って、21世紀におけるテロ対策ではサイバー空間における対策が重要となっているが、欧米諸国のサイバー空間における情報収集の実態を述べ、我が国との違いを提示する。更に、「第４章　その他の課題」では、テロ対策におけるその他の我が国の課題を述べ、以上で我が国のテロ対策の課題の全体像を、そして背景にある国家安全保障上の課題を含めて論述する。

[7] これは同時にスパイ対策、政府転覆活動対策における情報収集手法と収集力でもある。

第１章　思考と認識におけるギャップ

１　思考の枠組・座標（スライド５頁参照）

テロ対策の課題を考える場合、どのような思考の枠組、座標軸で考えるのかを確認しておくことが重要である。この点においても、我が国と世界標準の間には微妙なズレがあると見られるからである。

（１）テロ対策の目的；「事案対処」と「未然防止」

テロ対策の目的、目指す目標は何かを考えると、「事案対処」と「未然防止」の二つの方向性がある。「事案対処」は、テロが発生した際に被害を限定する、捜査をする、検挙するという方向性であり、「未然防止」は、そもそもテロを起こさせないという方向性である。当然の事ながら、テロ対策の主目的は未然防止であり、未然防止に失敗した場合に事案対処の機能が必要となる。

未然防止の為に重要なのは、何といってもテロを企図する者・組織に対する情報収集力である。情報無しに警備部隊或いは警備実施で守ろうとしても、到底テロの完全抑止は望めない。「至る処守らんとすれば、至る処弱し」であって、全てを守ることは出来ないからである。

（２）テロ対策の機能：「法執行」と「国家安全保障」

テロ対策というものを如何なる社会機能、国家機能と位置付けるかを考えると、「法執行」機能と「国家安全保障」「ナショナル・セキュリティ」機能と二つの側面がある。

「法執行」機能とは、テロを犯罪行為として、刑事司法制度の一連の過程、即ち犯罪の予防、捜査、裁判、処罰、法秩序の回復という流れの中で捉える視点である。テロ行為に対しては刑事裁判に至ることが通常であり、テロ対策には当然「法執行」側面がある。他方、テロリストの目的は、単に犯罪を敢行することにあるのではなく、特定の主義主張に基づいて特定の国家を攻撃し国家体制・国家秩序に動揺弱体化を来すことにある。テロ対策は、国家に対する攻撃から国家を防衛する機能を持つのであるから「国家安全保障」機能の側面が大きいのである。従って、米国初め多くの国々は、テロ対策に必要な情報取集権限を、刑事司法制度の中というよりも国家安全保障のための行政調査として位置付けているのである。

我が国では、テロ対策を議論する際に、テロ対策には「法執行」機能と「国家安全保障」機能の両側面があり、「国家安全保障」機能が重要な要素であるという認識が必ずしも十分ではないと考えられる。

（３）テロ対策の主担任機関：「警察機関」と「インテリジェンス機関」

テロ対策には多くの行政機関が関与しているが、主たる担任機関を考えると、我が国では普通「警察機関」しか浮かんでこない人が多いのではないか。しかし、国際的には主担任機関としては通常「警察機関」と「インテリジェンス機関」の二つあげられるのである。

「インテリジェンス機関」の内、テロ対策に関与する主たる機関は、欧米民主主義国家ではセキュリティ・サービスとシギント機関である。セキュリティ・サービスとは、テロ対策、スパイ対策、国家転覆活動対策など「国家安全保障」のための情報収集を行うことを主任務とする組織である。元々は警察機関の一部であった場合が多いが、その任務の特殊性や広汎な情報収集（行政調査）権限のために、一般警察機関から分離した国が多い。正にテロ「未然防止」のための「国家安全保障」機能を担う組織である。なお、米国には独立したセキュリティ・サービスは存在せず、FBI 内の国家安全保障局[8]がその任に当たっている。

また、シギント機関の役割も重要である。テロ対策においてサイバー空間の重要性が増大しており、そのためサイバー空間の情報収集を担当するシギント機関の役割が増大しているのである。

２　テロ等準備罪に対する評価：認識ギャップの一例（スライド６頁参照）

テロ対策における認識ギャップの事例として指摘しておきたいものに、いわゆるテロ等準備罪、即ち 2017 年制定の「組織的犯罪処罰・犯罪収益規制法」第６条の２についての認識がある。

本条は 2017 年に追加制定された条文であるが、制定時には、これが制定されたら自由がなくなるなどと大反対運動があったのは記憶に新しいところである。そのためか、一部の民間研究者には、テロ等準備罪の制定で我が国のテロ対策は相当進展したと誤解している者もいる。そのような誤解が存在する事実にも、テロ対策の実態に対する認識ギャップが伺われるのである。

テロ等準備罪の立法目的や内容については、法務省のウェブサイト「テロ等準備罪について」[9]に詳しいが、ウェブサイトを見れば分かる通り、テロ等準備罪の立法目的は、先ず第１に国際組織犯罪防止条約（TOC 条約）の締結であった。立法当時の未締結国は、200 ヵ国に近い国連加盟国中僅か 11 ヵ国、主要国では日本のみであり、条約締結のための国内法整備が急がれたのである。そのためテロ等準備罪は、我が国のテロ対策における実効性よりも立法自体が優先されている。

それはテロ等準備罪の構成要件を見れば一目瞭然である。即ち、テロ対策で同条の

---

[8] FBI 国家安全保障局が行うテロ対策（情報収集）は、刑事捜査活動というよりは、国家安全保障のための行政調査と位置付けられている。

[9] 法務省ウェブサイト「テロ等準備罪について」参照。
http://www.moj.go.jp/keiji1/keiji12_00143.html

犯罪の成立には次の三つの要件が必要である。

①「組織的犯罪集団（テロ集団）」の関与。即ち、多人数の継続的な集団であって、犯罪実行部隊のような組織性を有し、重大犯罪の実行目的で集まっている集団（テロ集団）の存在と関与の立証が必要である。

②　「テロ計画」。即ち、「団体の活動として」、具体的且つ実行可能性のあるテロの犯罪実行の合意をしたことの立証。

③　計画に基づく「実行準備行為」が行われること。

本条は刑罰の実体法であるが、これだけ厳格な構成要件①②③を同時に要求する立法例は、筆者の知る限りでは他国のテロ対策処罰法では見られない。例えば、フランスの立法例では、上記①のテロ集団への加入だけで可罰的である[10]。また、米英法では共謀罪の理論によって、テロの共謀に加えて「徴表的行為 overt act」（即ち③の準備行為）が認められれば可罰的となり、テロの共謀には①や②のような要件の立証は必要ない[11]。

このように我が国のテロ等準備罪の構成要件は極めて厳格であるが、この厳格な①②③の構成要件を如何にして立証するのであろうか。我が国当局に与えられた権限は諸外国と比べて極めて限定されている。通信傍受[12]も、囮捜査・調査も、司法取引も、秘密捜索も、認められていないか、認められていても極めて限定的である。限定された権限で極めて厳格な構成要件を立証するのは、至難の業である。そもそも、立証どころか、テロリストとテロ準備行為の探知自体ができるのか、問題がある（この情報収集力の課題については後に詳述する）。

更に、現在の国際テロの実態を見た場合に、国際テロはそもそも①②③の三つの構成要素を満たさずに敢行されているものが多い。或いは、仮に①②③の要素を満たす国際テロであっても、①と②の要素は国外に存在している場合が多いと考えられる。9.11 同時多発テロ事件を例に取れば明らかである。では我が国当局は、国外テロ集団が我が国に対するテロ実行を国外で計画していることを立証できるのであろうか。それ以前に探知する情報収集力を有しているのであろうか。結論は明らかであろう。

以上をまとめれば、実務家の感覚としては、テロ等準備罪は、殺人予備罪等の他罪の捜査の結果、出口として他罪と合わせてテロ等準備罪も成立し得ることはあっても、テロ事件捜査の入口でこの罰条が役立つことはまず考えられない。従って、本罰条がテロ抑止に貢献するとは考えれない。これは、実務家の間では共通認識であろう。平

10　警察庁・平成 28 年版『警察白書』第 1 部国際テロ対策第 2 節 32 頁参照。

11　英国 2006 年テロ法 Terrorism Act 2006 第 5 条のテロ行為準備罪は、単純に個人によるテロ準備行為を可罰的としている（終身刑）。また、2000 年テロ法第 57 条のテロ目的での物資保持罪も、挙証責任の一部を実質的に被告人に転換するなど、立証が容易なものとなっており、実際のテロ防止に効果のある法制となっている。

12　法務省ウェブサイトでは、テロ等準備罪の捜査で「通信傍受」はできないことを強調している。

成 28 年版『警察白書』は「国際テロ対策特集」をし他国の立法例にも言及しているが、我が国のテロ等準備罪について全く言及していない。その背景には本罪に対するこのような評価があると考えられる。

このような実務家の認識が社会で共有されていない事実に、テロ対策における我が国における認識のギャップが見られるのである。

３　テロ対策情報収集力に対する認識ギャップ

テロ対策に関する認識ギャップの典型として、我が国当局の情報収集力を見てみよう。我が国当局のテロ対策関係の情報収集力は、国際標準と比べて決して高くないが、それが必ずしも認識されていないと考えれる。具体的な事例を四つ挙げる。

（１）オウム真理教地下鉄サリン事件　1995 年 3 月（スライド 7 頁参照）

1995 年に地下鉄サリン事件がオウム真理教によって敢行されたが、本事件は世界初の大都市における化学兵器使用の無差別テロであった。被害は甚大であり、死者 13 人[13]、負傷者 6 千人以上（その内重傷者千人以上、要介護者数十人）の被害者を生んでいる。

オウム教団が本事件を敢行するまでには様々な事前の活動・兆候があったが、残念ながら、テロ計画を未然の内に探知して阻止することができなかった[14]。このようなテロ事件を二度と起こさせてはならないことは明白であり、そのためどのような対策が採られたのか気になる所である。

そこで政府の対応を見ると、1999 年に無差別大量殺人団体規制法、いわゆるオウム新法を制定している。しかし法律の内容を見ると、これは実質オウム残党監視法に過ぎない。オウム真理教の残党（＝「無差別大量殺人行為を行った団体」）が再びテロ等の犯罪を行わないように監視するための法律であって、他の未知のカルト集団によるテロ行為を未然に探知阻止するための法律ではない。即ち、大規模テロを未然防止するための立法はなされなかったのである。

そもそも地下鉄サリン事件のような無差別大量殺人が惹起された国家において期待される対応は、政府が調査委員会を設置して事件の原因と対策を明らかにする、そして、再びカルト集団による同種事件を発生させないため、未然に探知し阻止するため立法措置を含め各種の対策を採ることあろう。残念ながら、我が国では政府レベルでそのような対策は採られなかった。

そこで、主務官庁である警察庁の対応を見ると、平成 8 年版『警察白書』第 1 章に

---

[13] 本事件を原因とする死者は、2020 年 3 月 10 日に 14 人となったと報道されている。その他にも現在でも後遺症で苦しむ者がいる。『産経新聞』2020 年 3 月 20 日付「地下鉄サリン 56 歳被害女性死去」参照。

[14] 筆者の経験から言えば、これ程の準備活動・兆候があったテロ事件は、国際標準の情報収集力（後述）があったならば、確実に事前に探知し抑止できていたであろう。

「新しい組織犯罪への対応～オウム真理教関連事件を回顧して～」と題して、オウム真理教特集を行っている。そして、事件の反省教訓として次の三つを挙げている[15]。即ち、

① 高度な科学技術についての知識不足
② 特殊な閉鎖的犯罪組織についての情報不足
③ 都道府県警察の管轄区域外の権限についての制限

さて課題は②の情報不足、即ち、情報収集力の不足である。事件後、情報収集力の不足は解消されたのであろうか。そのための組織権限、特に潜在的テロ集団に対する情報収集権限は強化されたのであろうか。

国際テロ組織は基本的に全て「特殊な閉鎖的な組織」であるから、「特殊な閉鎖的犯罪組織」に対する情報収集力の向上なくして、国際テロの未然防止は覚束ないのである。

（２）中核派・大坂正明の逮捕　2017 年 5 月（スライド 7 頁参照）

2017 年に中核派・大坂正明が逮捕された。大坂は、1971 年 11 月のいわゆる渋谷暴動で警察官を殺害したとして全国指名手配され、全国警察が追及していた者である。それが、2017 年に至って遂に広島で大阪府警によって逮捕されたのである。1972 年の指名手配以来実に 46 年間、大坂は中核派・非公然組織の支援を受けて国内に潜伏していたのである。

これを国際標準の情報収集力の視点で見るとどうであろうか。日本の警察当局は中核派の非公然組織の全容を解明できていないという事実が浮かび上がるのである。解明できていれば、46 年間の長期に亘って大坂の逃走を許すことはなかったからである。

誤解してはならないのは、これは現場の警察官の資質や努力の問題ではないのである。関係の公安担当警察官は、必死に任務を遂行している。必死に任務を遂行したからこそ、漸く大坂の逮捕に至ったのである。関係者の努力に敬意を表するものである。

しかし他方、現在の我が国の制度・権限を前提にする限り、これが日本警察の組織としての情報収集力の実態なのである。我が国に「中核派」という極左暴力集団があり、その中に相当の非公然部門が存在するが、日本警察にその全容を解明する力はない。この情報収集力で、国際テロにどこまで対抗できるのか、大きな課題である。

しかし、警察の情報報集力に課題があるという声は起こってこない。ここにも認識のギャップが存在する。

（３）リオネル・デュモンの日本潜伏（1999 年～2003 年）

フランス人リオネル・デュモンは、アルカイダ系の活動家で、爆弾テロ未遂等のテ

[15] 警察庁・平成 8 年版『警察白書』第 1 章第 5 節参照。

ロ容疑で国際刑事警察機構から指名手配を受けていた者であるが、日本国内に潜伏していたことが判明した[16]。

デュモンは、1990 年代にボスニアの警察官殺害の罪で懲役 20 年の刑を宣告され服役していたが、脱獄して逃亡したため、1999 年に国際指名手配を受けていた。そして 2003 年 12 月にドイツで逮捕されフランスに送還された。2004 年 5 月に我が国警察は、デュモンの日本滞在に関連して関係個所を捜索し出入国管理法違反の罪などで 5 人を逮捕した[17]。

そこで判明したのは、デュモンは 1999 年 9 月から 2003 年 9 月の間、偽造旅券で我が国に 6 回も入国し[18]、その内 2002 年 7 月から 2003 年 9 月の間には合計 9 か月間、新潟市内を中心に滞在していたことである。日本滞在の目的が、単なる逃亡なのか、テロ資金活動かテロ支援活動であったのかは判明していない[19]。

問題は、このデュモン滞在の事実を、我が国当局が把握できていなかったと見られることである。警察庁の公刊文書は「我が国への入出国を繰り返していた事実が、ドイツにおける同人の逮捕（2003 年 112 月）を端緒として判明」[20]と記述しており、同人の日本国内潜伏時に、我が国当局がその事実を把握していなかったことが伺われる。

テロで国際手配されていたデュモンの入国滞在を探知できず、仮に彼がテロを企図していたとしてもそれを探知できていなかった。この事例は我が国当局の国際テロ対策に関連する情報収集力の現状を示しているのである。

（４）「イスラム国」戦士の帰国問題（スライド 8 頁参照）

「イスラム国」戦士の帰国問題には、各国とも頭を悩ませている。「イスラム国」の崩壊に伴い帰国して国内でテロを行われては困るからである。

ところが「イスラム国」戦士には日本国籍者もいる。報道[21]によれば、「イスラム国」戦士の幹部にバングラデシュ出身で日本に帰化した日本国籍者がおり、シリア国内で拘束されているという。さて、仮にこの者が帰国した場合に、我が国当局はどう

---

16 警察庁警備局『平成 26 年回顧と展望』（焦点第 284 号、2015 年 3 月）17 頁。

17 Eric Talmadge, “Al-Qaeda agent lived quiet life in Niigata,” *Japan Times*, 2 June 2004, accessed 5 April 2020, https://www.japantimes.co.jp/2004/06/02/announcements/al-qaeda-agent-lived-quiet-life-in-niigata/#.XomZcYj7SUk--

18 村田隆「我が国における国際テロ対策の現状」大沢秀介・小山剛編『自由と安全―各国の理論と実務』（尚学社、2009 年）69 頁。
- 公安調査庁『国際テロリズム要覧 2019 年（ウェブ版）』国際テロ組織・ルーベ団、2020 年 4 月 5 日閲覧、
http://www.moj.go.jp/psia/ITH/organizations/europe/the_roubaix_group.html

19 板橋功『国際テロ情勢と対策』（関西大学邦楽研究所、ノモス第 28 号、2011 年 6 月）15 頁。https://www.kansai-u.ac.jp/ILS/publication/asset/nomos/28/nomos28-01.pdf

20 警察庁警備局『治安の回顧と展望（平成 26 年版）』76 頁。

21 例えば、『産経新聞』2019 年 6 月 7 日付「立命大元准教授　米軍が拘束～IS 危険人物テロ容疑」

対応できるのかという課題がある。

先ず、処罰できるのかという課題がある。私戦予備という罰条があるがその適用はなかなか難しいと考えられる。また、処罰できないまでも国内でテロを起こさせないように拘束できるかというと、そのような行政権限は存在しない。それでは、テロを起こさせないように十分監視できるのか、どの様な監視手段があるのか、ということになると、これまたその実効性は覚束ない。

先ず、我が国の警察にできることは、本人に任意に面接すること、或いは本人の近辺に協力者を得ること位であるが、本人も自分が当局の関心対象であることは十分自覚する筈であるから、仮にテロを企図していたとしても容易にその企図を明かすことはないであろう。また、尾行張込をするにしろ、労多い割にはその実効性は不明である。警戒している者に気付かれずに尾行張込をすることは実は相当に困難が伴う。こうして帰国者の監視すら十分にはできないのである。これに対して、欧米諸国は実効性のある種々の監視手法を持っているのである[22]。

しかし、我が国警察の監視能力、即ち情報収集手法の貧弱さについては、余り意識されていない。

つまり、以上の四つの事例を通して見ると、テロ対策に関して、我が国の警察の情報収集力は不十分であるが、それが必ずしも国家指導層を含む国民には認識されていないと考えられるのである。

[22] 後述するが、欧米諸国の標準的な監視手法としては、先ず行政傍受によって本人のメール通信やウェブ閲覧の内容を把握することが考えられる。その内容によって本人のテロ関連容疑性をある程度推定できるであろう。本人が通信内容秘匿のために、TOR 通信や PGP 暗号通信などを使用すれば、使用方法や頻度によってこれも本人の容疑性推定の指標となるであろう。容疑性が高まれば、住宅の秘密捜索や預入手荷物の秘密検査、更には住居への会話傍受装置や撮像装置の設置も手段として持っている。諸外国担当機関は、我が国と比べて極めて多彩な監視手法・情報収集手段を持っているのである。

第２章　20 世紀以来の情報収集力の違い

第１章、特に「３　テロ対策情報収集力に対する認識ギャップ」において、我が国のテロ対策における情報収集力は、決して高くないことを見てきた。

ところで筆者は、前世紀において国際テロ対策に従事して欧米諸国のテロ対策諸組織と遣り取りをした経験がある。その際に痛感したのは、欧米諸国と我が国の間の情報収集力に格段の差があるということであった。欧米の諸機関と遣り取りしていると、「何故ここまで知っているのか」と感心する経験が度々あった。つまり、欧米諸機関の情報収集力の方が格段に強力だったのである。

情報収集力に格差が生じる理由は、情報収集手法・手段の違いである。

当時は、現在ほど情報公開は進んでおらず、また、テロ対策諸組織も、特にインテリジェンス機関は現在よりも遥かに秘密主義的傾向が強かった。具体的な情報収集手法は言わば「手の内」であって、その全体像を開示するようなことはなかったのである[23]。しかし、相手組織との遣り取りの中から情報収集手法を推測することは可能であった。こういう情報ソースがなければこの情報は取れないだろうと推測できることがあるのである。筆者はそうした経験を積み重ねて欧米諸国の情報収集手法の全体像を推測した。

そこで本章では、先ず、20 世紀における欧米諸国と我が国の情報収集手法の違いについて、経験に基づく推論を述べる。

その後欧米諸国でも情報開示が進み、筆者の推論を裏付ける資料が公表されている。そこで、次に英米について情報収集手法の全体像を示唆する公表資料を見た後に、具体的な情報収集手法の一部について情報が開示されている個別の事案調査・捜査を例に取って、論述する。

１　欧米諸国と我が国の情報取集手法の違い

（１）我が国の情報収集手法（スライド 10 頁参照）

我が国警察の基本的な情報収集手法は、任意手段による情報収集である。即ち、行動確認（尾行張込）や協力者運用である。また、捜査機関として事件捜査の権限も活用している。しかし、これらの手法では限界があり十分な情報収集は期待できない[24]。

次に、行動確認、協力者運用、事件捜査について若干敷衍する[25]。

---

[23]　単にテロ関連情報の交換の場合には外国機関に情報源（即ち≒情報収集手法）を開示することは一般的には行わない。他方、テロ対策の共同作戦を行えば、当然、必要な範囲で具体的な情報収集手法について情報共有をすることとなる。

[24]　地下鉄サリン事件の未然防止や大坂正明の早期逮捕が出来なかった主因はここにある。

[25]　本文に記述した他、21 世紀に入るとテロ関連情報活動でもサイバー空間の重要性が高まり、現在、日本警察もサイバー空間からの情報収集に力を入れている。例えば 2016 年 4 月警察庁はインターネット・オシントセンターを警備局内に設置している。しかし、我が国警察が

○　行動確認（尾行、張込）：我が国警察の特色は、尾行や張込など人力による行動確認を広汎に実施していることである。しかし、警戒する相手に気付かれずに行動確認をするのは、極めて困難であり、膨大な人員を必要とする。

○　協力者運用：「特殊な閉鎖的な組織」であるテロ組織内に、或いはその周辺に情報入手が可能な協力者を得ることは大変難しい。

○　事件捜査：警察の事件捜査の権限を最大限に活用して、司法捜査の一環として、テロ組織・集団に対して積極的に捜索差押を行い情報収集を行っている。但し、そのためには裁判所から捜索差押許可状を得るだけの必要性の疎明が必要である。また、捜索をしても、極左暴力集団のように文書（水溶紙）を直ぐに廃棄して情報を得ることができないことも多い。

○　警察の総合力：我が国警察の特色は、47 都道府県警察が全国に警察署 1160、交番 6 千以上、駐在所 6 千以上を配置し、国民の支持を得てこれらが相互に密接に協力して活動している点にある。テロ対策に当たる警備警察部門もこの全国警察組織の一部として、警察の総合力を活用している。

（２）欧米の情報収集手法（スライド 11 頁参照）

これに対して、欧米諸機関の情報収集手法は多彩であり格段に強力である。欧米諸国でも、我が国同様に。行動確認（尾行張込）[26]、協力者運用、事件捜査権限も活用するが、寧ろ、「技術能力」（technical capabilities）と呼ぶ通信傍受、信書開披、或いは容疑者宅等の秘密捜索やマイク設置などを多用している。また、「ヒューミント」ではテロ容疑集団への潜入調査や囮調査を実施している。

欧米諸国が標準的に行っている手法について若干敷衍する[27]。

○　通信傍受：標準的な情報手段であり、益々重要となっている。

○　信書開披：戦時中の軍事検閲では普遍的であったが、平時のテロ対策でも標準的な情報収集手段であった。

○　秘密捜索：旅客機での預入手荷物や住居内の秘密捜索による情報収集である。警

サイバー空間で行っているのは、インターネット上に公開されている情報の収集・分析であって、一般人に許されない特別な情報収集を実施している訳ではない。平成 28 年版『警察白書』21 頁参照。

[26] 筆者の体験から判断して、欧米諸機関は、尾行などの行動確認は我が国と比べて頻繁広汎に行う訳ではない。他の手段では代替できない、真に尾行が必要な場合に限られるようである。欧米諸国は有効な情報収集手段を多数持っており、それらと対比して、秘匿の行動確認は、多くの人員を必要とし、費用対効果が低いからであろう。

[27] 本文に記述した他、21 世紀に入ると、サイバー空間の監視が大きな課題となっており、欧米諸機関は各種権限を駆使して広汎な情報収集を行っている。テロ容疑者の保持する通信機材に対するハッキングも行われている。この点については第 3 章で詳述する。また現在、画像認識機能の高度化により、監視カメラを利用した広汎な情報収集システムは、中国が積極的に開発し導入している他、積極的に輸出もしている。広汎な画像利用監視システムは、欧米諸国においても課題となっている。

戒心を起こさせないために、捜索の事実自体を本人に認識されないようにする必要がある。預入手荷物の秘密捜索では、時間を稼ぐため必要とあれば、関係機関の協力を得て旅客機の出発を遅らせるなどの措置を採ることもある。

○　監視機材の設置：住居や車両の中にマイクやカメラなどの監視機材を設置して行う情報収集である。当然、住居や車両内への秘密侵入が必要である。

○　潜入調査・囮調査：テロ組織への潜入には、潜入エージェントの犯罪実行に対する免責措置が不可欠である。テロ組織の中で、犯罪実行を忌避すれば不審を惹起して本人の命すら危ういからである。組織やテロ仲間の信頼を勝ち取るには寧ろ犯罪行為に積極的となる必要がある。また、身分偽変を確実にするための行政措置が必要となる。潜入調査は、場合によっては長期間に及ぶ人生を賭けた作戦となる場合があり、それだけの覚悟がなくては実施は難しい。

以上は私の経験に基づく情報収集手法全体像の推論であった。ところで、前世紀ではこの全体像を欧米諸国の公開公文書で示すことは難しかったが、今世紀になると全体像を示す政府公開資料が出て来る。次に、英国と米国について、資料を見てみよう。

２　英国の資料：2000 年調査権限規制法[28]（スライド 12 頁参照）

英国においてテロ対策の情報収集手法を明示した公刊資料としては、2000 年調査権限規制法 RIPA2000（Regulation of Investigatory Powers Act）が挙げられる。同法には、通信傍受、通信データの使用、指向性監視、侵入的監視、及び秘匿ヒューミントが規定されており、テロ対策で使用できる情報収集手法が法律で明示されている[29]。

これら各種情報収集手法については、同法第 71 条に基づき、内務大臣が制定する各種実施規範 Codes of Practice が公開されている[30]。実施規範は実施のための手続規定であり、各手法の内容を具体的に記述している訳ではないが、それでも手法の内容がある程度読み取れる。以下、各手法について見てみる。

○　通信傍受 interception of communications（RIPA2000 第 1 部）

通信傍受、郵便検閲が該当する。

---

[28] 一部に RIPA2000 を「捜査」権限規制法と訳す者がいるが正しくない。RIPA200 は犯罪捜査に限定されず、英国の行政調査一般に関する権限規制法である。

[29] RIPA2000 第 1 篇の通信傍受、通信データ関係については、その後 2016 年調査権限法 IPA2016 によって改正され更に詳細な規定が置かれた。また、機器干渉（いわゆるハッキング）に関する規定も置かれた。情報収集実務の基本部分には変更がないので、本稿では同法の内容には立ち入らない。本稿は情報収集手法に関する法解釈自体よりもテロ対策の実態を主題にしているからである。

[30] 英国政府のウェブサイト”RIPA codes”に一括掲載されている。
https://www.gov.uk/government/collections/ripa-codes
なお、IPA2016 附則第 7 に基づく内務大臣制定の実務規範は、英国政府のウェブサイト“Investigatory Powers Act 2016 – codes of practice”に一括掲載されている。
https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

実施規範 Interception of Communications(2016 年版)

○　通信データ use of communications data（RIPA2000 第 1 部）

通信メタデータ（通信に付随する通信内容以外の情報）、通信サービス利用情報、契約者・アカウント保有者情報が該当する。

実施規範 Acquisition and Disclosure of Communications Data
Retention of Communications Data(共に 2015 年版)

○　指向性監視 directed surveillance（RIPA2000 第 2 部）

侵入を伴わない特定人物に対する監視・情報収集である。行動確認の他、公開の場所での会話の秘密録音や車両への位置発信装置設置など非侵入的な機材を使用した監視を含む。街頭監視カメラ・システムを特定人物の動向監視のために使用すればこれも含まれる。

○　侵入的監視 intrusive surveillance（RIPA2000 第 2 部）

居住施設（住居やホテル客室）又は自動車内への侵入を伴う秘匿監視であり、秘密捜索やマイクやカメラなど監視機器の設置が含まれる。

実施規範 Covert Surveillance and Property Interference(2018 年改訂）が上記「指向性監視」と「侵入的監視」の両者について規定している。

○　秘匿ヒューミント covert human intelligence sources（RIPA2000 第 2 部）

秘匿情報源（協力者又は偽装工作員）の運用

実施規範 Covert Human Intelligence Sources (2018 年改訂)

ここで注目すべきは、これらの諸権限は全て行政権限であって、基本的に所管大臣又は省庁や警察本部幹部の指示において実施できることである。また、このような調査手法は、2000 年調査権限規制法が制定されて初めて英国で実施されるようになったのではなく、同法制定以前の 20 世紀の長期間に亘って法律の根拠なしに、実施されてきたのである。

3　米国：2016 年国防総省諜報活動実施手続（スライド 13 頁参照）

米国における情報収集手法の全体像が分かる文書としては、2016 年改訂の「国防総省諜報活動実施手続」マニュアル DoD Manual 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities[31]がある。

本マニュアルは、国防総省傘下のインテリジェンス組織の活動手続であるが、大統領命令 12333 号「米国諜報活動」[32]に基づき、国家諜報長官と協議の上、国防長官と司法長官の同意を得て制定されている。国防総省系の諜報組織のための基本マニュアルであって、CIA や FBI 国家安全保障局には適用されないが、情報収集手法について

---

[31] 米国 DoD, *DoD Manual 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities,* 8 August 2016, https://www.hsdl.org/?abstract&did=794860

[32] Executive Oder 12333, United States Intelligence Activities.

は CIA や FBI についても同様であると考えられる。

本マニュアルの特徴は、各情報収集手法について用語解説があるなど、英国の法律よりは各手法が理解し易く定義されていることである。これも、軍隊という典型的な官僚組織の性格を反映したものであろう。なお、本改訂は 1982 年以来であり、この間の諸事情を反映してより米国人の人権に配慮したものとなっているとされる[33]。

本マニュアルに規定されている情報収集手法は、電子的監視、秘匿監視、物理的捜索、郵便検閲、物理的監視、身分偽変の六つであり、それぞれの手法について見ていく。

○　電子的監視 electronic surveillance（Manual 3.5）

電子的通信の傍受。居住施設へのマイク・カメラなど監視機材を設置して行う監視（後者は対外諜報監視法 FISA101(f)(4) に該当）

○　秘匿監視 concealed monitoring（Manual 3.6）

住居などプライバシーが期待される施設以外で、電子装置、光学装置、機械装置を使用して行う機械監視。

○　物理的捜索 physical searches（Manual 3.7）

個人又は個人の財産や所有物に対する侵入行為であって、財産、情報、電子データや通信記録を入手する目的で行う捜索（仮に法執行目的であったならば令状を必要とする捜索である）。典型的なものは、住居等の秘密捜索、旅客機搭乗の際の預入手荷物の秘密捜索など。国外の米国人に対して又は米国内で実施するには、原則として対外諜報監視法に基づく令状（特別裁判所による秘密令状）を必要とする。捜索の実施は、国内では FBI に依頼し、国外の米国人に対しては CIA と調整しなければならない。

○　郵便検閲 searches of mail（Manual 3.8）

郵便物の開披検査（捜索）。米国内での実施は FBI に依頼する。

○　物理的監視 physical surveillance（Manual 3.9）

住居などプライバシーが期待される施設以外で行う人的監視。尾行張込の類。米国内では、FBI と調整の上で実施し且つ軍関係対象者に限る。米国外で米国人を対象とする場合は CIA と調整しなければならない。

○　身分偽変 undisclosed participation in organizations（Manual 3.10）

身分偽変や潜入。但し、全て FBI、CIA その他関係機関と調整した上で実施しなければならない。また、軍諜報機関は米国内で米国人を標的にして行ってはならない。

以上見たように、通信傍受、郵便検閲、秘密捜索、マイク・カメラなど監視機材の設

---

[33] 米国 DoD, *Fact Sheet – DoD Manual 5240.01,* 8 August 2016, https://fas.org/irp/doddir/dod/m5240_01_fs.pdf

置、身分偽変・潜入調査などが、標準的な情報収集手段とされていることが分かる[34]。

4　情報収集手法：具体的事例

以上の米英の資料で見たように、米英の諸機関においては、テロ対策のための情報収集では、通信傍受、信書開披、秘密捜索、監視機材の設置、潜入調査・囮調査などの手法が一般的である。

それでは、これらの手法が使用されている実例を幾つか見てみよう。これら 20 世紀以来の情報収集手法については、米国における有名なスパイ検挙事案での使用が知られているので、その事例を中心に紹介する。テロ対策とスパイ対策と適用対象は異なっても、FBI 国家安全保障局が行う 20 世紀以来の情報収集手法の有効性と法的位置付けに違いはないからである。

なお、米国内でのこれら情報収集手法の実施に当たっては、対外諜報監視裁判所の秘密令状に基づいて行われる場合が多い[35]。

（１）秘密捜索（1985 年 11 月スパイ検挙事例）

自宅の秘密捜索や預入手荷物の秘密捜索は、標準的情報収集手法であるが、預入手荷物の秘密捜索のため空港当局上層部の協力を得て旅客機の離陸時間まで遅らせた事例[36]があるので紹介する。

ラリー・ウータイ・チンは、1922 年北京生れであるが、英語が堪能であったため大戦中に米軍の通訳となり、そのまま極東で、米国務省や米軍の通訳を継続。1952 年に CIA の外国放送情報サービス部に就職し、その後米国本土に移動。1965 年に米国籍を取得したため、CIA の機密情報にもアクセスできるようになった。チンは実は大戦中から中国共産党のスパイであり、情報を継続的に中国に提供してきた。1981 年に CIA

---

[34] なお、注意を要する点が二つある。

一つは裁判所の関与である。一定の情報収集手法を米国内で実行するには、対外諜報監視法に基づく対外諜報監視裁判所の令状を必要とする。但し、本令状は司法捜査令状ではなく、国家安全保障のための行政調査令状であって、通常秘匿され監視対象者に知らされる訳ではない。また、発布の要件も司法捜査とは異なっている。

また、もう一つは、軍の諜報機関の活動、特にヒューミント活動は国内では強い制約が掛けられていることである。米国内で行うヒューミント活動の調整責任者は FBI 長官であり、物理的捜索、郵便検閲、物理的監視、身分偽変による作戦などは、軍諜報機関には禁止されており、FBI に依頼して行うこととされている。また、ヒューミント活動全般の統括責任者は CIA 長官であり、軍が国外で行うヒューミントは CIA と調整した上で行うこととされている。Executive Oder 12333, United States Intelligence Activities.Part 1, 3(b)(12)(A)(ii), 3(b)(20)(A)(B)参照

[35] 対外諜報監視法の物理的捜索の規定は 1994 年に追加規定されたものであるので、（１）の秘密捜索は、裁判所の関与なしに実行されたものである。

[36] David Wise, *TIGER TRAP* (Boston: Houghton Mifflin Harcourt, 2011), Chapter 19, pp.202-213. 本書は FBI のスパイ摘発のための具体的な情報収集手法について比較的詳しく記載しており参考となる。

副長官から直接勲章を授与され退官した。

ところが 1982 年、中国公安部の（米国亡命希望の）愈真三が、米国諜報機関内の中国スパイの情報をもたらした。情報は断片的で人定不詳であったが、同年 9 月には FBI にも通報された。FBI は調査の上で容疑者をチンに絞り込んだ。そしてチンの自宅電話に盗聴器を設置して電話の傍受を開始し、チンが 1983 年 5 月に香港への旅行を計画していることを把握した。そこで FBI は首都ダレス空港で預入手荷物の秘密捜索をすることとしたが、荷物を開いて中を調べ且つ気付かれないように元通りに戻すには時間が足りなかった。そこで、ダレス空港当局の協力を得て、適当な名目を付け旅客機の離陸を遅らせて秘密捜索を実施した。秘密捜索では機密書類は発見できなかったが、後にチンの自供に繋がる重要証拠（北京の宿泊ホテルの客室鍵）の写真を撮影することができた。また、チンは同年 9 月には中国公安部の担当官（ハンドラー）オー・チーミンと香港のホテルで密会したが、そのホテルにはマイクを仕掛けて会話を記録した[37]。

これらが決定的証拠となり、1985 年 11 月チンは取調べで自供し逮捕された。彼は翌年 2 月に陪審裁判で有罪評決（終身刑 2 つに相当する罪）を受けたが、刑の宣告を受ける直前に拘置所内で自殺した。

（２）監視機材の設置（1997 年 7 月スパイ検挙事例）

住居やホテルの客室へのマイクやカメラなど監視機材の設置も、国際標準の情報収集手法であり、住居へのマイクの設置事例を一つ[38]を紹介する。本事例は、マイクの故障のため監視対象に探知されてしまったために公知のものとなった興味深い事例でもある。

ピーター・フンイー・リーは、1939 年重慶生れ台湾育ちであるが米国に移住し、カリフォルニア工科大学を卒業した優秀な物理学者である。1975 年に米国に帰化して、核兵器関連のロスアラモス研究所や国防企業 TRW で勤務してきた。彼は 1985 年 1 月に 4 週間ほど中国に旅行したが、その際に中国の核兵器開発担当幹部と会ってその質問に答え、1997 年 5 月には中国を訪問して専門家を対象に対潜水艦戦について講義をしており、共に機密漏洩に当たる。この他にも機密を漏洩していた推定されているが、その内容は解明されていない。

リーについては、1991 年に情報協力者からの通報があり FBI が内偵を開始した。1994 年 2 月には通信傍受（電話とメール）を開始、更に 1996 年 8 月にはリー家の台

---

[37] 当時の香港は英国支配下にあったので、英国諜報当局の協力を得て、ホテル居室の盗聴をしたものと推定できる。

[38] US Senate, Subcommittee on Department of Justice Oversight Committee on the Judiciary, *Report on the Investigation of Peter Lee*, 20 December 2001, accessed 1 April 2020, https://fas.org/irp/congress/2001_rpt/peterlee.html
-- Wise, *op.cit.*, Chapter 15, pp.154-166.

所のコンセントにマイクを設置した。ところが 1997 年 7 月にマイクが故障して電気が不通となったため、妻がコンセントのカバーを開けたところ不審物を発見、リーは不審物を見てこれが秘匿設置された小型マイクであることを見抜いてしまった。

そこで FBI は捜査を急いで、同年秋には本人は一部の罪（秘密漏洩と FBI 捜査官に対する虚偽供述）を認める司法取引で事件が終了した[39]。

（３）通信傍受、監視機材の設置、秘密捜索の事例（2003 年 4 月著名スパイ検挙事例）

過去数十年間でも最重要な対米スパイの検挙事件[40]であるので、その検挙に至る情報収集手法と合わせて紹介する。

カトレーナ・レオンは、1952 年頃広州市生れで 3 才で香港に移住、更に 1970 年米国に移住してコーネル大学を卒業、シカゴ大学で MBA を取得した。その後カリフォルニア州に移住したが、中国に対する不法な技術移転事件の容疑者と関係があったため、1982 年 FBI エージェント J.J.スミスがレオンに接近して、FBI の情報協力者（information asset）とした。ところが 1983 年には二人は愛人関係となり、レオンは工作協力者(operational asset)に昇格、対中情報収集に携わるようになった。1984 年には米国籍を取得して、FBI のために中国国家安全部の首脳に食い込み情報収集に当たる二重スパイ[41]となった。

レオンはその後今世紀に入るまで、FBI の対中・二重スパイの役割を演じてきた。レオンは中国権力中枢について米国が持つ殆ど唯一の情報源であり、江沢民など中国最高権力者の「本音」を米国にもたらした。彼女の情報は歴代大統領 4 人(レーガン、ブッシュ、クリントン、ブッシュ Jr)にも報告されており、米国の対中政策決定に大きな影響を与えてきたのである。ところが、後に判明したのは、中国最高権力者の「本音」とは実は中国側からの情報工作であり、他方、FBI の対中監視活動に関する機密情報が中国側に提供されていたことである。レオンは中国側のスパイであった[42]。

レオンの疑惑を示す兆候や情報はあったものの、J.J.スミスがレオンを擁護し続けてきたのである。しかし、スミスが 2000 年に退官すると、FBI によるレオンの監視が

---

[39] この司法取引による罪名は、合衆国法典第 18 編第 793 条（ｄ）国家防衛情報漏洩罪と同第 18 編第 1001 条虚偽供述罪で、刑罰は更生施設収容 1 年、社会奉仕 3 千時間、罰金 2 万ドルと軽いものであったため、後に連邦議会でも問題とされた。

[40] Wise, *op.cit.*, Chapters 2～4, 11, 13, 14, 18 を参照。

[41] FBI の協力者であることを中国側に明らかにして中国の協力者を演じつつ、実は中国情報を収集する役割。そのため FBI が提供する「極秘情報」を中国側に提供して信頼を得て、中国情報を収集することとなった。

[42] レオンが何時から真に中国側のスパイであったかは、明らかになっていない。1990 年 12 月に NSA の通信傍受によって、レオンが中国国家安全部の担当官（ハンドラー）に許可されていない情報を通報していたことが判明したが、J.J.スミスは詰問の上で不問に付した。その際のレオンの説明（1991 年初）では、1986 年か 1987 年に米国の二重スパイであることを探知され、逆に中国側に全てを話すことになったとされる。この説明は疑わしく、最初から、即ちスミスと愛人関係になる 1983 年前後から中国側のスパイであった可能性が高い。

始まった。2001 年 12 月にはレオンの自宅に隠しマイクが仕掛けられ、電話、Fax、E メールの傍受と尾行も始まった。すると翌年 3 月にはレオンと J.J.スミスの愛人関係が確認された。そこで 4 月には、J.J.スミスも監視対象となり、スミスの電話の傍受と尾行が開始された。更に同年 11 月には二人のホテルでの密会（性関係）の様子をビデオに収録。同月レオンが中国訪問のためロサンゼルス空港から出国した際には、空港で預入手荷物の秘密捜索を実施して、レオンが中国に提供するため持参した書類と FBI 捜査官の写真 6 枚を発見記録した。2 週間後に帰国の際にも、乗継のサンフランシスコ空港と目的地ロサンゼルス空港の 2 か所で預入手荷物の秘密捜索を実施して、FBI 捜査官の写真がなくなっている（中国側に提供された）ことを確認した。この後二人は取調べを受け、2003 年 4 月に逮捕された[43]。

ここで注目すべきは、FBI が、通信傍受、自宅への隠しマイクやホテルでの隠しビデオの設置、預入手荷物の秘密捜索など、各種の情報収集（監視）手法を駆使している点である[44]。

（4）潜入調査・囮調査の事例（2005 年 1 月環境テロ「阻止」事例）

テロ対策での潜入調査・囮調査の実例として、2006 年の環境「テロリスト」による爆弾テロの未然防止・検挙事例[45]を見てみよう。

本件は、アンナという女性の秘匿協力者を囮として使った事案である。彼女は 2003 年 17 歳でコミュニティ・カレッジ 2 年生の時、研究の一環として、米州自由貿易協定への反対グループに潜入して研究レポートを作成発表した。これが FBI の目に止まり、FBI の秘匿協力者として働く契約を結んだ。そして、環境問題や動物保護の活動家に

---

[43] レオンが司法取引で有罪を認めて受けた刑罰は、保護観察 3 年、社会奉仕 200 時間、罰金 1 万ドルと極めて軽い。これは、レオンが一流の弁護士を雇う資金を保持していたことや検事の訴訟指揮の不手際が影響しているとされる。

[44] カトレーナ・レオンがスパイとして重要である由縁は、（鄧小平や江沢民は親米で、米国のような民主主義を好ましいと考えているという）多くの偽情報を米国諜報機関に提供して、中国の「韜光養晦」戦術・米国の親中国認識の形成に大きく寄与したことであろう。即ち、2001 年の CIA 分析では、「中国は自由市場経済に向かっており、大規模な国営企業を全て売却するだろう」「中国が米国に経済的に勝つ可能性はなく、例え勝ったとしても中国は、自由市場を擁し平和を愛する民主主義の国になっているだろう」と見ていたのである。今やこの分析が誤りであることは明白であるが、この分析に導く対米工作が実施されていたのである。マイケル・ピルズベリー『China 2049』（日経 BP、2015）249 頁参照。

[45] 茂田忠良『米国の治安と警察活動』（警察政策学会資料第 96 号、2017 年 8 月）36－38 頁（警察政策学会資料ウェブサイト）参照。本事件自体は、「犯意を誘発し、且つ、犯罪の機会も提供する」FBI による囮捜査の典型的悪例とされる。即ち、本事件では、マクデビッドがアンナに対して恋愛感情を懐いたのを利用して、むしろアンナが爆弾テロに誘導したのである。更に、裁判では、アンナは恋愛関係を餌にした犯行誘導を否定し、FBI は関連証拠を隠匿した。この事実が 2015 年に至って判明したため、マクデビッドは減刑されて釈放された。「犯意の無いところに犯意を誘発させた」このような囮捜査は到底容認できないものであろう。但し、ここで注目すべきなのは、FBI による証拠隠匿や法廷におけるアンナの偽証は論外として、資金、アジト、ノウハウなどを FBI が提供していても爆弾テロの共謀罪の成立が認められていることである。

よるテロ情報収集に当たることになった。

2004年夏、アンナは環境問題に関心を持つアナキスト達の集会に潜入し、エリック・マクデビッド当時26歳とその友人2人と知合いになる。2005年2月FBIはある環境テロリストを逮捕したが、同人はマクデビッドの友人であった。そこで、2005年夏にアンナによるマクデビッドへの接近工作が始まる。そして、この工作はマクデビッドと友人2人を加えた合計4人による爆弾テロの計画へと進展する。FBIはこの作戦のためアンナに、資金、移動用の車、犯行準備のための隠れ家を提供し、更に爆発物製造のマニュアルも提供した。当然、車や隠れ家には隠しマイクやカメラを設置し証拠を収集した。そして、2006年1月マクデビッドやアンナら4人が爆発物の材料をスーパーで買った[46]ところを一斉逮捕し、テロを「阻止」したのである。

本件では、FBIが囮を通じて、資金、移動用自動車、アジト、爆発物製造マニュアルまで提供していたが、それでもマクデビッドは主犯として懲役20年を宣告された。また、アンナが起訴されていないことは言うまでもない。

米国ではこのように囮を利用して、且つ資金、アジト、爆弾製造ノウハウまでFBIが提供しても、有罪となるのである。他方、テロ組織に潜入すれば、当然組織からはテロ行為への積極的参加が期待されるのであり、テロ行為やテロ支援行為が潜入工作員としての正当業務行為として刑事責任を免責されるのでなければ、潜入調査は行い得ないのである。このような囮調査や潜入調査は、20 世紀以来の標準手法であるが、我が国では現行法制の下では到底実施しえない情報収集手法であろう。

なお、FBIは2006年当時秘匿協力者1万5千人を運用してテロの抑止に取り組んでいたといわれる[47]。

本章では、テロ対策のための情報収集では、通信傍受、信書開披、秘密捜索、監視機材の設置、潜入調査・囮調査などの手法が世界標準であると述べたが、本節の幾つかの事例で、これが筆者の単なる「体験的推論」であるだけではなく、「実態」でもあることが明確になったと考える。

さてところが、21世紀は更にサイバー空間の問題が出てくるのであり、テロ対策でもサイバー空間にどう対処していくかが重要課題となった。

---

[46] 爆弾テロの共謀とその徴表的行為としての爆弾材料の購入を以て、爆弾テロの共謀罪が成立したものと考えられる。

[47] Trevor Aaronson and Katie Galloway, “Manufacturing Terror: An FBI Informant Seduced Eric McDavid Into a Bomb Plot. Then the Government Lied About It,” *The Intercept,* 20 November 2015, accessed 20 November 2015, https://theintercept.com/2015/11/19/an-fbi-informant-seduced-eric-mcdavid-into-a-bomb-plot-then-the-government-lied-about-it/

第３章　サイバー空間の課題

１　サイバー空間の重要性

（１）サイバー空間の状況（スライド 15 頁参照）

21 世紀の特徴は、サイバー空間が主要な情報空間として登場したことである。今や情報活動の中心はサイバー空間であり、社会活動、文化活動、生産活動、金融取引、政治活動など、あらゆる活動が行われる巨大空間である。且つ、この空間には国境がなく、世界が一体化した情報空間でもある。

その当然の帰結として、テロに関連する情報活動もサイバー空間に移行している。例えば、

○　テロ集団の思想宣伝、リクルート、思想教育

「イスラム国」のダービク（Dabiq）や「アラビア半島のアルカイダ（AQAP）」のインスパイア（Inspire）が有名であるが、ウェブ出版によってテロ集団の宣伝やリクルートが行われている。また、イスラム過激派の説教師アンワル・アルアウラキのウェブ説教によって過激思想に染まる者もいる。

テロ集団の思想宣伝やリクルートは、20 世紀では紙媒体が中心であったが、今や中心はサイバー空間に移っている。サイバー空間における思想宣伝は、紙媒体よりも制作も容易安価であり、読者からのアクセスも極めて容易となった。その結果、ウェブを通じて過激思想との接点が増大している。

○　テロ技術の伝達

次に、テロ技術の伝達であるが、爆弾製造方法などのテロ手法については、20 世紀は地下出版物が主要な伝達経路であった。1950 年代日本共産党の武装闘争時代には『球根栽培法』『栄養分析表』などという名前で本に偽装してテロ技術が伝播された。1970 年代の極左暴力集団「反日武装戦線」による『腹腹時計』は都市ゲリラ教本として有名である。しかし、これらの出版物は作成に手間暇がかかり、且つ何人でもアクセスできる訳ではなかった。

ところが現在は、サイバー空間にアクセスすれば爆弾製造法や車両を使ったテロの方法など、テロ技術へのアクセスは極めて容易である。特に 2010 年インスパイア第 1 号に掲載された「ママのキッチンで爆弾を作ろう」という記事は有名で、2013 年のボストン・マラソン爆破テロ事件の犯人も同記事から「圧力鍋爆弾」の知識を得たとされる。

○　テロの計画立案、準備

テロの計画立案、準備でもサイバー空間が役立っている。サイバー空間のお蔭で日々の生活における情報収集は極めて容易になったが、それと同様にテロの企画立案のための情報もサイバー空間で容易に収集できるようになったのである。例えば、テロの標的の調査では、嘗ては事前に何回も現地を調査して、テロ計画を立案する必要があ

った。ところが現在では、グーグルマップやグーグルアース、ウィキマピア[48]などを利用して相当の調査ができる。実際の下見の回数は最低限に減らしてテロの事前準備ができるようになったのである。

○　テロの実行の際の通信連絡

テロの実行の際の通信連絡でもサイバー空間を利用できる。

2008 年にラシュカル・エ・タイバいう過激派がインドのムンバイで同時多発的に極めて凶悪なテロを敢行した。その際実行犯 10 人はパキスタン・カラチの本部から携帯電話を通じて、リアルタイムで音声指示（激励、情報提供と作戦指示）を受けていたが、その電話通信は VoIP のインターネット通信網を利用したものであった[49]。

○　活動資金調達

テロ組織やテロ支援組織は、その資金調達にインターネットを利用している。

○　サイバーテロ

そして、遂には攻撃自体がサイバー空間でも実行されるようになっている。「イスラム国」のハッキング部隊「Cyber Caliphate」が積極的に攻撃を仕掛けていたのはよく知られている。

このようにサイバー空間が世界で主要情報空間となるのに従って、テロ関連活動もサイバー空間に移行しているのである。

従って、当然テロ対策もサイバー空間において進めなければいけないこととなる。

（２）テロ対策諸機関（スライド 17 頁参照）

ここで、テロ対策に当たる主要機関を確認しておきたい。

テロ対策には、警察機関のみならず、出入国管理、金融監督など様々な機関が関係してくる。しかし、主要機関は何かと尋ねた場合、我が国では、警察機関しか頭に浮かばない者も多いのではないかと思われる。ところが、世界の多くの国では、インテリジェンス機関もテロ対策の主要機関なのである。

インテリジェンス機関は、セキュリティ・サービスの他、対外諜報のヒューミント機関、シギント機関、イミント機関、そして軍諜報機関、通常この五つが基本単位である。我が国でインテリジェンスというと、対外諜報のヒューミント機関ばかり念頭

---

[48] 2008 年 11 月ムンバイ同時多発テロ事件では、襲撃場所の事前調査にグーグルマップ、グーグルアースなどウェブ情報が利用されている。本事件は、パキスタン・カラチから海上侵入した実行犯 10 人が、2 人一組となってカラチの本部から指示を受けながら、鉄道駅、ホテル、病院、レストランなどを自動小銃、手榴弾、時限爆弾等で襲撃して、死者 160 人以上、負傷者 300 人以上を出した凶悪な事件である。

[49] Mumbai Terrorirst Attacks (Nov., 26-29, 2008) - Dossier of evidence, January 2009, *The Hindu,* http://hindu.com/nic/dossier.htm. カラチの本部はニュース報道などで得た情報を基にして、実行犯に対して、作戦情報を提供すると共に作戦指示と激励を与えている。なお、本件では未然防止はできなかったものの、事案解明にはシギント情報が貢献している。茂田忠良『米国国家安全保障庁の実態研究』（警察政策学会資料第 82 号、2015 年）120－122 頁参照。

に置く者が多いようであるが、現実は異なるのである。

テロ対策では 20 世紀以来セキュリティ・サービスの役割が重要である。セキュリティ・サービス[50]とは、国内で国家安全保障関係の情報収集を担当する組織で、米・FBI 国家安全保障局、英・セキュリティ・サービス、独・連邦憲法擁護庁、仏・対内安全保障総局などがある。通常、警察同様に治安担当大臣の指揮下にある。即ち、20 世紀のテロ対策は、治安担当大臣の下に警察機関とセキュリティ・サービスが主要機関として相互に協力しながら取り組んできたのである。その協力分担では、セキュリティ・サービスは、先に紹介した通信傍受、信書開披、秘密捜索、監視機材の設置、潜入調査・囮調査などの手法を使って情報収集に当たるのが通常であった。

ところで、1970 年代からテロが国境を越え、国際テロの色彩を強くするのに従い、テロ対策でも対外諜報機関の関与が増大してくる。米国でいえば、ヒューミント機関の CIA 中央諜報庁、シギント機関の NSA 国家安全保障庁である。特に、先述したようにテロ関連活動がサイバー空間に移行してくると、サイバー空間を主戦場とするシギント機関の重要性が増大してくる。

（３）シギントの重要性（スライド 18 頁参照）

今や、シギント組織は、テロ対策の主要機関である。特に、米国シギント機関 NSA の役割は重大となっている。

それについて、米国の元国家テロ対策センター長マイケル・ライターは、「NSA が傑出した（preeminent）或いは中心(central)選手（player）でなかったテロ調査というのは思いつかない」と言い、また「NSA ほどアルカイダの内部状況について知見（insight）を与えてくれたものはなかった」とまで語っている[51]。

一部の米国の研究者は 9.11 同時多発テロを分析して、シギントだけでは駄目でヒューミントがなければ十分なテロ対策はできないと述べている[52]。これに影響されたのか、テロ対策の主体はヒューミントであると我が国でも述べる者がいるが、シギントの情報収集力やテロ対策で挙げてきた成果を踏まえた上での認識とは考えられない。アルカイダ対策の歴史をみれば、NSA こそがアルカイダ対策の中心選手であり傑出した役割を果たしてきたが、その NSA ですら 9.11 を予知することは出来なかったとい

---

[50] セキュリティ・サービスの主要任務は、スパイ対策（Counter-Intelligence）、政府転覆活動対策（C-Subversion）、テロ対策（C-Terrorism）、大量破壊兵器拡散対策（C-Proliferation）、個人の適格性調査である。元来警察の一部門であったが、その任務の特殊性・専門性から警察から分離した国が多いが、今でも警察の一部門としている国も多い。

[51] Dana Priest, “NSA growth fueled by need to target terrorists,” *The Washington Post,* 21 July 2013, last accessed 29 March 2020, https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

[52] Matthew Aid, “All Glory is Fleeting: Sigint and the Fight Against International Terrorism,” *Intelligence and National Security,* Vol. 18, No.4 (Winter 2003)

うことなのである[53]。シギント能力なしでも、ヒューミントに注力すればテロ情報が取れるということでは決してないのである。

NSA が如何にテロ対策に注力してきたかは、各種公表資料、機密開示資料から明白である。1970 年代に国際テロの増加と共に NSA も取り組み始め[54]、1980 年代には時のレーガン大統領の指示もあり更にテロ対策に注力するようになった[55]。漏洩された米国の極秘文書「2007 年シギント戦略的任務リスト」では、テロ対策が NSA のシギント任務の第 1 番目に記載されているのである[56]。

それでは次に、NSA が如何にしてテロ情報収集の中心選手となっているのか、NSA の情報収集力の基盤を簡単に見ていこう。

２　NSA と UKUSA シギント同盟

現在、世界のテロ対策で、重要な役割を果たしているのが、UKUSA 協定に基づく米英加豪ニュージーランド 5 ヶ国のシギント協力である。この協力関係は米国シギント機関 NSA を中心とするものであるが、余りにも強固であり強力な関係であるので、「シギント同盟」と呼んでも差し支えないと考える。

それでは、このシギント同盟と情報収集力について、テロ対策を理解するため、骨格を説明する[57]。

（１）UKUSA シギント同盟と収集態勢

ア　UKUSA シギント同盟[58]（スライド 20 頁参照）

---

[53] この経緯については次を参照。茂田忠良「オサマ・ビンラディンを追え（上）」『現代警察』第 156 号（2018 年 4 月）18-26 頁。同「オサマ・ビンラディンを追え（下）」『現代警察』第 157 号（2018 年 7 月）36-41 頁。

[54] US NSA/CSS, *60 Years of Defending Our Nation*, 55,74, last accessed 29 March 2020, https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/nsa-60th/NSA-60th-Anniversary.pdf?ver=2018-08-07-102513-607

[55] Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, BookIV : Cryptologic Rebirth, 1981-89* (Center for Cryptologic History, 1999), 345-360, last accessed 29 March 2020, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB426/docs/2.American%20Cryptology%20During%20the%20Cold%20War%201945-1989%20Book%20IV%20Cryptologic%20Rebirth%201981-1989-1999.pdf

[56] 茂田『実態研究』29 頁参照。

[57] 本節の記述は、基本的に茂田『実態研究』第 1 部、第 2 部に拠っている。

[58] NSA, *UKUSA Agreement Release 1940-1956,* accessed 2 May 2016, https://www.nsa.gov/public_info/declass/ukusa.shtml
--NSA, “Six Decades of Second Party Relations,” Cryptologic Almanac 50th Anniversary Series, updated 28 February 2003, accessed 6 May 2016, https://www.nsa.gov/news-features/declassified-documents/crypto-almanac-50th/assets/files/six_decades_of_second_party_relations.pdf
--Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book I: The Struggle for Centralization, 1945-1960* (Center for Cryptologic History, 1995), 19, accessed 5 May 2016, https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_i.pdf

UKUSA 協定の前身は、第二次世界大戦時の米英のシギント協力関係である。

米英は、1940 年 4 月に対日独伊の戦争を前提として諜報協力を開始した。次に、1940 年 12 月シギント面の協力でも合意をして、1941 年 2 月から実務レベルでの協力が始まる（欧州ではロンドン、極東ではシンガポールで開始）。協力関係には、カナダ、豪州、ニュージーランド（以下、NZ と略称する）も英連邦の一部として参加している。

この協力関係は大戦で大きな成果を挙げたので、大戦後も協力関係を維持することとなり、1946 年 3 月に BRUSA（British-USA）秘密協定が締結され、1954 年に英国の申出により UKUSA（UK-USA）協定と改称された。

カナダの正式加盟は 1949 年、豪州と NZ は 1956 年であるが、協力関係自体は英連邦の一部として大戦中から戦後も継続していた。国としての正式加盟が遅れたのは、米国がカナダと豪州の秘密保全体制に疑念を持ち、秘密保全体制が向上するまで正式加盟を待たされたためである。

イ　米国 NSA（スライド 21 頁参照）

UKUSA シギント同盟の中心は、米国のシギント機関、国家安全保障庁 NSA である。2013 年のスノーデン漏洩資料によると、当時の NSA の職員は 3 万 5000 人であった。2018 年の報道によると、正規職員 3 万 8000 人、契約職員 1 万 7000 人で合計 5 万 5 千人である[59]。米国では NSA の他に陸海空軍、海兵隊、沿岸警備隊も作戦支援のためのシギント組織を持っており、これらは NSA に附置された CSS（Central Security Service）傘下で一体的に運用されている。

予算面は、NSA 単体では 100 億ドル程度であるが、国家偵察局や各軍シギント組織の予算を加えると、シギント関係予算の総額は、200 億ドル 2 兆円程度にはなると推定できる。正に、巨大組織である。

ウ　英・加・豪・NZ のシギント組織 Second Party（スライド 22 頁参照）

UKUSA 協定の米国外の 4 ヵ国、英・加・豪・NZ は Second Party と呼ばれる。英・政府通信本部 GCHQ 約 6000 人、加・通信安全保障局 CSE 約 2000 人、豪信号局約 2000 人、NZ・政府通信安全保障局 430 人である。

UKUSA 諸国の協力関係について、各種スノーデン漏洩資料から読み取れるのは、５つの国の５つの互いに独立した機関が相互に協力している関係というよりは、共同の収集分析、共同のシステム構築など統合運用の段階にあり、米 NSA 指導下に 5 機関

--NSA, *New UKUSA Agreement - 10 May 1955*, accessed 2 May 2016, https://www.nsa.gov/news-features/declassified-documents/ukusa/assets/files/new_ukusa_agree_10may55.pdf
特に、本資料中の 1956 年改訂の Appendix J1 を参照。

[59] Ellen Nakashima, "Senate confirms Paul Nakasone to lead the NSA, U.S. Cyber Command," *The Washington Post,* 24 April 2018, last accessed 24 March 2020, https://www.washingtonpost.com/world/national-security/senate-confirms-paul-nakasone-to-lead-the-nsa-us-cyber-command/2018/04/24/52c95ca4-47e8-11e8-9072-f6d4bc32f223_story.html?utm_term=.b0afce22d9f1

が殆ど一体として運用されているように伺われる。但し、全データ・全情報にアクセスできるのは NSA のみで、他の国々はそれぞれの貢献度に応じて情報成果を得られる関係のようである。

エ　民間協力企業（Special Source Operations）（スライド 23 頁参照）

特別資料源作戦 Special Source Operations は、民間企業の協力を得て行うシギント資料収集活動である。NSA の収集データではコンテンツ情報の 60%、メタデータの 75%近くは、民間企業の協力を得て収集しているとされる。

オ　Third Party 諸国（スライド 23 頁参照）

2013 年スノーデン漏洩資料によれば、Third Party33 ヶ国がシギント資料収集に協力している[60]。

Third Party 諸国は、UKUSA 諸国からみれば、協力者であり、同時に情報収集の標的でもある。協力関係がどこまで密接か、どこまで標的とされているかは、両国関係、即ち米国・UKUSA 諸国と Third Party との関係で決まってくる。

カ　収集態勢

NSA は巨大であるが、それにしても単独では世界を覆うシギント・データの収集態勢は構築できない。UKUSA 同盟の Second Party 諸国、民間企業、Third Party 諸国の協力関係を活用して、世界を覆うシギント資料収集システムを構築している。

スノーデン漏洩資料を詳細に分析している米国研究者によると、米国シギントの通信傍受施設は、第二次世界大戦以来現在まで全部合わせると 2000 以上あるが、その内 2013 年現在運用されているのは約 500 である[61]。その中でも主要なサイトは約 150 ヵ所と推定できる[62]。

（２）収集プラットフォーム（スライド 24 頁参照）

UKUSA シギント同盟の情報収集システムは世界中に広がっているが、主要な収集

---

[60] スノーデン漏洩資料によれば、2013 年現在のアジアにおける NSA の主要な協力国は、シンガポールと韓国である。

[61] “SIGINT Activity Designators(SIGADs),” *Electrospaces,* updated 27 June 2019, accessed 24 March 2020, http://electrospaces.blogspot.jp/p/sigint.html
本サイトの分析によれば、2013 年現在で世界中に 504 の運用中の傍受施設がある。一つの傍受施設は必ずしも一つの傍受サイトではなく、複数のサイトを持つものもある。従って、収集サイトということになれば実際は 500 ヵ所以上となる。

[62] 推定の根拠は次の通り。即ち、XKeyscore という NSA にとって重要な世界中を覆うシステムがある。これは、収集データの一次的記憶装置であると同時にデータ検索用のシステムでもあある。この重要システムのサーバーの設置個所が世界中で 150 ヵ所と下記のスノーデン漏洩資料に記載がある。重要なサーバーが世界中で 150 ヵ所に設置されている訳であるから、重要な収集サイトも 150 ヵ所はあると推定できる。
--ス資料：NSA、*XKEYSCORE,* 25 February 2008, last accessed 24 March 2020, http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

システムは次の通りである。

○「プリズム」（Downstream）

○　通信基幹回線からの収集（Upstream）

○　外国衛星通信の傍受（FORNSAT）

○　特別収集サービス（Special Collection Service）

○　コンピュータ網資源開拓 Computer Network Exploitation

○　シギント衛星・機上収集（Overhead）

○　従来型 Conventional：短波や超短波の無線通信傍受。

○　秘匿シギント活動 CLANSIG（clandestine sigint）：内容は殆ど不明

データ収集量では上記の最初の五つが多いようであり、この五つについて簡単に説明する。

ア　「プリズム」計画 Downstream（スライド 25 頁参照）

「プリズム」は、民間企業の協力を得て行う特別資料源作戦の一種であり、米国内の企業のデータセンターから必要な情報を収集するものである。協力企業は、マイクロソフト、ヤフー、グーグル、フェイスブック、パルトーク、ユーチューブ、スカイプ、AOL、アップル。特に情報源として重要なのが、ウェブメール（Gメール、ヤフーメール、ホットメール）である。

米国政府の公表資料によれば、2013 年中に 2 億 5000 万件以上のデータを取得している[63]、[64]。

イ　通信基幹回線からの収集 Upstream（スライド 26 頁参照）

世界中の通信基幹回線からデータを収集している。これには多数の収集計画が含まれており、膨大なデータを収集している。

第 1 は、企業協力による収集計画である。米国内における収集計画は「ブラーニー」「フェアビュー」「ストリームブリュー」の三つがある。法的根拠は対外諜報監視法第 105 条によるもの、同第 702 条によるもの、大統領命令第 12333 号「合衆国諜報活動」のみによるものがある。「ブラーニー」は主として対外諜報監視法第 105 条によ

---

[63] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), 3 October 2011, released 21 August 2013, updated 16 July 2014, last accessed 24 March 2020, https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. 本資料によれば、第 702 条によるデータ収集は、プリズム計画と通信基幹回線からの収集の二つあり、通信データの取得件数は合計 2 億 5 千万以上であるが、その内通信基幹回線からの収集は全体の約 9 %で 2011 年 1 年間で約 2650 万件と推定している。これから推計すると、プリズム計画による通信データ収集件数自体が 2 億 5 千万件程度と推定できる。

[64] 因みに、2013 年のスノーデンによる情報漏洩時の報道で興味深いものに、「これで米国企業は断れなくなる」という報道があった。即ち、米国外にあるデータセンターに関して、所在国当局からデータ提供の協力を要請されたときに断れなくなるということである。「米国政府に対すると同様に、我が国にも協力してして欲しい」と要求された時に断れなくなる、というものである。「プリズム」の暴露報道以来、何年も経過している現在、日本以外の多くの国が「プリズム」と同じ方法でデータ収集をしていると推定できる。

る個別対象の行政傍受で、30 社以上の企業が協力している。この三つの外に「オークスター」があるが、大統領命令第 12333 号「合衆国諜報活動」による殆ど国外での収集計画である。

第 2 は、UKUSA 諸国(Second Party)と Third Party の協力による収集計画である。UKUSA 諸国の協力事業が「ウィンドストップ」、Third Party の協力事業が「ランパートＡ」で、それぞれに多くの小計画が含まれている。法的根拠は何れも大統領命令第 12333 号「合衆国諜報活動」である。

第 3 は、単独事業で「ランパート I/X」「ランパートM」「ランパートＴ」など五つの計画があるが、殆ど内容不明である。内容が判明しているのは「ミスティック」計画であるが、米国麻薬取締局 DEA や CIA その他の協力を得て、勝手に他国の通信システムから情報を取得できるススステムを設置している。

ウ　外国衛星通信の傍受 FORNSAT（スライド 27 頁参照）

外国衛星通信の傍受は、世界中に主要傍受施設 12 ヵ所を設置している。設置場所は、米英豪 NZ の本国内、英国の海外領土、その他オマーン、日本、フィリピンとタイである。また、次に述べる特別収集サービス約 40 ヵ所でも収集している。世界各地の米国の大使館や領事館から秘密裡に傍受しているのである。

エ　特別収集サービス Special Collection Service（スライド 28 頁参照）

特別収集サービスは CIA と NSA の共同事業で、1977 年以来の長い歴史がある。米国大使館や領事館に秘匿アンテナを立てて、通信傍受をしている。2010 年現在、世界 80 ヵ所で、衛星通信、マイクロ波、Wi-Fi 通信など無線 LAN、携帯電話などを対象として各種アンテナを設置して収集している。

オ　コンピュータ網資源開拓 Computer Network Exploitation（スライド 29 頁参照）

コンピュータ網資源開拓は、一言で言うと、ハッキングであり、コンピュータネットワークに入り込んで各種情報を取っている。2011 年現在で 7 万件近くの侵入に成功しているが、人手不足のため実際に運用して情報を収集していたのは 8448 件であった。そこで NSA では操作員不要の自動運用システムを開発中であった。

以上で略記したように、NSA・UKUSA シギント同盟の情報収集態勢は世界を覆っている。世界を覆うシギント・システムを如何にテロ対策し使用しているのかを次に見てみよう。

３　シギントによるテロ対策：使用可能なシギント能力（スライド 16 頁参照）

前節では、NSA と UKUSA シギント同盟のデータ収集プラットフォームが全世界を覆っており、卓越したシギント能力を構築していることを略述した。そして、NSA がこのシギント能力を国際テロ対策に指向して成果を挙げてきたことは前々節で述べた通りである。

それでは UKUSA シギント同盟諸国は、国際テロ対策でシギント・システムを具体

的にどのように使用しているのであろうか。サイバー空間におけるテロ容疑者の発見、監視、追跡活動をどのように実施しているのであろうか。

この点については、残念ながら、ウィリアム・スノーデンが漏洩した内部機密資料の記述は断片的であり、シギント・システムのテロ対策使用の全体像を包括的に記述した資料は見当たらない。そこで、シギント能力の中からテロ対策に使用できるものを次に記述する。シギント能力の全体像については、拙著『米国国家安全保障庁の実態研究』[65]で分析したので、詳細は同書を参照されたい。

テロ対策へのシギント使用としては、テロリストの捕捉殺害など攻撃面を別とすれば、テロ容疑者の容疑解明（Target Development）とテロ容疑者の発見（Target Discovery）の二つに分類できる。更に後者は既知のテロ関係者から手繰って発見する場合と、サイバー空間における行動分析から発見する場合の二つがある。それぞれについて、使用可能なシギント能力は次の通りである。

（1） テロ容疑者の容疑解明（Target Development）

先ず、テロ容疑者（既にテロリスト又はテロ支援者としての容疑があり関心対象となっている者）の容疑解明である。どれ程過激思想にのめり込んでいるのか、本当にテロを行う容疑性が高いのかなどにについて解明し、もし、容疑性が高い場合にはテロ抑止のため行動を追跡監視することである。

ア 通信傍受による通信内容分析

容疑者の使用するパソコンやスマートフォンなど通信機器を傍受して、その通信内容から、容疑を解明することができる。G メールやヤフーメールなどのウェブメールは「プリズム」[66]で容易に監視することができる。また通常の E メールについても「ブラー二一」その他通信基幹回線や衛星通信などのデータ取得で相当の監視が可能である。

対象者が通信傍受を嫌って、TOR 通信や PGP 暗号通信などを使用すれば、使用方法や頻度によって、これも本人の容疑性推定の指標とできる。

なお、容疑者が通信保全を徹底すれば容疑解明は困難であるが、オサマ・ビンラディン捕捉作戦でもその側近の不注意な通話からオサマ発見に至る重要情報が取得されている[67]。テロ容疑者の通信保全も完璧である訳ではない。

イ ネットワーク閲覧履歴や SNS による人物分析（メタデータ分析）

---

[65] 茂田忠良『米国国家安全保障庁の実態研究』（警察政策学会資料第 82 号、2015 年）（警察政策学会資料ウェブサイト）

[66] 米国外居住者も G メールなどのウェブメールを多用し、「プリズム」ではその通信も多く捕捉できたために極めて有効であった。但し、スノーデン情報漏洩によって米国関係ウェブメールやメッセージ・アプリの信頼性が低下し、現在 Telegram Messenger という非米国系の暗号化メッセージ・アプリが普及しつつあり、テロ対策における「プリズム」の有効性が低下していると言われている。

[67] 茂田「オサマ・ビンラディンを追え（下）」37 頁参照。

メタデータ分析[68]によって、ウェブサイトの閲覧履歴や E メール・SNS の交信履歴を分析することにより、当該人物の交友関係、団体活動履歴、何時何処で誰と会ったかなどを把握することができる。

これに、FBI などのセキュリティ・サービス機関が収集できる銀行口座情報、保険情報、旅客名簿、選挙人名簿、財産情報、税務情報などを加えれば、当該人物の全体像を把握することができる[69]。

ウ　携帯電話やスマートフォンを使用した行動監視（位置情報分析）

NSA のデータベースの一つに位置情報を集めた FASCIA[70]がある。これは携帯電話接続のために通信事業者が常時取得している位置情報やスマートフォンに対するネットサービスのために取得している位置情報を各種の方法で収集して構築したデータベースである。これを使うことにより、容疑者の移動状況を人が尾行することなしに監視することができる[71]。

エ　スマートフォン攻略による行動監視[72]（ハッキング）

更に、容疑が深まった人物については、同人のスマートフォンをハッキングすることにより、記録内容を取得したり、或いは、スマートフォンのカメラやマイクを遠隔で捜査して監視機材として使用することができる。

以上が、スノーデン漏洩資料からみえるシギント能力のテロ対策への適用の例である。なお、これらシギント能力によって容疑者の容疑を完全解明する必要はないので

---

[68] 通信メタデータとは、(通信内容を除く)通信に付随するデータ全てである。具体的には、携帯電話通話であれば、通話当事者の電話番号、携帯端末識別番号（IMEI)、利用者識別番号(IMSI、シムカードに記載）、回線識別符号、通話日・時刻、通話時間、テレホンカード番号、携帯端末位置データ等である。また、インターネット通信であれば、当事者のメールアドレス、IP アドレス、通信日・時刻、通信時間。SNS 通信では通信内容以外のデータ、ネットワークに於ける活動履歴（訪問ウェブサイト、ログイン時刻、地図検索履歴等）、その他各種のデータが該当する。NSA はメタデータ専用のデータベースを構築して世界中から収集したメタデータの分析に役立てている。茂田『実態研究』105,107 頁参照。

[69] FBI は国家安全保障書簡（National Security Letter:NSL）という行政命令によって相当の民間業務情報を取得することができる。また、政府他機関の保有する行政情報の取得に関しては基本的に制限がない。

[70] 茂田『実態研究』107-110 頁参照。

[71] これらの諸システムは高度な監視システムのようにも見えるが、共産中国は更に進んだ監視システムを構築している。中国専門家の遠藤誉氏によれば、中国の全人民には身分証番号が付与されているが、この番号には全ての個人情報（生年月日、両親の名前・職業、持ち家、貯金残高、借金、車の種類・ナンバー等の財産、犯罪歴、学歴、職歴、趣味、電話番号、交流関係、購買動向など）が紐付けられており、当局者は身分証番号により全て閲覧可能である。更に、中国全土の監視カメラ（約 2 億台といわれる）には顔認識機能が付加されているが、この情報も身分証番号に紐付けられているため個人の位置移動状況も把握可能である。（遠藤誉「中国の無症状感染者に対する扱い」中国問題グローバル研究所、2020 年 3 月 26 日、同日閲覧、https://grici.or.jp/1272）　中国は、この他サイバー空間にも極めて高度な監視システムを構築しており、中国のいうウィグル族による「テロ抑止」にも大きく貢献しているものと考えれる。

[72] 茂田『実態研究』85－87 頁、147-155 頁参照。

ある。容疑性が深まれば、その先はFBIやその他セキュリティ・サービスが、住居の秘密捜索、預入手荷物の秘密捜索、住居内への監視機材の設置、潜入調査・囮調査などの手法も駆使して、更に容疑の解明に当たることができるのである。

（２）容疑者発見（Target Discovery）～既知の関係者から

次に既知のテロ容疑者から出発して、その交友関係から未把握のテロ容疑者を発見する手法である。最も有名なものは接触連鎖分析である。

ア　接触連鎖分析（contact chaining）[73]

メタデータ分析の一手法に、接触連鎖分析という手法がある。これは、誰が誰と直接又は間接に連絡を取り合っているかを、収集したメタデータから自動的に分析する手法で、自動的に人物相関図が作成できる。これによって、既知の容疑者を取り巻く関係者の相互連絡関係が自動的に検出できるのである。

9.11同時多発テロに関して、この接触連鎖分析をしていれば、テロ実行集団を早期に発見できていた可能性が指摘されている。

イ　同伴者分析（co-taravel analytics）[74]

位置情報データベースFASCIAを使用した分析方法の一つで、携帯電話やスマートフォンの位置情報を分析することにより、一定期間中に特定の既把握テロ容疑者と類似の行動をとる者（即ち位置情報が一致する携帯電話）を検出することができる。位置情報の一致度をどれ程に設定するかは分析官の裁量が可能である。

ウ　通信コンテンツからの容疑者発見（通信内容分析）

既知の容疑者のメールや通話を通信傍受により監視することにより、その通信相手や通信内容から新たな容疑者を発見することができる

（３）　容疑者発見（Target Discovery）～行動探知技術から

現在は、ローンウルフ型のテロが増加している。これは、特定のテロ関係者からの直接的影響ではなく、サイバー空間における思想宣伝に感化されて自ら過激化してテロに至る者である。この発見は極めて難しく各国のセキュリティ・サービス機関に大きな挑戦を突き付けている。

そこで、テロ容疑者の発見では、既知の関係者から手繰って発見するだけではなく、サイバー空間における特定の行動を探知してそこから発見しようとする技法（行動分析）が発展している。その幾つかを次に見てみよう。

ア　エックスキースコア[75]**使用による行動探知**

---

[73] 茂田『実態研究』106頁参照

[74] 茂田『実態研究』109-110頁参照

[75] エックスキースコアとは、NSAが世界中で収集したシギント・データの一次記憶装置であり、同時に、同装置から必要なデータを検索抽出するための分析システムである。NSA版「グーグル」とも言われている。システムの詳細については、茂田『実態研究』115-122頁

エックスキースコア X-Keyscore は NSA 版「グーグル」とも呼ばれるシステムであり、極めて利用価値が高い。不特定者がインターネット空間において行う様々な行動を捕捉し分析することより、テロ容疑者の発見に貢献できる。例えば、

○　特定の過激なウェブサイトを頻繁に閲覧する者を検出抽出する。

○　特定の単語によってウェブ検索をする者を検出抽出する。

○　グーグルマップやグーグルアースの検索状況から、テロ準備の為の調査活動を行っている可能性のある者を検出抽出する。（即ち、テロの標的とされそうな施設を頻繁に検索する者を捕捉する）

○　インターネット空間に流通するテロを使嗾する文書の作成者と作成場所を特定する。

○　特定の地域（例えばパキスタンの危険地域）と頻繁に暗号通信をする者、特定の地域（例えばシリアの「イスラム国」支配地域）から特定言語（例えば日本語）でメール通信をしている者を検出抽出する。

インターネット空間でこのような行動をする者は多数に上る可能性があり、必ずしも一つの行動分析のみによってテロ容疑者を発見できる訳ではないが、NSA などシギント機関は試行錯誤しながら分析アルゴリズムを開発向上させて、テロ容疑者の可能性がより高い者を検出抽出していると考えられる。

スノーデンの漏洩資料によれば、ドイツのセキュリティ・サービス機関である連邦憲法擁護庁 BfV は、取得した通信データの分析のために、米国からエックスキースコアのソフトウェアの提供を受けている[76]。これはそのテロ対策における有用性を示したものと言えよう。

イ　カナダの「レヴィテーション」計画[77]（カナダ CSE）

過激派は、無料ファイル共有サイトを利用して、過激思想の宣伝を行い、更に、爆弾製造教本などテロのマニュアルを拡散させている。そこで、カナダのシギント機関 CSE は、無料ファイル共有サイトの監視によって、テロ容疑者を発見しようとしている。

2012 年時点でカナダ CSE は、世界の 102 の無料ファイル共有サイトの特定部分 2200 ヵ所を監視し、過激ビデオや過激文書のダウンロードを分析して、月に 350 件程度の「興味深い」者を発見し IP アドレスを取得している。これら IP アドレスについて、更にその使用者についてのデータ収集分析を行い、テロ容疑者と判断した場合には、個別にセキュリティ・サービス（カナダ国内の容疑者であれば CSIS）に資料を提供して調査を進めることとなる。

参照。-

[76] 茂田『実態研究』255-256 頁参照

[77] 茂田『実態研究』216-218 頁参照

ウ　「通信保全活動」をする者を発見[78]（FASCIA の利用）

テロ容疑者は監視を逃れるために通信保全を行っている可能性が高いが、これを逆手にとって、携帯端末について通信保全活動をする者を発見することによって、テロ容疑者を発見しようとするものである。

具体的には、位置情報データベース FASCIA を使用して、次の行動をする者を抽出しようとしている。即ち、

○　通話時だけ電源を入れる者（逆に言えば、頻繁に電源を切る者）

○　幾つかの携帯電話を使い分ける者（一つの携帯電話の電源を切り、近くで別の携帯電話の電源を入れる行動）

○　会合地点近くで電源を切る行為（近くで複数の携帯電話の電源が相前後して切られる）

○　使い捨て携帯電話の使用

これらの行為を自動的に検索するシステムがあると言われる。

本節では、NSA のシギント・システムの中から、テロ対策に使用されていると合理的に推定できるものを記述した。これ以外にも、テロ対策に使用できるシギント・システムがある可能性はあるが、以上見ただけでも、テロ対策に占めるシギントの重要性が理解できるのではないかと考える。

４　シギントによるテロ対策：具体例

今まで、①テロ関連活動ではサイバー空間が重要な活動空間となっており、従って、テロ対策でもサイバー空間への取組が重要であること、②このサイバー空間に対して米国 NSA を中心とする UKUSA シギント同盟がどのような情報収集態勢を構築しているか、③その情報収集態勢を基礎にテロ対策で使用できるシギント・システムにはどのようなものがあるかについて、述べてきた。

そこで次に、本シギント・システムのテロ対策に対する貢献の実態を、具体的事例を通じて確認したい。

ところで、本来シギントの収集態勢自体が秘密事項であり、テロ対策における具体的な活用実態も秘密事項である。従って、従来政府公刊資料もなく、その実態を知ることは困難であった。ところが、2013 年のスノーデンによる NSA 機密資料漏洩によって、UKUSA シギント同盟の広汎な収集態勢が暴露され、驚いた国民から厳しい批判が巻き起こった。そこで、米英政府は、そのシギント収集態勢を維持するため（新規立法に際しては必要性を疎明するためにも）、テロ対策へのシギント情報貢献事例について一定の情報開示を余儀なくされたのである。

---

[78] 茂田『実態研究』109 頁参照

斯かる資料中、特に重要な資料には次の資料がある。米英政府は、これら資料の中で、シギント情報によって多数のテロを阻止したと報告している。

○　米国：「プライバシーと市民的自由監視委員会」『対外諜報監視法第 702 条に基づく監視プログラムについての報告書』2014 年[79]

○　英国：内務省『包括的収集権限のための事例』2016 年[80]

勿論、これらの資料でも、最も秘匿したい部分は開示していないと考えられる。また、そもそもこれら資料は、シギントによるテロ対策の全体像を記述したものではない。米国資料は対外諜報監視法第 702 条に基づく収集情報、英国資料は「包括収集」とよぶ収集情報についてのみの資料である。しかしながら、一部であってもこれら資料はシギントによるテロ対策の一端を伺うため貴重な手掛かりを提供している。

これら資料と、関連事件の広報資料、宣誓供述書その他の情報を総合して具体的事例において、シギント情報がどのような利用されているか、実態を見ることとする。

（１）2009 年ニューヨーク地下鉄同時爆破テロ未遂事件[81]（スライド 31 頁参照）

---

[79] USA, PCLOB（Privacy and Civil Liberties Oversight Board）, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,* 2 July 2014, pp. 107-110, last accessed 4 September 2019, https://www.pclob.gov/library/702-Report.pdf

この他にも対外諜報監視法 702 条に関する次の資料も興味深い資料である。

-- ODNI, *The FISA Amendments Act: Q&A,*18 April 2017, last accessed 4 September 2019, https://www.dni.gov/files/icotr/FISA%20Amendments %20Act%20QA%20for%20Publication.pdf

-- ODNI, *Section 702 Overview,* late December 2017, last aeecessed 4 September 2019, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf

[80] UK, Home Office, *Operational Case for Bulk Powers*, 1 March 2016, last accessed 4 September 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf. 本資料は 2016 年調査権限法案の審議資料として内務省が英国議会に提出したものである。

[81] PCLOB, op. cit.の他、次の資料参照。

--USA, DoJ Press Release, “Najibullah Zazi Pleads Guilty to Conspiracy to Use Explosives Against Persons or Property in U.S., Conspiracy to Murder Abroad, and Providing Material Support to Al-Qaeda,” 22 February 2010, accessed 9 September 2019, https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo022210.htm

--Garrett Cumbinner,"Affidavit in Support of Complaint and Arrest Warrant; U.S. v. Zazi," 19 September 2009, accessed 21 March 2020, http://www.nefafoundation.org/miscellaneous/FeaturedDocs/US_v_NajibullahZazi_complaint.pdf

--Benton J. Campbell, "Memorandum of Law in Support of the Government’s Motion for a Permanent Order of Detention; U.S. v. Zazi," 24 September 2009, accessed 21 March 2020, https://www.justice.gov/archive/usao/co/news/2009/September09/Zazi_Detention_Motion.pdf

ニューヨーク市地下鉄における同時 3 ヵ所の自爆テロを阻止した事例である。敢行されていれば、2005 年ロンドン同時爆破テロ（死者 56 人、負傷者約 700 人）に匹敵する 9.11 以来の大被害をもたらす事件であった。

NSA は米国内から FISA702 条（プリズムと推定）に基づき、パキスタンを拠点とするアルカイダ連絡員の E メールアドレスを監視していた。すると 2009 年 9 月初めに米国内の不明人物からのメールを何度も捕捉した。メールは隠語を使い内容を秘匿していたが、TATP（過酸化アセトン）爆弾作成に当たり配合する化学薬品の詳細について緊急に助言を求めていると推定できたので、FBI に通報した。FBI は国家安全保障書簡（NSL：National Security Letter）を発出して情報を収集し、当該人物をコロラド州居住のナジブラ・ザジと特定した。

ザジは、アフガニスタン生まれで 10 代で米国に移住し米国永住権を持っているが、インターネットで過激派アンワル・アル・アウラキ師の説教を聞き過激なイスラム思想に傾斜した。2008 年夏ザジは米国と戦う為に仲間（高校同級生）2 人と共にアフガニスタンに向かったが、途中のパキスタンでアルカイダに勧誘され参加した。同地のアルカイダ訓練場で各種戦闘訓練を受けたが、アルカイダ指導者から米国での自爆攻撃を要請され承諾した。その後、爆弾作成の訓練を受け攻撃目標について協議し、2009 年初米国に戻った。帰国後、ザジは仲間 2 人とニューヨーク地下鉄の同時爆破テロを計画。7 月 8 月には爆弾材料を大量に購入し、8 月末 9 月初めとホテルで爆弾作りに取り組んだ。その後、9 月 9 日にレンタカーに爆弾用の爆薬と部品を積んでコロラド州を出発し、10 日に NY 市に着いた。

NSA は 9 月初めの爆弾作りの際のザジの通信を捕捉した推定できるが、通報を受けた FBI は、捜索（ホテル客室の捜索により爆弾作りの痕跡を把握）や（秘密令状を得て）同人の電話やインターネット活動の監視など、徹底した監視を実行した。ザジは 9 月 10 日にニューヨーク市に着いた際に、交通検問に合ったり、レンタカーを検索されパソコンなど所持品を捜索されるなど、法執行機関に監視されていることを知り、テロを中止して 9 月 12 日にコロラド州に戻った。

コロラドに戻ったザジは、FBI から任意の事情聴取を受けたが、爆弾テロの準備行為について虚偽の供述をしたため、虚偽供述の罪で逮捕された（証拠としては、主にパソコンからの押収データと供述との矛盾が使われている）、後に大量破壊兵器（爆弾）使用の共謀に罪名が変更され、その後の継続捜査により共犯者が解明された。

一連の事案の経緯を見ると、先ず通信傍受により米国内のテロ容疑者を把握し、次に国家安全保障書簡（行政命令の一種）により人定を特定。秘密捜索により爆弾テロ

--Catherine Tsai and P. Solomon Banda, "Timeline of events in NYC terror probe". *Boston Globe*. 21 Septemver 2009, accessed 21 March 2020, http://archive.boston.com/news/nation/articles/2009/09/21/timeline_of_events_in_nyc_terror_probe/

関連資料を押収し且つ電話やインターネット通信を傍受して、テロ準備行動を把握しつつ、示威的な監視活動によりテロ企図を断念させた。その後、ザジの任意聴取を行ったが、既に収集された証拠と矛盾する虚偽の供述をしたこと(嘘偽供述罪)[82]により逮捕に漕ぎ着けたものである。爆弾テロの阻止と犯人逮捕に至る過程で行使された権限（通信傍受、国家安全保障書簡、秘密捜索）や当初の逮捕の犯罪は、何れも我が国には存在しないものである。

（２）他国におけるテロ対策への米国による貢献[83]（スライド 32 頁参照）

米国による通信傍受は、米国内でのテロ抑止に貢献しているのみならず、他国におけるテロ対策へも貢献している。事例二つを紹介する。

ア　他国におけるアルカイダ同調者の発見事例（時期不明）

機関名は不明であるが（NSA と推定）、米国内からの FISA702 条による情報収集によって某国内にアルカイダ同調者を発見した。CIA が当該国政府に通報したところ、同国政府は同人を調査した上で協力者として獲得した。それ以来、同人は同国内のアルカイダと「イスラム国」関係者に関する情報を提供している。

この事例は、CIA が外国政府に対してシギント情報の提供窓口となっている事例である。但し、CIA は情報源を秘匿するためシギント情報であることは開示していないと考えられる[84]。

イ　アフリカ某国での「イスラム国」によるテロ阻止事例（時期不明）

「イスラム国」関係戦闘員 2 名が、米国人と米国権益に対するテロを計画して、トルコからアフリカ某国へ入国したが、その脅威は具体的且つ差し迫ったものだった。これに対して、CIA が 702 条による情報収集（プリズムと推定）によって写真その他詳細な個人情報を入手して当該国に提供したため、当該国当局は 2 名を逮捕した。

2 名の逮捕により、「イスラム国」のテロ支援ネットワークや攻撃計画に関する具体的な情報を得ることができた。

---

[82] 18USC §1001：合衆国法典第 18 篇（刑法・刑事訴訟法）第 47 章（欺瞞・虚偽供述）第 1001 条（虚偽供述：懲役 5 年以下等）。FBI 特別捜査官に対して虚偽の供述をすると犯罪になる。

[83] USA, ODNI, *The FISA Amendments Act: Q&A,* p. 4 参照。

[84] 注目すべきは、外国政府に通報したのが CIA であったことである。シギント情報だからといって NSA が通報窓口になる訳ではない。秘密保全のためにも NSA はシギントで恒常的な協力関係がない国とは関与しない。従って、テロ対策で言えば恒常的にテロ対策で協力関係がない国に対しては、NSA が通報するのではなく、対外的に米国インテリジェンスを代表する CIA が通報することになる。従って CIA がテロ関係情報を提供しても、情報源がヒューミントであるとは限らないのである。本文前述のガイトナーの発言などから考えれば、むしろシギント情報の可能性が高いのである。
茂田『実態研究』第 3 部第 2 章 1 「サードパーティ関係とは？」219-220 頁参照。

（３）2010 年アルカイダ支援者の逮捕[85]

NSA は、FISA702 条に基づき、イエメンを拠点とする過激派の E メールアドレスを監視していたところ、ミズーリ州居住の不明人物との繋がりを発見して、FBI に通報。FBI は調査により、不明人物をカーリド・クアザニと特定し、更に同人と米国内アルカイダ関係者エル・ハナフィとサビルハン・ハサノフとの繋がりを発見し、彼らを逮捕した。

クアザニは、モロッコ生れで米国に帰化していたが、2008 年にはアルカイダに忠誠を誓った。同人は中古車部品販売業を営んでいたが、2007 年 8 月から 2010 年 2 月に逮捕されるまでの間に、事業資金を名目に借り入れた資金を事業外で運用して（銀行には殆ど返済せず）、2 万 3 千ドル以上の資金を送金したほかアルカイダの活動を支援していた。

クアザニの供述から、同人と米国内アルカイダ関係者エル・ハナフィとサビルハン・ハサノフとの繋がりを発見したが、ハナフィとハサノフはニューヨーク証券取引所の爆破計画を立案して調査活動を行ったり（実行は中止）、アルカイダに対する資金や手製爆弾用タイマー（カシオ腕時計）の提供、更に通信傍受を回避するための IT 技術支援を行っていた。

このような事件検挙によって、アルカイダなどのテロ組織に対する支援を制約しているのである。

（４）英国におけるテロ対策への貢献[86]

次に、英国に事例であるが、英国の公表資料では提示されている事例は多いが具体性に乏しい特色がある。そこで、報道等で補いつつ、具体的事例を見ていく。

ア　2006 年ロンドン発北米行き旅客機に対する同時多発爆破テロの阻止[87]

---

[85] PCLOB, op. cit.の他、次の資料参照。
--USA, DoJ Press Release, “Al Qaeda Supporter Pleads Guilty to Supporting Terrorist Organization, 19 May 2010, accessed 21 March 2020, ”https://archives.fbi.gov/archives/kansascity/press-releases/2010/kc051910.htm
--“Plea Agreement ; U.S. v. Quazzani,” accessed 21 March 2020, https://www.wired.com/images_blogs/threatlevel/2013/06/ouazzaniplea.pdf
--Bill Draper, “US man gets 14 years for sending funds to al-Qaeda,” *Times of Israel,* 8 October 2013, accessed 9 September 2019, dhttps://www.timesofisrael.com/us-man-gets-14-years-for-sending-funds-to-al-qaeda/
--Antonio Antenucci and Rich Calder, “Al Qaeda ‘tech-geek’ gets 15 years for plotting attack on NYSE,” *New York Post*, 20 January 2015, accessed 9 September 2019, https://nypost.com/2015/01/20/al-qaeda-tech-geek-gets-15-years-for-plotting-attack-on-nyse/

[86] UK, Home Office, *Operational Case for Bulk Powers*

[87] UK, Home Office, op.cit.,p.42. 本件関連の報道は多いが、次が参考になる。
-- Dominic Casciani, “Liquid bomb plot: What happened,” *BBC News*, last updated 9 September 2008, accessed 22 March 2020,

2006 年英国各地に居住するテロ集団が、ソフトドリンクに偽装した手製液体爆弾（TATP）によって、英国と北米間に就航する多数の旅客機の爆破を計画。仮に成功すれば、英国史上最大、9.11 同時多発テロ事件に匹敵する被害を生ぜしめるところであった。

主犯アブドラ・アハメド・アリは、アフガン難民支援活動をしていたが、パキスタンの難民キャンプの悲惨な状況を見て過激化し、過激な言動をしていたため、治安当局の関心対象となった。同人が 2006 年 6 月にパキスタンから帰国の際に、空港で預入手荷物の秘密捜索を行ったところ、爆弾材料と思しきものを発見した。そこで監視態勢を強化し、MI5 がアハメド・アリ居住のアパートを秘密捜索したところ、爆弾工場の様相であったため、秘密裡にカメラとマイクを設置した。すると、8 月 3 日アハマド・アリらが飲料ボトルを使用して爆弾を製造している状況を映像で把握した。秘匿設置したマイクから、犯行には 18 又は 19 が関与することを把握（爆弾数又は実行者数と推定される）。また、8 月 6 日にはインターネット・カフェで北米行き旅客機の時刻表を調査しているのを把握した（通信傍受）。

このまま推移すればテロの実行は真近と見られた。そこで共犯者を割り出してテロ実行を阻止するため、治安・諜報諸機関は、通信メタデータの分析により、アハメド・アリらの関係者とその相互関係を迅速に解明し、8 月 10 日未明 24 人を一斉検挙してテロの実行を阻止した[88]。迅速に検挙できたのは包括収集された通信メタデータの分析の成果である。

なお本事件を契機に、旅客機客室へのペットボトルの持込が制限されることとなった。

イ　2007 年英国兵士に対する誘拐殺人テロの阻止[89]（スライド 33 頁参照）

パルビス・カーンは 2006 年から、英国内でイスラム教徒の英国兵士を誘拐し首を切断して殺害する計画を立てていた。彼は犯行の状況をビデオ撮影し、それを海外の関係者に送信して画像をインターネットで公開することによって、イスラム教徒の英国

---

http://news.bbc.co.uk/2/hi/uk_news/7564184.stm

[88]容疑者の多くには終身刑が言い渡されている。

[89] UK, Home Office, op.cit.,p.41.

--Terri Judd, “Man admits plot to behead British Muslim soldier,” *Independent,* 30 January 2008, accessed 5 September 2019, https://www.independent.co.uk/news/uk/crime/man-admits-plot-to-behead-british-muslim-soldier-775588.html

--Cominic Casciani, “The jihadi and the beheading plot,” *BBCnews*, 18 February 2008, acceseed 22 March 2020, https://web.archive.org/web/20080222205434/http://news.bbc.co.uk/1/hi/uk/7241778.stm

--Russell Jenkins and Daniel McGrory, “How al-Qaeda ‘tried to bring Baghdad to Birmingham’,” *TimesOnLine*, 1 February 2007, accessed 22 March 2020, https://web.archive.org/web/20070224025422/http://www.timesonline.co.uk/tol/news/uk/crime/article1308572.ece

兵士に恐怖を巻き起こそうと企図していた。

カーンは元々アフガニスタン支援の活動家であった。人道支援の名の下、実際は、戦闘に有用な一般商品（携帯電話、携帯無線機、ゴルフ用測距離機、（狙撃に使える）手袋等々）を支援物資としてタリバンに提供していたのである。カーンが監視対象となった経緯は不明であるが、英国シギント機関 GCHQ が海外テロ関係者の通信を監視していたところカーンとの通信を捕捉した可能性と、元々危険分子として監視対象に入っていた可能性が考えられる[90]。当初はカーンしか把握できなかったため、MI5 がカーンの自宅にマイクなど監視機材を秘匿設置すると共に、カーンの通信を傍受し、更に通信メタデータ分析により他のメンバーを発見し、テロ・グループを解明することができた。その情報に基づき、警察が関係施設の一斉捜索を行い、誘拐殺人テロを阻止した。

調査開始時点では、グループの構成員は未把握であったので、通信メタデータの包括的収集がなければ、迅速な検挙は出来なかったとされる。

ウ　2007 年ロンドンでの爆破未遂事件とグラスゴー空港攻撃事件[91]

2007 年 6 月 29 日未明ロンドン市内で自動車爆弾爆破未遂事件が 2 件発生した。2 件ともベンツに石油、ガス缶、釘を積み込み、携帯電話による起爆装置が設置してあった。一両目の自動車は近くで石油臭を嗅いだ者の警察通報で発見され、二両目は駐車違反で撤去されていたが一両目の報道を聞いた職員が警察に通報した。自動車爆弾は携帯電話による遠隔操作で爆発するように作られていたが、何らかの不具合で起爆しなかった。

ところが、翌 6 月 30 日には、スコットランドのグラスゴー空港ターミナル建物にプロパンボンベを積み込んだ犯人 2 人が乗車したジープが突っ込んだ。ジープには、ガソリン、プロパンボンベ、火炎瓶などが積み込んであり、自動車爆弾を意図したものであったが、車止めに阻止されて建物内への侵入に失敗し、炎上したのみで、犯人 2 人は取り押さえられた。犯人 2 人ビラル・アブドラとカフィール・アハメド。

これらの事件について、治安・諜報諸機関は、ロンドン事件で使われた（携帯）電

---

[90] 他の一説には、アルカイダ系のダークウェブサイト（パスワードを使用して初めてアクセスできるサイト）での交信から捕捉したとも言われる。

[91] UK, Home Office, op.cit.,p.41.
--“Behind the London-Glasgow plot,” *BBCnews*, 16 December 2008, accessed 22 March 2020, http://news.bbc.co.uk/2/hi/uk_news/7772925.stm.
--Kim Sengupta and Cahal Milmo, “Police link suspects held over failed attacks,” *The Independent,* 5 July 2007, accessed 22 March 2020, https://web.archive.org/web/20071001002250/http://news.independent.co.uk/uk/crime/article2737136.ece
--“2007 London car bombs,” *Wikipedia*, accessed 5 September 2019, https://en.wikipedia.org/wiki/2007_London_car_bombs
--“Glasgow Airport attack,” *Wikipedia*, accessed 22 March 200, https://en.wikipedia.org/wiki/Glasgow_Airport_attack

話の通信メタデータの分析により、数時間後には 3 つの事件の犯人は同一であり、これ以上の攻撃の危険はないことを迅速に解明することができた。

包括収集による通信メタデータの分析がなければ、これ程、迅速に分析することは出来なかった。

エ　2010 年ロンドン証券取引所他に対する同時多発テロの阻止[92]

過激派アンワル・アルアウラキの過激な説教に影響を受けた 9 人が、2010 年のクリスマスや翌年の復活祭の時期に、爆弾と銃を使用してのテロを計画[93]し、手製爆弾を製造したり、攻撃対象として政治家や聖ポール大聖堂、ロンドン証券取引所などを物色していた。

本件テロ計画捕捉の端緒は不明であるが、9 人は従前から過激な言動で監視対象となっていた者が多いようであり、監視の結果、一部のメンバーがテロを企図していることを把握したものと見られる。そこでテロ集団を全て把握するために、通信メタデータ分析を中心とする調査の結果、広範囲に分散していたグループ構成員全てを解明し、12 月 20 日に全員逮捕してテロを阻止した[94]。

通信メタデータの大量分析により、迅速にグループの解明と検挙に至ったものであり、これは対象を特定した通信傍受では困難であり、国内通信メタデータの包括的収集の成果であった。

オ　2013 年乃至 2014 年北アイルランドでの爆弾テロ阻止[95]

過去 3 年程、あるグループが北アイルランドでテロを企図していた。そして、同グループは既に爆発物を入手し、活動が活発になって来ていた。活動活発化は、テロ実行が近付いている指標であるが、同グループは秘密保持に力を入れていたので、テロの実行予定日など具体的情報は入手できなかった。（註：即ち、同グループは通信傍受による探知を回避するため、メールや電話ではテロ計画については言及しなかったと思われる。）

その時、通信メタデータの分析により、突破口が開かれた。同分析により、グループの未解明メンバーを発見し、グループ構成員全体の活動を監視の対象とした。そして、メンバー間の通信量（そして活動）の激増を探知したため、警察が捜索を行い手

---

[92] UK, Home Office, op.cit.,p.40.
--"Terrorism gang jailed for plotting to blow up London Stock Exchange," https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9072455/Terrorism-gang-jailed-for-plotting-to-blow-up-London-Stock-Exchange.html
--"London Stock Exchange bomb polt admitted by four men," BBC, 1 February 2012, accessed 5 September 2019, https://www.bbc.com/news/uk-16833032

[93] 本文のテロがモデルとしたのは、2008 年 11 月インドのムンバイで、ラシュカル・エ・タイバが敢行した同時多発テロで、手製爆弾や自動小銃で武装した 10 人が移動しながら各所を攻撃し、死者 160 人負傷者 300 人以上の甚大な被害を生んだ。

[94] 関係者 9 人は全員罪を認め、最高 18 年の懲役刑に付された。

[95] UK, Home Office, op.cit.,p.39.本件については関係報道を特定できなかった。

製爆弾を発見することが出来た。

通信メタデータ分析による通信量の激増が、爆弾の準備完了とテロ実施直前の準備活動を示唆したため、警察がグループの中心人物を逮捕する根拠を提供したのである。

カ　2014 年西側某国における爆弾テロ阻止[96]

2014 年に治安・諜報諸機関のシギント情報の分析から、シリア内の「イスラム国」関係の過激派と接触を持っている某国の者を特定できた。更なる分析により、同人が最近欧州の某国を訪問したこと、テロ攻撃を計画していることが判明した。そこで、関係国政府当局に情報を提供したところ、同国政府は攻撃を防止し、手製爆弾数個を押収した。

これは、英国も国外にもシギントデータの収集能力を及ぼしており、外国におけるテロ準備活動を把握した事例である。

以上は、英国で通信傍受でテロが阻止された事例であるが、こうして見てくると、スノーデン漏洩資料にも拘らず、英国で広汎な通信傍受が受け容れられている理由が理解できる。

第２章では、テロ対策のための世界標準の情報収集手法として、（旧来型）通信傍受、信書開披、秘密捜索、監視機材の設置、潜入調査・囮調査などを紹介して、20 世紀において既に欧米諸国と我が国とでは情報収集力に大きな差異があったことを述べた。

本章では、21 世紀にはサイバー空間が主要な情報空間として出現したために、テロ対策においてもサイバー空間への対処が喫緊の課題となり、シギント機関の関与が必要となったこと、特に UKUSA シギント同盟による情報収集力が、如何にテロ対策に貢献しているか、また、当該諸国以外のテロ抑止でも貢献していることを述べた。

我が国は、20 世紀の情報収集手法においても、21 世紀のサイバー空間に対する情報収集力においても、欧米諸国と対比して全く異なるレベルにあり、我が国はテロ対策では大きな課題を抱えたままであることが明白となった。ところが、我が国のテロ対策における課題はこれが全てではないのである。その他の課題を次章では見てみよう。

[96] UK, Home Office, op.cit.,p.28.

第４章　その他のテロ対策の課題

１　平成 28 年版『警察白書』が提示した課題（スライド 35 頁参照）

我が国のテロ対策における課題を見る上で、平成 28 年版『警察白書』の国際テロ対策特集[97]が参考になる。

同特集ではその「第 2 節　国際テロ対策」中「３　諸外国の国際テロ・サイバー攻撃対策」[98]で、米英仏独のテロ対策を紹介している。諸外国の対策紹介ではあるが、白書で取り上げている趣旨は、警察当局は実効あるテロ対策のためには紹介した諸対策が必要であると考えていると推定できる[99]。

その中で、米英独仏四カ国に共通する項目を見てみよう。

（１）通信傍受（行政傍受）

米英独仏四カ国共に、テロ対策に使用できる行政傍受の制度を持っている。これは、第 2 章と第 3 章で米国英国について詳述したところであり、通信傍受はテロ対策における必須アイテムである。

ここで、強調しておきたいのは、この通信傍受は国家安全保障のための行政傍受であって、司法捜査のための司法傍受ではないことである。そのため、通信傍受の要件や通信傍受対象者への通知不要など、実施手続（要件と効果）が異なることである。テロ対策に必要な通信傍受を、司法傍受の枠組で行うのは殆ど不可能である[100]。我が国には、極めて限定的な司法傍受の制度がある[101]だけで、国家安全保障のための行政傍受の制度は存在していない。

（２）テロ周辺行為（準備、支援、唱道など）の犯罪化

何れの国でも、テロ行為自体は犯罪とされているが、それだけではテロを事前に阻

---

97 警察庁・平成 28 年版『警察白書』第 1 部国際テロ対策、第 2 節国際テロ対策

98 前掲、30-33 頁。

99 実効性のないものをわざわざ白書で取り上げる必要はないからである。また、我が国では、警察庁が欧米諸国並みのテロ対策権限が必要と公式に主張するだけで、政治問題化は必至であろうから、必要性の意思表示は白書で諸外国の例として紹介するのが限界であろう。

100 米国の行政傍受については、茂田忠良『米国における行政傍受の法体系と解釈運用』（警察政策学会資料第 94 号、2017 年 6 月）参照。

なお、一部に米国の対外諜報監視法による通信傍受を司法傍受と解釈する者がいるが誤解を招く解釈である。対外諜報監視法第 105 条に基づく通信傍受は、対外諜報監視裁判所による令状を必要とするが、司法捜査目的の通信傍受ではなく、国家安全保障目的の通信傍受である。また、対外諜報監視裁判所は特別の裁判所であり、令状は秘密令状であって傍受対象者に開示されることはない。米国の制度は、行政傍受手続に特別の裁判所を関与させるという独特の制度である。

101 政府『犯罪捜査のための通信傍受に関する法律 に基づく報告（平成 31 年 1 月 1 日から令和元年 12 月 31 日）』（2020 年 2 月）によれば、2019 年 1 年間の司法傍受の件数は、薬物犯罪、窃盗、殺人など 10 事件で合計 31 の令状が発布されているに過ぎない。

止することは困難である。テロを未然に防止するには、テロ敢行に至らない周辺行為を犯罪化し処罰することが重要である。欧米諸国では、テロ実行の前段階の準備行為、テロリストに対する支援行為などが幅広く犯罪化されている[102]。

米英仏独諸国のテロ周辺行為の犯罪構成要件は、第1章で取り上げた我が国の「テロ等準備罪」とは全く異なる。我が国の「テロ等準備罪」はテロ阻止に関しては実効性を期待できないことは既述の通りである。

（3）テロ容疑者に対する各種行動制限

テロ周辺行為、特に準備行為を犯罪化しても、テロリストと合理的に疑われる者やテロを行おうと疑われる者を必ずしも逮捕できる訳ではない。そこで、欧米諸国はテロ容疑者に対する行政拘束（48時間、96時間、外国人6か月、不定期限など国によって異なる）の制度を持っている。その他、テロ容疑者に対して、一定の条件下での出入国の制限、特定場所への立入禁止、警察署への定期的出頭命令など、各種の行動制限措置を採ることが可能である。

我が国に、テロ容疑者に対する行動制限措置は、存在しない。

（4）テロ関連情報の集約・分析

テロ対策は、警察機関、インテリジェンス機関、その他様々な行政機関が関与するので、関係情報を一元的に集約して分析して、必要な諸機関と共有する態勢が必要である。

そのため、諸外国ではテロ関連情報を集約・分析する組織が設置されている。米国：国家諜報長官下の「国家テロ対策センター」NCTCとFBI管理の「テロリスト・スクリーニング・センター」、英国：セキュリティ・サービス内「合同テロリズム分析センター」JTAC[103]、ドイツ：「共同テロ対策センター」GTAZ[104]などである。何れもテロ対策に深く関与するインテリジェンス機関又は警察機関内に設置されている。

これに対して、我が国では、内閣官房に2015年12月に「国際テロ情報集約室」（室長：官房副長官（事務））が新設され、次に同室の下に2018年8月「国際テロ対策等情報共有センター」が設置された[105]。「集約室」は官房副長官が室長であるので、実

---

102 テロ周辺行為の犯罪化の例については、平成28年版『警察白書』前掲参照。

103 英国の「合同テロリズム分析センター」JTACは16の行政機関からの代表・派遣者で構成する合同組織であるが、センター長はセキュリティ・サービス長官の指揮下にある。Security Service website, “joint terrorism analysis centre,” https://www.mi5.gov.uk/joint-terrorism-analysis-centre.

104 ドイツの「共同テロ対策センター」GTAZは40の関係機関で構成する合同組織である（構成機関は、連邦刑事庁、連邦憲法擁護庁、16の州警察、16の州憲法擁護庁その他である。）

105 内閣官房「国際テロリズムに対する取組～テロの未然防止に向けて～」undated、2020年4月12日最終閲覧。https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/torikumi.html

働の組織としては期待できない。そこで「共有センター」であるが、11の関係機関から十数人を集めて外務省出身者がセンター長を務めるということである[106]。欧米諸国のテロ関連情報の集約・分析センターと対比すると、人員面でも組織面でも異なっており、これがどの程度有効に機能するかは、今後の進展を待つこととなろう。

また、2017年7月警察庁は東京オリンピック・パラリンピック対策として「セキュリティ情報センター」を設置したが、テロ対策を含め東京大会の脅威・リスクに関する情報を集約・分析・評価し、関係省庁に提供することとされている[107]。警察庁情報センターがテロ対策で情報集約・分析組織として如何なる役割を果たすのかについても、今後の進展を待つこととなろう。

２　その他の重要課題（スライド36頁参照）

『警察白書』では取り上げられていないが、その他にも重要な課題がある。幾つかを指摘しておく。

（１）行政情報・民間業務情報の国家安全保障目的での収集権限

テロ対策における情報収集では、地方公共団体を含む行政機関や民間企業が所有しているテロ容疑者に関する情報もテロ対策上重要であることは言を俟たない。

さて先ず、行政情報、即ち国の行政機関・地方公共団体の保有する情報の収集の現状はどうであろうか。行政機関個人情報保護法は、8条2項で「他の行政機関・地方公共団体が法令の定める事項又は業務の遂行に必要な限度で利用することに相当な理由のあるときは、提供することができる」旨規定している[108]。警察は、警察法2条によって「公共の安全と秩序の維持」をその責務としており、テロ対策はその一部であるから、必要な情報は本規定によって支障なく収集できる筈である。しかしながら、一部の地方自治体は、行政機関個人情報保護法を理由として提供に消極的であり、情報収集に支障を来していると聞く。地方自治体に対する正しい解釈の普及徹底が必要

106　「省庁横断でテロ情勢分析　政府、五輪など備え新組織」（日本経済新聞電子版、2018年8月1日）2019年9月20日閲覧。https://www.nikkei.com/news/print-article/?R_FLG=0&bf=0&ng=DGXMZO33654620R00C18A8MM0000.

107　第32回犯罪対策閣僚会議・資料2「2020年東京大会等を見据えた主なテロ対策の推進状況（第2班）」（2019年12月）
https://www.kantei.go.jp/jp/singi/hanzai/dai32/siryou2.pdf

108　同法8条1項で「法令に基づく場合を除き個人情報を提供してはならない」旨規定しているが、ここで言う「法令に基づく場合」とは法令の個別具体的規定に基ずく場合である。刑事訴訟法197条2項の捜査関係事項照会が典型である。
個人情報保護委員会『個人情報の保護に関する法律についてのガイドライン　（通則編）』（2016年8月制定、2019年1月一部改正）29頁参照。
しかし、本照会は、「犯罪ありと思料するとき」に行う捜査（同法189条2項）に伴うものなので、犯罪がない段階では本照会はできない。我が国法令の違反行為が全く把握されていない国際テロ容疑者について、本照会による情報収集は困難であろう。

であろう。

また、民間企業が保有する業務情報、特に金融情報、クレジット情報、通信関係情報（機器の契約者情報、通信履歴情報など）は、テロ対策では必須情報であるが、これらはどうであろうか。個人情報保護法 16 条 3 項は、「国・地方公共団体が法令の定める事務を遂行することに協力する場合…」には個人情報を提供できるとし、国の定めた『個人情報の保護に関する法律についてのガイドライン （通則編）』でも「事業者が警察の任意の求めに応じて個人情報を提出する場合」はこれに該当するとしている[109]。ここでの課題は、提供があくまで任意であることで、任意の協力が得られなければ、情報収集はできない。

これに対して、米国の国家安全保障書簡 National Security Letter は強力である。これは、通信関係情報[110]、金融情報[111]、クレジット情報[112]を、FBI が国家安全保障書簡という行政命令によって、提出を強制でき、且つ同書簡には殆どの場合に秘密保持命令が付加されている[113]。米国ほど強力なものは過大との評価もあろうが、テロ対策という国家安全保障目的のために任意で十分な収集ができなければ、一定の条件下で提出を強制できる制度の創設も検討すべきであろう。

（２）通信メタデータの取扱い

通信メタデータの分析はテロ関係容疑者の容疑解明、組織解明のため極めて有効な手段である。第 3 章第 3 節で述べた通りである。

そして、欧米諸国では通信メタデータは「通信の秘密」でいう通信に当らないとされ、通信内容と比して簡易な手続による収集が認められている。そこで、既述した「接触連鎖分析」その他の手法でテロ対策に活用されている[114]。

---

[109]個人情報保護委員会、前掲、31 頁。

[110] 保管通信法（Stored Communications Act）18 U.S.C. §2709 により、個人の契約者情報、支払料金情報、（通信内容を除く）通信履歴情報を収集できる。.

[111] 金融プライバシー権法（Right to Financial Privacy Act）12 U.S.C. §3414 により、金融機関から個人の金融情報を収集できる。

[112] 公正信用報告法（Fair Credit Reporting Act）15 U.S.C. §1681u, §1681v により、クレジット会社から個人の信用情報を収集できる。

[113] 2018 年中に FBI はテロ調査やスパイ対策のために 10235 人に関して国家安全保障書簡 3 万 8872 件発出している。US Assistant Attorney General, *A Letter to the President of US Senate,* 30 April 2018, last accessed 15 April 2020, https://www.justice.gov/nsd/nsd-foia-library/2017fisa/download
--ODNI, *Statistical Transparency Report Regarding the Use of National Security Authorities (Calender Year 2018)*, April 2019, last accessed 17 April 2020, https://www.dni.gov/index.php/newsroom/reports-publications/item/1987-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2018

[114] テロ対策又はスパイ対策で、（容疑者の監視等の）情報収集で通信メタデータをを使用している国々は、2020 年新型コロナウィルス感染症対策においても、感染者との濃厚接触者の割出と追跡にも利用していると見られる。イスラエル、シンガポール、韓国は確実に使

ところが、我が国所管官庁では通信メタデータは通信の秘密に含まれるという我が国独自の解釈がされている[115]。そのため、我が国では現行法制上、テロ対策当局は通信メタデータを収集することができない。テロ対策、即ち国家安全保障上の犯罪の未然防止のため当局が通信メタデータを入手する手続制度が存在しないためである。

他方、グーグル、ヤフー、ツイッターその他いわゆるプラットフォーマーと呼ばれる民間営利企業は、通信メタデータを実質上殆ど自由に利用してマネタイズして利益をあげている。営利企業による通信メタデータ利用は実質上無制限で、他方、行政機関がテロ対策という公益目的のために通信メタデータを収集する手続制度が存在しないのは、実に奇異なことである。

検討を要する課題であろう。

（３）重要施設職員・従業員の適格性の審査

テロリストに攻撃を受けては困る特定の重要施設については、テロリスト又はテロ支援者の立入を禁止阻止すべき必要があることは、自明である。我が国でも原子力施設については、漸く 2016 年に発電炉、再処理施設の立入について、個人の信頼性確認制度が導入された。更に、2019 年には研究炉その他の原子力施設についても適用されることとなった。しかし、原子力規制委員会の「個人の信頼性確認の実施に係る運用ガイド」[116]を見ると、基本的には本人の自主申告による確認に留まり、米国における適格性の審査制度の厳格さには遠く及ばない。

また、原子力施設に対する規制は、国際原子力機関 IAEA の勧告に基づくものである。本来、特定の民間重要施設への立入者の信頼性確認や適格性確認は、当該国が自国の国家安全保障の観点から自ら必要性を判断して実施すべきものである。IAEA の勧告対象ではない、その他の重要施設の有無や規制の必要性の検討もなされるべきであろう。

更に、特定秘密保護法が制定されて、特定秘密にアクセスする者には適格性の審査がなされている。ところで、特定秘密には関わらないものの、テロリストやテロ支援者が就いては困る職位も公務員組織の中には多く存在するが、それらの職員の適格性の審査制度も検討されるべき課題であろう。

用していると見られる。また、英国、豪州なども使用している可能性が高い。桜井紀雄『韓国、経路不明わずか２％』（産経新聞、2020 年 4 月 15 日）、八十島綾平、長尾里穂『濃厚接触　アプリで通知』（日本経済新聞、2020 年 4 月 14 日）参照。

115　通信の秘密に関して、通信内容の収集と通信メタデータの収集の規制を区別しないことの不合理性については、次の論文に詳細に記述されている。
--林紘一郎、田川義博『サイバー攻撃対策としてのログの知得・利用と「通信の秘密」』（情報セキュリティ総合科学第 11 号、2019 年 11 月 1 日）
--林紘一郎、田川義博『サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か：日米比較を軸に』（情報セキュリティ総合科学第 10 号、2018 年 11 月 1 日）

116 原子力規制委員会 2016 年 9 月 21 日決定、2019 年 3 月 1 日改正。

欧米諸国では、テロ企図者が従業員等の資格でアクセスしないように、重要施設等の従業員については適格性の審査制度を保持している。

（４）外国人管理の制度と思想

筆者がテロ対策での欧米諸国治安当局との交流を通じて学んだことは、諸国の治安当局は、外国人を国家安全保障に対する潜在的脅威として捉えているということである。

そもそも近代国民国家においては、国家は人民のものであり人民の運命共同体であるので、人民は自己の国家に忠誠を尽くすのは当然の義務であると認識されている。これは、米国帰化に際しての忠誠宣言などを見れば明白である[117]。即ち、忠誠宣言では、国家への忠誠・国家の擁護を誓うと共に徴兵徴用の義務に服することを誓う[118]。

これに対して、外国人は、在留国に対する忠誠義務を持たず他国に忠誠義務を負っている人間である。これを極端な形で表現したのが、2017年制定の中国・国家情報法である。同法第７条は「国民は、国の情報活動に協力しなければならない」旨規定しているが、これは外国に滞在する中国人は法律上皆潜在的に中国政府のスパイであると定めていることになる。これは極端な例としても、在留国に忠誠義務を持たない外国人は、当該国にとっては何時でも脅威となり得る人物である。従って、各国は国家の安全保障のために在留外国人を把握し管理する政策制度を取ることとなる。

そして外国人管理は、通常内務省の所管であり、出入国管理と在留管理の二つの手法を併用するのが基本である。出入国管理は警察の一部門が担当する場合、警察外の専門部署を創設して担当させる場合がある。また、欧州諸国の在留管理では、ホテルの宿泊カード管理と長期滞在者の登録によって、外国人の短期長期滞在者を治安当局が把握し確認する制度が整備されている。詰まり、内務省の指揮下に、出入国管理部署と警察が協力して外国人管理に当たっている。

ところが我が国は、島国であることもあって、出入国管理にのみに焦点が置かれてきた。外国人管理の基本法である「出入国管理及び難民認定法」の第１条（目的）には、従来、外国人の「出入国管理」しか記載されておらず、「在留管理」が掲げられた

---

117 我が国は、帰化に当たって、日本国民としての忠誠、良き日本国民としての決意を誓う儀式のない珍しい国である。これについては、日本国籍を取得した人々が驚きを持って言及しているところである。

118 米国に帰化する際の忠誠宣言の核心部分は次の通りである。①私は、旧君主、旧所属国への忠誠を完全に放棄し拒否します。②私は、内外の全ての敵に対して、米国憲法と諸法律を支持し擁護します。③私は、米国憲法と諸法律を、信頼し忠誠を保持します。④私は、法律の定める処に従い、米国の為に武器を取って闘い、或は米国軍隊で非戦闘員としての任務を遂行し、或は文民の指揮下で国家の必要とする任務を遂行します。以上、忠誠義務と、徴兵・徴用義務が強調されているのである。U.S. Citizenship and Immigration Services, *Naturalization Oath of Allegiance to the United States of America,* https://www.uscis.gov/us-citizenship/naturalization-test/naturalization-oath-allegiance-united-states-america.

のは実に 2018 年 12 月法改正であった。それまでは、外国人の在留管理の思想自体が表明されていかったのである。正に、奇観と言えよう。　その背景には、外国人管理の思想自体が希薄であったことを示している。

2019 年 4 月に出入国在留管理庁が発足し、外国人の在留管理の態勢が強化されたのは好ましい改革であるが、これで外国人管理の態勢が十分となったのか、引き続き注視する必要がある。

第 1 章第 3 節で述べた通り、国際テロ容疑者リオネル・デュモンの潜入滞在を当局は捕捉できなかったと見られるが、責任を分担すべき部署は何れであろうか。テロ対策の視点からは警察であるが、外国人管理の視点からは出入国在留管理庁であろう。

3　我が国に存在しない国家諸機関（スライド 37 頁参照）

我が国には、テロ対策に必要な情報収集手段や制度が殆ど存在しないことが明白となった。更に、欧米諸国には普通に存在する国家機関、普通の民主主義国家に存在するテロ対策に有効な国家機関であって、我が国には存在していないものがある。その代表的な機関を次に三つ挙げる。

（1）権限を有するセキュリティ・サービス

欧米諸国は、主として国内で活動するインテリジェンス機関としてセキュリティ・サービス組織を設置している。セキュリティ・サービス[119]組織とは、「国家安全保障」を担当する機関であり、テロ対策やスパイ対策、国家転覆活動の阻止などが主要任務である。第 2 章、第 3 章で述べた情報収集に関する各種行政権限を駆使して任務遂行に当っている。警察機関と分離して設置している場合と警察機関内に設置している場合がある。

警察機関と分離している例としては、英セキュリティ・サービス SS、仏・対内安全保障総局 DGSI、独・連邦憲法擁護庁 BfV、豪安全保障諜報局 ASIO、加安全保障諜報局 CSIS[120]等である。これら諸組織の多くは警察の一部門として発足したが、任務の特殊性から警察とは分離して、警察を所管する内務大臣の下で警察と協力して任務に当っているのが通常である。

119　「セキュリティ・サービス」の邦訳は一定していない。それは「セキュリティ」の邦訳自体が、安全保障、保安、治安、警備など一定していないためである。欧文では「セキュリティ」と同一語彙であるのに異なる邦訳をすることによって、正確な理解から遠ざかる可能性がある。例えば、フランス諜報機関 DGSI を「対内安全保障総局」と邦訳すべきところを「対内治安総局」と邦訳すると、「対外安全保障総局」DGSE との相関関係が見えなくなってしまうことである。従って筆者は、国家機能として「セキュリティ」の語を使う場合は「安全保障」の訳語で統一すべきものであると考える。

英セキュリティ・サービスの邦訳は、保安局ではなく安全保障局とすべきである。

120　カナダ CSIS は、2016 年法改正でカナダ国外での情報収集も可能とされ、対外諜報機関としての性格も強くなりつつあるようである。

他方、警察機関の内部にセキュリティ・サービスを設置している国もある。典型的なのは米国であり、連邦の一般警察機関と言えるFBIの中に司法捜査部門とは別の国家安全保障局National Security Branchを設置して、セキュリティ・サービス機能を担っている。また、フランスは、元々セキュリティ・サービス（対内諜報中央局DCRI）を内務省警察総局内に設置していたが、2014年の組織改編で警察総局から分離して、内務大臣に直結する組織とした。先進民主主義国においては、警察機関から分離する方向にあるようである[121]。

ところで、我が国には、通信傍受、侵入的監視、潜入その他諸々の情報収集のための行政権限を持つセキュリテイ・サービスが存在しない。戦後の我が国では、警察の警備警察部門が、セキュリティ・サービスの権限無しに、（テロ対策やスパイ対策などの）セキュリティ・サービス機能を担ってきたというのが実態である。しかし、権限無しに十分な機能を果たすことは難しい。

今後の課題として、警察内の一部の組織に欧米諸国並みの情報収集のための行政権限を付与するのか、或いは、警察とは別に国家公安委員会の下にセキュリティ・サービスを新設するのか、などの議論が必要になろう。なお、公安調査庁が現状のままセキュリティ・サービスとなり得ないことは、松本光弘氏がその著書で指摘する通りである[122]。

（２）権限を有する国家シギント機関

米国NSAについて既に言及したが、欧米諸国の多くは国家シギント機関を設置している。大統領や首相等の最高行政責任者初め政府全体のためにシギント業務を行うインテリジェンス機関である。NSAの他に、英・政府通信本部、豪・信号局、加・通信安全保障局などがある。また、シギント組織を独立組織とせずに国家中央諜報機関の中の一部門として設置している国もある。独・連邦情報局や仏・対外安全保障総局などである。

国家シギント機関は、対外諜報一般で不可欠な組織であるが、本稿で述べた通り、国際テロ対策においても極めて重要な機関である。

（３）総合治安を担当する省（＝内務省）

---

[121] スウェーデンもセキュリティ・サービス組織SAPOが警察組織内に設置されていたが2014年に独立して、治安担当省である司法省傘下に警察と共に置かれるようになった。

[122] 松本光弘『イスラム聖戦テロの脅威』（講談社、2015年）224-225頁参照。即ち、公安調査庁は、破壊活動防止法による団体規制のための準司法的な認定資料収集機関である。破防法の主目的は、暴力主義的破壊活動を行った団体に対して、各種活動を制限し、必要な場合は、団体の解散指定を行うことである。しかし、オウム真理教のように、明確な指揮系統を有し国内でテロを繰り広げた団体ですら解散指定できなかったのであり、海外を基盤にし指揮系統も不分明な国際テロに対して有効な対策が可能とは考えられない。松本氏は以上の趣旨を述べているが、全く同感である。

欧州諸国では、（災害対処を含む）広義の治安を総合的に担当する中央官庁として、内務省が存在する。欧州諸国の内務省の組織を調べてみれば容易に気が付くことであるが、内務省の所管には、警察、セキュリティ・サービス、国境警備、出入国管理や外国人の在留管理、消防を含むのが通常である。内務大臣は、これら諸機関を統括し相互協力関係を確保して総合治安に責任を持っている。ここで言う総合治安とは、単なる刑事司法や法執行を超える国家安全保障を含む広義の治安である。内務省の傘下に必要な諸機能の多くが集約されているために、テロ対策においても、一人の大臣が総合調整機能を発揮することが出来るのである。

なお、米国には欧州型の内務省が存在しなかったため、2001 年 9・11 同時多発テロ事件を受けて国土安全保障省が設置された。国土安全保障省とは、米国における欧州諸国の内務省の代替物である。

これに対して、我が国では、警察庁、海上保安庁、出入国在留管理庁、消防庁は全て別の府省に属しており、これら諸機関を統括して総合治安に責任を持つ大臣が存在しない。我が国の国家行政機関の構成は、独立国家としては極めて特殊な国であることを認識する必要がある[123]。

4　背景にある思想的課題

テロ対策に係る諸々の課題を述べてきた。そこで、何故、欧米諸国とこれ程異なるのか、何故、これ程の課題が存在するのか、何故、多くの課題が放置されてきたのかと考えると、結局、我が国における思考の枠組の問題に帰着するのである。即ち、一言でいえば「国家安全保障」的思考の希薄、乃至不存在である。

第 1 章の「思考の枠組・座標」で述べたように、テロ対策は、「法執行」の問題でもあるものの、第一義的には「国家安全保障」の問題であると捉える思考法。そして、「国家安全保障」を確保するには、「法執行機関」の他に「インテリジェンス機関」が必要であるという常識。テロ対策に当たる「インテリジェンス機関」の中では、主として国内において安全保障任務に当たるセキュリティ・サービス（＝安全保障局）、そして、サイバー空間が重要性を増すにつれ国家シギント機関が重要であるという認識。また、内務省とは国内において国家安全保障を担当する官庁であるという認識。そのような認識なり思考の欠如こそ最大の課題ではないだろうか。

---

[123] 米占領下の内務省解体が、独立回復後も維持されているのである。

一部に、国家公安委員会・警察庁が総合治安担当行政庁と考える者がいるかも知れないが、筆者には到底そうとは考えられない。セキュリティ・サービスも傘下に持たない。国境警備にも権限がない。外国人管理にも権限がない。消防にも権限がない。普通の国の内務省は、皆これらの機能を傘下に持って一人の大臣の下に諸機能を統合している。従って、テロ対策でも総合的な対策を取ることができる。それが我が国には存在しないのである。

まとめ（スライド 39 頁参照）

以上、我が国のテロ対策の課題を見てきた。テロ対策全体を俯瞰すると、権限面や組織面において、我が国の対策は極めて不十分であることが明かとなった。欧米諸国で実施されている対策の多くが我が国では実施されていない。

先ず、この実態、即ち我が国のテロに対する脆弱性とテロ対策の不十分性を認識し自覚することが重要である。「我が国でも欧米並みのテロ対策ができている」と自己欺瞞に陥いると、そこで思考が停止してしまう。実態を前提として議論をすることが重要である。

次に、それでは何故、我が国では今まで国際テロが少ないのであろうか[124]。我が国独自のテロ対策の効果であるのか、或いは、国際テロリストに狙われることが少なかっただけなのか。答えは明白である[125]。それでは今後も従来の状況が継続するのであろうか。それは望み薄ではあろう。既に、海外では日本人も標的として国際テロが敢行されているのである[126]。更に、今後は国内でも、テロの脅威は増大することが予想される。グローバル化の進展により国境の障壁は今後も下がり続けることが予想され[127]、我が国だけ国際テロの脅威から自由であるとは考えられない。また、実質的な移民が増えた場合、移民二世を低賃金労働者に留めることなく差別のない社会統合に成功しなければ、差別と貧困がテロリストの温床となろう。

この認識を前提とした上で、今後我が国の採るべき方針を考えると、選択肢は大きく二つの方向があろう。一つは、欧米型のテロ対策を採用しテロ対策を抜本的に強化する方向である。もう一つは、我が国の現在のテロ対策の構造をそのまま維持しつつ、可能な範囲でテロ対策を強化する方向である。

欧米諸国と対比すれば、我が国における国際テロによる被害は依然として極めて少ない。また、欧米諸国と比べテロ対策が進んでいないという事は、同時に国民の権利自由に対する制限が欧米諸国よりも少ない事でもあって、利点もある。従って、選択肢として後者、即ち現在の構造の維持も存在するであろう。但し、後者を選ぶ場合には、テロ対策において極めて不十分な現状を維持するのであるから、「テロに屈しない」覚悟をより強く固める必要があろう。即ち、万が一、大規模テロが実行されても、国民は冷静さを保ち日常生活を継続しなければならないし、国の指導者はテロの脅威に屈して国策を変えてならない。テロは恐怖を惹き起こすことによって目的を達成す

---

124 警察庁・平成 28 年版『警察白書』の国際テロ対策特集では、我が国内での国際テロ事件 3 件、我が国を場とした航空機爆破テロ計画 1 件が記述されている。（12 頁参照。）

125 前註で言及した我が国内の国際テロ事件で、我が国当局によって解明検挙された事案は一件もない。

126 警察庁・平成 28 年版『警察白書』14－15 頁参照。

127 今回のコロナウィルス感染症問題で、グローバル化には一定の揺戻しがあろうが、かと言って、国境障壁が 20 世紀に戻るとは考えられない。国境障壁を高く築けば、そのような国は世界経済競争で効率性低下により敗北してしまうからである。

るのであるから、恐怖により行動を変えれば、テロリストの企図に沿うこととなるからである。9.11 同時多発テロの被害は甚大であったが、それでも死者数は、我が国 1 年間の交通事故死亡者数には及ばない。国民と政治指導者による選択と覚悟が問われている。

最後に附言しておきたいのは、本稿で記述した我が国のテロ対策の現状は、同時にスパイ対策の現状でもある事実である。即ち、テロ対策において情報収集力が弱体である事は、同時にスパイ発見・検挙のための情報収集力も弱体である事である。そして、情報収集力の弱体さの弊害は、テロ対策よりもスパイ対策において深刻である。テロ対策の弱体さの弊害は、終局的にはテロを抑止し得ずテロという結果が発生することによって、国民の目にも明らかになる。他方、スパイ対策の弱体さの弊害は、その事実を国民が認識することが出来ないのである。

2020 年 1 月ソフトバンクの元社員がロシア諜報機関員（在日ロシア通商代表部アントン・カリニン、ライン X）に機密情報を漏洩していたとして逮捕された。また、同月元一等空佐 K が「特別防衛秘密」の防衛商社への漏洩で逮捕された。これにより、政府職員による情報漏洩や民間企業に対する産業スパイ工作の一端が明らかになった。担当者の努力に敬意を表する次第である[128]。

しかし、これらの事例はたまたま露見した氷山の一角であろう。国民の知らない内に、政府の機密情報や日本企業に蓄積された産業技術情報が盗まれても、或いは我が国に対する積極工作が成果を挙げ国策に不当な影響を受けていても、検挙されない限り、国民は知ることがないのである。国民が知らないうちに、国益が損なわれ国富が流失している可能性は大きいのである。

国際テロ対策の課題の背景には、国際テロ対策に止まることのない、国家安全保障上の大きな課題が伏在しているのである[129]。

---

[128] もし仮に、警視庁公安部に、欧米セキュリティ・サービス組織と同様な情報収集権限が付与されたならば、我が国におけるスパイ検挙事案は激増するであろう。

[129] サイバーセキュリティ対策についても、現在の我が国の取組態勢には同様な課題がある。本稿では触れなかったが、米英加豪 NZ などの取組を見ていると国家シギント機関の関与なしに十分な対策ができるのか疑問である。サイバーセキュリティに関するシギント機関の役割については、茂田忠良『サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～』（情報セキュリティ総合科学第 11 号、2019 年 11 月）参照。

添付資料

日本のテロ対策の課題

～欧米諸国との対比において～

2019年10月3日

日本大学　危機管理学部
茂田忠良

1

1

内　容

序　問題意識
１　認識と思考におけるギャップ
２　情報収集手法の違い
３　サイバー空間
　３－１　サイバー空間の重要性
　３－２　NSAとUKUSAシギント同盟
　３－３　シギントによるテロ対策
４　その他の課題
まとめ

2

2

序　問題意識

○　実務家の立場：

現状を前提

漸進的、incremental

H16政府「テロの未然防止に関する行動計画」他

○　OB研究者の立場：

適正な対策が出来ているのか

国際標準に達しているの

○　国際協力上の必要：

世界（欧米諸国）標準は

3

3

内　容

4

4

1（1）思考の枠組（座標）

（目的）

○ 事案対処 ⟺ 未然防止

（被害限定、犯罪捜査）

（機能）

○ 法執行 ⟺ 国家安全保障

（担任機関）

○ 警察機関 ⟺ インテリジェンス

セキュリティ・サービス

シギント機関

5

5

1（2）テロ等準備罪に対する評価

「組織的犯罪処罰・犯罪収益規制法」第6条の2

国際組織犯罪防止条約（TOC条約）締結するため

2017年制定（法務省Website）

＜構成要件＞

① 「組織的犯罪集団」の存在、 且つ

② 団体の活動として、具体的且つ実現可能性のある計画の存在、 且つ

③ 計画に基づく実行準備行為の存在

○ どうやって立証するのか。

その前に、探知できるのか。

6

6

1（3）考えるヒントとなる事例

① オウム・地下鉄サリン事件1995年3月20日

- ○ 世界初の大都市、化学兵器使用、無差別テロ
- ○ 政府対応：オウム新法1999年
- ○ 平成8年版警察白書　反省教訓の一つ
  「特殊な閉鎖的犯罪組織についての情報不足」

今後は未然に探知し、阻止できるのか。

② 中核派・大坂正明の逮捕　2017年5月

- ○ 警察官殺害（渋谷暴動）で1972年に指名手配

日本警察の情報収集力

7

7

1（3）考えるヒントとなる事例

③ IS戦士の帰国者対策

- ○ 処罰できるのか。
- ○ 拘束できるのか。
- ○ 十分な監視ができるのか。

（普通の国の手法）

- ・ 面接
- ・ 周辺に協力者
- ・ メール通信の監視、ウェブ閲覧の監視
- ・ 秘密捜索、秘密手荷物検査
- ・ 住居への傍受・撮像装置設置

8

8

内　容

序　問題意識

１　認識と思考におけるギャップ

２　情報収集手法の違い

３　サイバー空間

　３－１　サイバー空間の重要性

　３－２　NSAとUKUSAシギント同盟

　３－３　シギントによるテロ対策

４　その他の課題

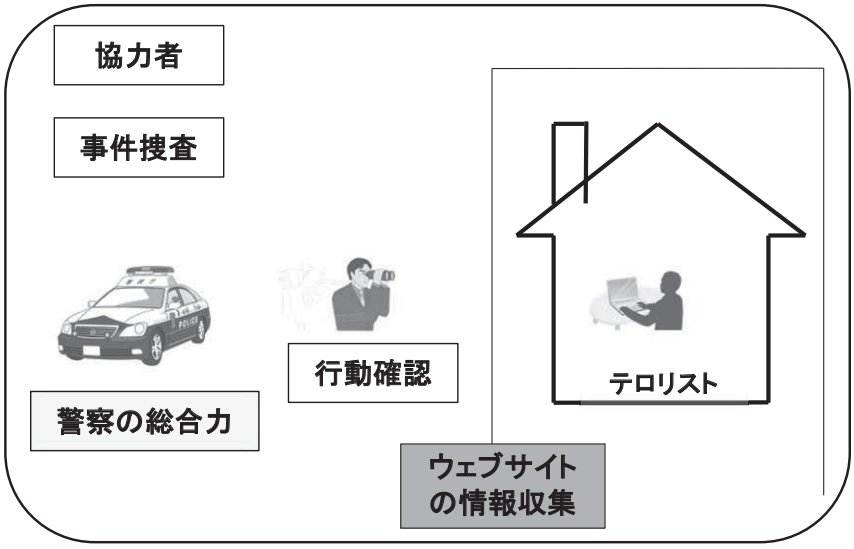
まとめ

9

9

２(１)我が国の情報収集手法

○　日本

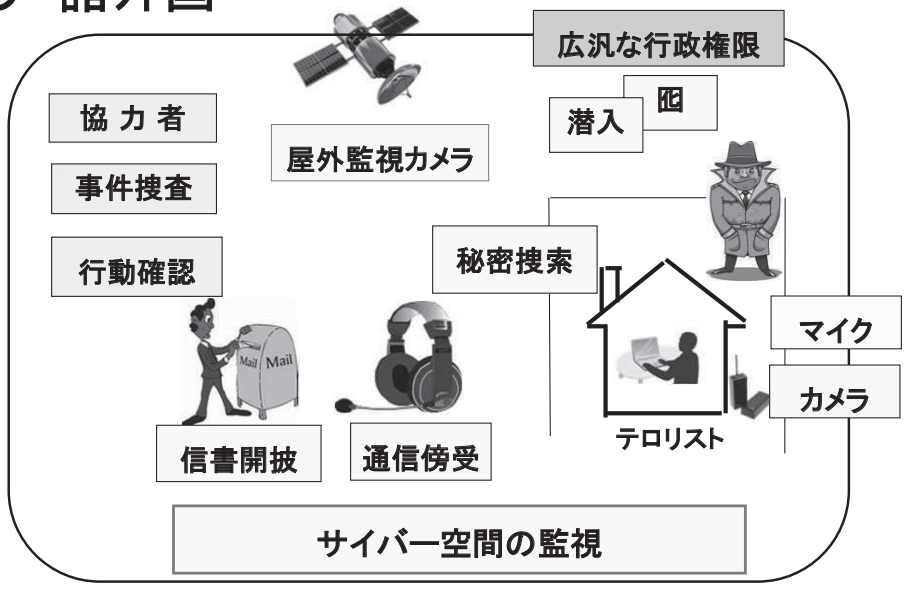


10

10

2（2）諸外国の情報収集手法

○ 諸外国



11

11

2（3）英国RIPA2000、IPA2016

2000年調査権限規制法、2016年調査権限法

○ 通信傍受・郵便検閲 interception of communications

○ 通信メタデータ use of communications data

○ 監視（車両への位置発信装置設置を含む）
directed surveillance

○ 侵入的監視（住居、ホテル客室、自動車内：
秘密捜索、監視機器設置） intrusive surveillance

○ ヒューミント（潜入、協力者）
covert human intelligence source

内務大臣制定の各種実施規範Codes of Practice
RIPA2000第71条、IPA2016附則第7

12

2（4）米国米DoD Manual 5240.01

2016年8月国防総省諜報活動実施手続

- ○ 物理的監視（人的監視） physical surveillance
- ○ 秘匿監視（電子装置、光学装置、機械装置の使用） concealed monitoring
- ○ 電子的監視（通信傍受、住居内傍受等） electronic surveillance
- ○ 物理的捜索（秘密捜索）
  住居、スーツケース他手荷物 physical searches
- ○ 郵便検閲 searches of mail
- ○ 身分偽変（潜入） undisclosed participation

実施の根拠規定：EO12333、FISA

参考：『米国における行政傍受の法体系と解釈運用』2017年警察学会資料94号

13

内　容

14

14

3-1（1）サイバー空間の状況

＜サイバー空間＞

あらゆる活動がなされる巨大空間。国境がなく、世界一体化。

○ テロに関連する活動

- テロ集団の思想宣伝、リクルート、思想教育
  ～DABIQ, Inspire,説教
- テロ技術の伝達
  （爆発物製造方法、車両使用の殺害方法）
- テロ計画の立案、準備
  （標的調査、グーグルマップ、攻撃手段）
- テロ実行の際の通信連絡
  ～2008年ラシュカル・エ・タイバVoIP
- 活動資金調達
- サイバー・テロ　～「イスラム国」CyberCaliphate

15

15

3-1（2）サイバー空間の状況

○ サイバー空間における対テロ活動

サイバー空間における容疑者の発見、追跡、監視

① テロ容疑者の容疑解明　Target Development

② テロ容疑者の発見　Target Discovery

～既知のテロ関係者から手繰り発見する。

③ テロ容疑者の発見　Target Discovery

～ネット空間における行動分析から発見する。

欧米のテロ対策の重点はサイバー空間

日本では？

○ サイバー空間で必要な情報活動の枠組

＜セキュリティ・サービス＞ ＜シギント機関＞

＜行政傍受＞

16

16

3-1（3）インテリジェンス組織

	セキュリティ・サービス	ヒューミント	シギント	イミント	軍諜報
米	FBI 国家安全保障局	CIA 中央諜報庁	NSA 国家安全保障庁	NGA 国家地理空間諜報庁	DIA 国防諜報庁
英	セキュリティ・サービス 安全保障局	SIS 秘密諜報局	GCHQ 政府通信本部	国防省DIJE	DIS 国防諜報局
豪	ASIO 豪安全保障諜報局	ASIS 豪秘密諜報局	ASD 豪信号局	AGO 豪地理空間諜報局	DIO 国防諜報局
加	CSIS 加安全保障諜報局	—	CSE 通信安全保障局	国防省地理空間諜報局	？
独	BfV 連邦憲法擁護庁	BND（連邦諜報局）			MAD 軍諜報局
仏	DGSI 対内安全保障総局	DGSE（対外安全保障総局）			DRM 軍諜報局

17

17

3-1（4）シギントの重要性

元米国家テロ対策センター長
マイケル・ライター

「NSAが傑出した選手或いは中心プレーヤーでなかったテロ調査・捜査というのは思い付かない。」

「NSAほどアルカイダの内部状況について知見を与えてくれたものはなかった。」

18

18

内　容

19

19

3-2-1　（1）UKUSAシギント同盟

- 1940年4月　英米諜報協力を協議
- 1940年12月　英米シギント協力で合意
- 1941年2月　実務レベル協力開始（ロンドン、シンガポール）
- 1946年3月　BRUSA協定締結（British-USA）
- 1954年　　UKUSA協定（UK-USA）と改称
- 他の3国の正式参加　UKUSA、FVEY（Five Eyes）
  - 加～1949年（CANUSA協定）
  - 豪、NZ～1956年（UKUSA附属文書J1記載）
- 2010年　UKUSA協定・情報開示

20

20

3-2-1　（2）米国NSA

NSA（National Security Agency）国家安全保障庁

1952年設立、1975年存在を公認

○ 職員：2013年定数　3万4901人（軍人1万4950人）

2018年報道：正規職員3万8千、契約職員1万7千人

加えて、陸海空軍・海兵隊・沿岸警備隊のシギント部隊を指揮下に。

○ 予算　：

2018会計年度諜報機関予算

国家諜報予算＋軍諜報予算＝合計

594億ドル　　212億ドル　　815億ドル

2013年

シギント予算＝NSA108億＋NRO＋軍予算他

総計、200億ドル、2兆円規模？

21

21

3-2-1　（3）英・加・豪・NZ

Second Party諸国

英：　GCHQ政府通信本部：約6千人、15億ポンド＋

加：　CSE通信保全局：約2千人、5億カナダドル程度？

豪：　ASD豪信号局：約2千人

NZ：GCSB政府通信保全局：430人、1億6千NZドル

共同の収集分析、共同のシステム構築など

統合運用の段階

22

22

3-2-1　（4）協力組織・国

（1）SSO（Special Source Op.特別資料源作戦）

民間企業の協力を得て行うシギント資料収集

NSAの収集データの内、コンテンツ情報の60%、

メタデータ情報の75%近くを占める

（2）Third Partyとの協力（パートナー＆標的、ギブ＆テイク）

（2013年現在33ケ国）

＜欧州＞18国：独、仏、伊、西、蘭、ベルギー、デンマーク、
ノルウェー、スウェーデン、フィンランド、墺、ポーランド、チェコ、
ハンガリー、クロアチア、ギリシャ、マケドニア、ルーマニア

＜アフリカ＞3国：アルジェリア、チュニジア、エチオピア

＜中東＞5国：イスラエル、トルコ、ヨルダン、サウジ、UAE

＜アジア＞7国：シンガポール、韓国、タイ、インド、日本、
台湾、パキスタン

23

23

3-2-2　収集プラットフォーム

NSAの主要な収集プラットフォーム

（1）「プリズム」計画（Downstream）

（2）通信基幹回線からの収集（Upstream）

（3）外国衛星通信の傍受　FORNSAT

（4）SCS（特別収集サービス）

（5）CNE（コンピュータ・ネットワーク資源開拓）

（6）シギント衛星・機上収集　Overhead

（7）従来型収集（無線通信の傍受）Conventional

（8）秘匿シギント活動　CLANSIG

24

24

3-2-2　（1）「プリズム」計画

協力企業の米国内データセンターから必要な情報を随時、検索取得

- ○ SSO（特別資料源作戦）の一つ
- ○ 2007年開始　　参加協力企業
  - 2007年　マイクロソフト
  - 2008年　ヤフー
  - 2009年　グーグル、フェイスブック、パルトーク
  - 2010年　ユーチューブ
  - 2011年　スカイプ、AOL
  - 2012年　アップル
- ○ 取得情報
  - ・ コンテンツ情報：メール、文章、音声、写真、ビデオ等
  - ・ メタ情報：メールアドレス、電話番号、通信時刻、位置等

（参考）2013年中に約2億5千万件以上のデータを取得

25

25

3-2-2　（2）通信基幹回線

世界中で通信基幹回線から収集

- ○ 企業協力　　4計画
  - 「ブラーニー」（米国内）30社以上、アクセス拠点70ヶ所以上
  - 「フェアビュー」ATT「ストームブリュー」ベライゾン（米国内）
  - 「オークスター」小計画8つ　　（殆ど米国外）
- ○ UKUSA＆Third Partyの協力　2計画
  - 「ウィンドストップ」～UKUSA諸国小計画4つ　（米国外）
  - 「ランパート A」～Third　Party　小計画多数　（米国外）
- ○ 単独事業　　5計画　　（米国外）
  - 「ミスティック」　小計画5つ
  - 「ランパートI/X」「ランパートM」「ランパートT」
  - 名称不明の1計画

26

26

3-2-2 （3）衛星通信の傍受

世界各地で衛星通信を受信

○ 主要傍受施設 12ヶ所

米本土 ： ヴァージニア州、ワシントン州
英国 ： メンウィズ・ヒル、ビュード
中東 ： キプロス、オマーン
アジア ： 日本・三沢 、フィリピン、タイ・コンケン
大洋州 ： 豪ジェラルドトン、豪ショアルベイ、
ニュージーランド

○ 特別収集サービス 約40ヶ所

（大使館、領事館等）

27

27

3-2-2 （4）特別収集サービス

SCS（Special Collection Service）

○ CIAとNSAの共同事業
○ 米大使館・領事館 ～各種アンテナを偽装して設置
○ 2010年現在 世界 約80箇所

内、欧州19（ベルリン、フランクフルト、パリ、
マドリッド、ローマ、プラハ、ジュネーブ等）

○ マイクロ波、 衛星通信、
WiFi、WiMAX等無線LAN、 携帯電話
○ その他UKUSA諸国の外交施設にも設置

28

28

3-2-2 （5）CNE（コンピュータ網資源開拓）

CNE（Computer Network Exploitation）

① 標的システムからデータを取得する

② 標的システムへのアクセスを獲得する

○ 主体：TAO（Tailored Access Operations）

- 1997年発足　　2013年度定員1870人
- 所在地：本部（Fort Meade）

ROC（地域センター）ハワイ、ジョージア、テキサス、コロラド

○ 成果：システム侵入（マルウェア累計注入件数）

2008年　　2万1252件

2011年　　6万8975件 （運用）8,448件

2013年末計画　8万5000～9万6000件

☆ 操作員不要の自動運用システム開発中

参考：『米国国家安全保障庁の実態研究』2015年警察政策学会資料第82号

29

内　容

30

30

3-3 テロ対策への貢献：米国

（1）2009年9月NY地下鉄同時自爆攻撃未遂事件

NSAは（FISA702条収集で）、アルカイダ連絡員（パキスタン拠点）のEメールアドレスを監視。9月上旬米国内の不明人物から同アドレスへのメール複数を捕捉。爆弾の作成方法の詳細について緊急に助言を求めていると推定し、FBIに通報。

FBIはNSLを発出して情報収集、コロラド州のナジブラ・ザジと特定。FBIは、秘密捜索やインターネット監視など、徹底した監視を実行。ザジは高校の同窓生2人と、NY市マンハッタンでTATP爆弾による地下鉄自爆攻撃（3箇所）を計画。

ザジは10日にNY市に移動したが、警察やFBIによる監視に気が付き、テロ実行を中止して爆弾材料を処分し、コロラドに戻ったが、逮捕された。

出典：PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA,* 2 July 2014

31

3-3 テロ対策への貢献：米国

（2）外国のテロ対策への貢献

事例①　FISA702条収集によって某国内にアルカイダ同調者を発見。CIAが当該国政府に通報。

同国政府機関は、同人を調査した上で、協力者として獲得。

同人は同国内のアルカイダとIS関係者に関して情報を提供。

事例②　CIAが、FISA702条収集（プリズム）によって写真他の詳細情報を入手してアフリカ某国政府に提供。

同政府は、IS戦闘員2名を逮捕。同人らはトルコから入国し、米国人と米国権益に対する近々の攻撃計画に関与。

逮捕により、CIAはISの組織や攻撃計画に関する情報を獲得。

出典：ODNI, *The FISA Amendments Act: Q&A,*18 April 2017

32

3-3　テロ対策への貢献：英国

（1）2007年英国兵士に対する誘拐殺人テロ阻止

テログループが、英国内でイスラム教徒の英国兵士を誘拐し殺害を立案。犯行状況をビデオ撮影し、海外関係者に送信して海外で公開企図。通信メタデータの通信パターン分析により、セキュリテイと諜報諸機関は、同グループを発見。

警察が関係施設の捜索、誘拐殺人計画を確認。

（2）2014年西側某国における爆弾テロ阻止

セキュリティと諜報諸機関のシギント情報の分析から、シリア内IS関係過激派と接触を持っている某国の者を特定。更なる分析により、同人が最近欧州の某国を訪問したこと、テロ攻撃を計画していることが判明。 関係国政府に情報を提供。同国政府は攻撃を阻止、手製爆弾数個を押収。

出典： UK Home Office、*Operational Case for Bulk Powers*, 1 March 2016

参考「オサマ・ビンラディンを追え（下）テロ対策に活用できるシギント能力」『現代警察』第157号

33

33

内　容

34

34

４　その他の課題

平成28年版『警察白書』特集：米英仏独の対策例

◎　テロ関係情報の集約・分析

2017年7月「セキュリティ情報センター」（警察庁）

2018年8月「国際テロ対策等情報共有センター」（内閣官房）

◎　テロ周辺行為（準備、支援、唱道など）犯罪化

2017年テロ等準備罪制定で充足されたのか？

◎　通信傍受（行政傍受）

◎　テロ関係容疑者に対する各種行動制限

身体拘束、居住制限、出入国制限等

35

35

４　その他の課題

他の諸課題

◎　業務情報（金融・通信等）の安全保障目的収集

個人情報保護法の解釈問題？

米National Security Letter

◎　通信メタデータの扱い

通信メタデータは「通信の秘密」に含まれない（諸外国）

通信履歴の保存義務

◎　重要施設従業員の適格性の審査制度

原発、原子力関連だけ？

◎　外国人管理の思想

出入国管理

在留管理の担保措置（住民登録情報、宿泊カード他）

36

36

４　その他の課題

＜通常の民主主義国家にあるもの＞

◎　調査権限を持つセキュリティ・サービス

調査権限～通信傍受、侵入的監視、潜入他

憲法35条の問題～行政通信傍受・監視裁判所の設置？

調査権限～一般行政・業務情報へのアクセス権

◎　調査権限を持つ国家シギント機関

通信事業者の協力義務

◎　総合治安担当省（＝内務省）

通常、内務大臣の指揮下にある関係機関

警察（警察庁）、セキュリティ・サービス（？）、

国境警備（海上保安庁）、外国人管理（入管庁）、消防

総合治安に責任を有する閣僚が不在

37

37

内　　容

38

38

まとめ

☆　脆弱性と不十分性の自覚

☆　実態を前提とした議論

○　欧米型のテロ対策に進むのか？

○　違いを認識しつつ現状の構造を維持？

※　情報収集力の弱体は
　　スパイ対策の弱体や
　　サイバーセキュリティ対策の弱体とも関連

39

39

内　容

ご清聴ありがとうございました。

40

40

国民保護における避難

―武力攻撃・大規模テロが本当に起きたら住民はどうなるのか―

防衛大学校国際関係学科教授　宮坂直史

＜目次＞

はじめに　国民を保護するための訓練が国民を危険に曝していないか

国民保護とは、日本に対して武力攻撃が加えられた場合や、その発生が迫っているような場合、あるいは大規模テロが生じた場合に、その被災地域または被害を受けそうな地域に居る者の生命や財産を守るための仕組みである。これは、2004 年に制定された「武力攻撃事態等における国民の保護のための措置に関する法律」（以下、国民保護法）が根拠法となっている。

日本では有事法制の議論が長年にわたって燻る中、特に 1990 年代以降の朝鮮半島情勢の緊迫化と、2001 年の 9.11 テロ後の国際情勢を受けて、2003 年に「武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律」（いわゆる事態対処法）が成立した。それに伴い翌年、新たに制定された、あるいは改正された有事関連法の 1 つが国民保護法ということになる。

その内容は、国が地方公共団体を通じて、該当する人々（「国民」や「住民」とは限らず、その場に居合わせた人々も含む）に対して避難を促し、避難者に救援を差し伸べ、そして武力攻撃によってもたらされる人的、物的災害に対処するというもので、これらが国民保護措置の中心を成している[1]。

そして、国民保護法制定以来、日本全国で国民保護訓練が多数行われてきた。地方自治体を中心に、消防、警察、自衛隊、海上保安庁、医療機関など多数の機関が合同で、戦争や大規模テロを想定して取り組むのだが、同法の制定以前はそのような訓練は行われなかった。だからこの進展は非常に画期的なことである。

ところが、国民保護訓練には大きな問題がある。シナリオ・想定のワンパターン化や、1 度の訓練で事案の詰め込み過ぎによる消化不良、訓練格差とでもいうべき自治体間の訓練回数の違いなどが見られるが、筆者が感じている最大の問題は、避難の在り方そのものに他ならない。何回となく訓練現場に立ち会っていると、「なぜこの想定で多数の住民を避難させるのか」「避難の道中や避難先が安全だという情報を得ているのか」「なぜ行政機関が避難を誘導しなければならいのか」「訓練で想定している事態が本当に起きたら行政機関が避難誘導などできるのか」、このような疑問が繰り返し浮かび、脳裏から離れない。

---

1 国民保護措置は本来、武力攻撃事態（外国からの、主に軍による攻撃）を想定したものである。しかし、国民保護法の第8章に記されているように緊急対処事態にも、国民保護措置に準じた措置（緊急対処保護措置）を実施することになっている。本稿では、国民保護措置と緊急対処保護措置を合わせて、国民保護措置の問題として扱う。なお、緊急対処事態とは「武力攻撃の手段に準ずる手段を用いて多数の人を殺傷する行為が発生した事態又は当該行為が発生する明白な危険が切迫していると認められるに至った事態で、国家として緊急に対処することが必要なものをいう」と定義される（「武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律」、いわゆる事態対処法の第 22 条）。政府が例示するのは NBC（核・生物・化学）テロ、重要インフラや集客施設への攻撃、ハイジャックによる自爆攻撃などであり、一般的に言えば大規模テロに相当する。通常の小規模なテロはここにはあてはまらない。ただし、死傷数などの数値が、緊急対処事態に相当するか否かの基準に定められているわけではない。

１つ２つの訓練だけが問題なのではなく、おかしな訓練が全国で常態化しており、何か変だと担当者が気づいても、彼らがその疑問を公の場で発言することはまずない。国民保護を所管している総務省消防庁内でのある会議の席上で、最近、救命救急の医者が、国民保護のある手順を指して、「国民を保護する訓練ではなく、国民を殺す訓練をやっているのではないか」と発言したことがあるが、人々の生死が係る避難についても同じ問いを投げかけたい。避難とは何なのか、そして武力攻撃や大規模テロが発生したら現場はどうなるのか、そういう根本の部分から国民保護の在り方を見つめ直さねばならない。

本稿の構成は以下の通りである。１章で国民保護訓練とは何か、その概要を述べて問題点を挙げる。2 章では、そもそも避難とは何かを整理する。避難はいくつかに類型化でき、行政機関が誘導するような避難はいかなる場合に有効で、いかなる場合に不向きなのかを考えてみる。3 章では、国民保護法において避難がどのように規定されているかを確認する。法律上は、武力攻撃やテロが起きたら自動的に屋外避難させるとはなっていない、むしろ慎重な判断が求められている。4 章では戦争やテロの場合、前もって避難を準備したり、事が起きてから避難させたりすることがどこまで可能で必要なのか、自然災害と対比しながら明らかにする。5 章では、現実の世界で起きている戦争やテロと、国民保護の担当者が想像している武力攻撃事態や緊急対処事態との間にどのようなギャップがあるのかをみる。そして最後に、いかなる訓練が求められるかを述べたい。

第１章　国民保護訓練と避難実施要領

１　訓練概説

（１）訓練の形式

国民保護訓練は、国民保護法制定（2004 年）の翌年度から現在にいたるまで全国各地で実施されており、日本に対する武力攻撃や日本国内での大規模テロの発生を想定して、関係する多機関が合同で取り組むものである。

国民保護訓練はその主催者の違いから大きく２つに分けられる。１つは、国と都道府県の共同訓練である。国、つまり国民保護を所管する内閣官房副長官補（安全保障・危機管理）と総務省消防庁が、都道府県ごとに共同で実施するもので、2005 年度から 2019 年度末までに全国で 226 回行われている。この共同訓練の概要（日時、場所、訓練想定概要など）は、内閣官房の「国民保護ポータルサイト」に公開されている[2]。訓練を実施した県庁やそれに参加した市役所のホームページにも、参加機関名を含めて概要が記載されていることもある。

もう１つは、国との共同ではなく、自治体（都道府県や市）が単独で企画し、関係機関に

[2]「内閣官房国民保護ポータルサイト」(www.kokuminhogo.go.jp)の中の[国民保護訓練]を参照。

呼びかけて実施する訓練である。どの自治体でも取り組んでいるわけではなく、毎年のように実施している自治体がある一方で、全く未経験の自治体も多数あると思われる[3]。

いずれの訓練でも、そこに参加する機関が法律などで指定されているわけではないが、定番と言えるようなラインアップはある。例えば〇県でやるならば、〇県庁の危機管理担当部局、そのときの訓練でテロが起きる場所が〇県△市ならば、△市役所の危機管理担当部局、△市消防局、〇県警（本部もしくは△市内の警察署の警備課）、〇県内の自衛隊（特に陸上自衛隊は、奈良県以外の全都道府県に駐屯しているのでほぼ必ず参加する）や海上保安庁、そのほか指定公共機関や医療機関、日本赤十字社、訓練シナリオに関係する事業者（例えば鉄道テロならば、その会社）などになる。

国との共同訓練の場合、所管する内閣官房や消防庁の職員も現場には来るが、上記機関のように「プレーヤー」として参加するのではなく、評価員役その他の視察に回る方が多い。実際に事が起きれば国自体が不可欠な「プレーヤー」になるのだが、訓練の中で他の機関と一緒になって苦悩し、汗を流すということは、まずない。

参加者数は、以上の関係機関（プレーヤーになる）だけでもおおむね 100 人以上になり、実働訓練[4]の場合はさらに避難者役や被害者役として市民が参加することもある。今では負傷者用のメイクも手が込んでいて、地元のデザイン専門学校の学生が参加してくれたりすると見栄えもよい。

どちらかというと、自治体単独企画の方が目的や目標を絞った地に足が着いた訓練が多い印象である。国（内閣官房と総務省消防庁）が入ってくると、訓練に画一的なパターン化を求めることがあり、そのような訓練では手順を確認するだけに終始して、手順そのものに内在する問題が見過ごされてしまう。

（２）訓練の全国への浸透

何はともあれ、大規模テロや武力攻撃が起きたという想定で行う訓練が、マスコミにもオープンにして全国各地で実施されるのは、国民保護法制定以前の日本では想像できない光景であった。戦争やテロで多数が死ぬ想定など、言霊信仰が残ると言われる日本では議論すら憚れる風潮があったし、戦争やテロは起きないように対策を打つ方が重要だという言説が根強かった。そのような訓練をやること自体が戦争やテロを誘発する、という何ら科学的根拠のない感情的非難さえも堂々と罷り通っていた。

---

[3] 「内閣官房国民保護ポータルサイト」によると、国と都道府県の共同訓練以外の、地方公共団体による単独訓練は、2008 年度から 2018 年度の間に総計 546 回行われていることになっている。それらがどの自治体で、どのような形式、内容で実施されているのかまでは記載されていないし、筆者も全貌を把握していない。筆者が監修役として 2008 年度から毎年関わっている横須賀市では、2019 年度まで 13 年連続で国民保護訓練を実施しており、毎回、想定や形式を変えている。それらの概要については横須賀市役所のホームページに紹介されている。

[4] 実働訓練とは、事案の現場に見立てた場所（屋外もしくは施設内）で車両、器材、装備を使用しながら基本動作や手順を確かめること。他方で図上訓練は、庁内などで行うもので、統制役（コントローラー）から対策本部や各部署に状況が次々に付与され、それに応じて机上で取り組む。

国民保護が画期的なことは、先にも例示したように多機関合同での取り組みであることだ。訓練にしても、市役所と市消防、都道府県庁と都道府県警、自衛隊、海上保安庁、医療機関などが合同で行うことに意義がある。このうち自衛隊には侵略の排除、警察にはテロリストの捕縛など主たる任務がある。とはいっても、警察官も自衛隊員も消防吏員と同じく被災現場で救命救助に加わったり、不審物の処理にあたったり、避難や救援の面でも自治体職員などをサポートしたりする機会もあるわけで、国民保護の措置において重要な一翼を担っている（法令上、指定行政機関に定められている）。だから、全国で実施されている国民保護訓練に参加するのは至極当然で、逆に、自衛官や警察官がいないと「今日は何かあったのか」と勘ぐられしまうくらいである。

また、自治体が中心になって取り組むことも、安全保障政策上の転機である。県庁や市役所の担当が「CBRN」（シーバーンと読む。化学剤、生物剤、放射性物質、核爆発それぞれの頭文字を重ねた造語で、広く国際的に使用されている）と口にしても今では何ら違和感がない。実際の訓練の準備は自治体職員（プロパーの事務官、警察からの出向者や異動した消防職員、あるいは元自衛官が退官後に任命される危機管理監など）が中心になって行われる。訓練には先に述べたように一般住民が参加することもある。このような地域的、職域上の広がりは、安全保障の問題を自身の身辺防護の問題として考える人々が増えることを意味するから、戦後日本に欠如していたシビルディフェンス（市民防衛または民間防衛）の活性化に繋がるかもしれない。

（３）地域間格差

その反面、今までの訓練にはいくつか大きな問題も露わになっている。まず訓練回数の問題である。それは法律や政令で定められているわけではない。国民保護法では訓練の実施は努力義務として規定されているにとどまる（42 条）。定期的に実施することを要請する通達が毎年発せられているわけでもない。他県がやっているからウチもやらねばならないという同調圧力や、議員、市民からの強い要望があるという話も各地の担当者から聞いたことがない。そうなると、常にやらねばならない業務に追われる中で、国民保護訓練をやる・やらないは多分に属人的な要因に左右される。危機管理担当部局にやる気があれば訓練は行われる。そうでなければやらないということになるのだろう。

その結果、国と都道府県の共同訓練に限っていえば、2005 年度以降、12 回（最多）実施している県がある一方で、2 回しか実施していない県もいくつかある。訓練は中身も問われるので、ただやればよいわけではないが、やらないのはより以上に問題である。担当者の異動を考えると、2 年に 1 回もやらないとなると訓練経験を引き継ぐことはできない。前回の訓練で何か問題があっても、次にやるときはリセットされてしまう。

また、地域間格差も望ましくない。大規模テロは都会で起きるものという思い込みがあれば、それは間違っている。テロリストにはさまざまな目的があるのだから、目的に応じて攻撃目標も変えてくる。例えば、オウム真理教による松本サリン事件は、松本市という地方都

市で起きた[5]。その死傷者から見ても、今ならば国民保護の事態認定に相当する事案であろう。

武力攻撃も同様である。弾道ミサイルであればどこに飛来するか分からないし、有事の際に真っ先に標的になる米軍基地や自衛隊駐屯地は日本全国に点在している。武力攻撃にサイバー攻撃は付随するものであり、それが銃後の市民生活に影響を及ぼすことは避けられない。ましてや大規模な避難を考えると、同一の市内、県内だけで完結する問題ではない。国民保護訓練は全国均一的な回数で行われるべきであって、自治体間で大きな格差があるのは望ましくない。

（４）大規模テロに偏重する想定

もう１つの問題は、訓練想定の偏りである。国民保護訓練の想定は、本来の武力攻撃事態よりも、緊急対処事態（＝大規模テロ）を想定した訓練が圧倒的に多い（100%に近い）。なぜそうなのかは幾つかの理由があるだろう。武力攻撃を想定するとシナリオも大規模になるし準備も大変になりそうだと尻込みしがちなのであろう。被害想定をどう立てるのかよく分からない。難易度の高い応用問題なのであろう。それに対して大規模テロならば国内でオウム事件もあったことだし、手が着けられる基礎問題に映るのだろう[6]。2005 年の最初の訓練が大規模テロ想定で行われたので、それに続く多くの訓練は、この初回モデルを踏襲する習性に無意識に引きずられているのも間違いない。加えて 2000 年代は世界的にみてもテロの時代であることがかなり大きく影響しているだろう。この間、日本では大規模テロが起きてはいないが、日本でもそれが起きるかもしれないという漠然とした不安は、いくつかの世論調査でもかなり明確に示されていた。

だが現実に目を向けると、日本国内を含め日本の周辺国に大規模テロを実行できるテロ組織は存在しない。また、かつてアルカイダ系グループや「イスラム国」が日本や日本人を標的にすると公言したが（日本だけを標的にすると言ったのではない）、それらを含めて「外国人の国際テロ組織」が日本に乗り込んで大規模テロを行う（これが日本の訓練想定に最も使われる）というのは可能性こそゼロではないが、蓋然性で測るとどうなのか。これは比較の問題になるが、例えばインドが海外テロ組織による大規模テロを想定するのは、隣国パキスタンにインドを敵対視するテロ組織が存在し、実際に起こしているから当然である。日本は東アジアにおいて、インド的な状況には置かれていない。日本を取り巻く東アジアの国際環境を考えた場合は、国際テロリストの密入国以上に、周辺国と軍事的な緊張状態がエスカレ

---

[5] オウム真理教は松本地方裁判所で民事訴訟を係争中に裁判官を殺害しようとした。だが、サリンとその噴霧器を搭載した車両で同裁判所に到着したのは午後 5 時を過ぎた閉所時間だった。そこで裁判官官舎のある近くの住宅街に移動してサリンを一帯に散布した。その結果、死者 8 名、重軽傷者は 600 名（裁判官を含む）になった。松本市は事件当時（1994 年）、人口約 20 万の地方都市である。

[6] 筆者は、地方公共団体の国民保護担当者にインタビュー調査をした時に、西日本のある県から、「テロは基礎問題、武力攻撃事態は応用問題」であり、「本県は基礎からやる。特にサリンが基礎。戦争や核爆発の想定はタブーだとか、反対があって訓練をしないわけではない」という回答を得たことがある。なぜテロやサリンを基礎と考えるのか、筆者には今でもその基礎の意味が分からない。

ートして、たとえ限定的であっても交戦状態を迎える状況のほうが現実的というものだ。国民保護訓練のほぼすべてがテロ想定というのは、やはり望ましくはない。

勿論、日本国内でテロを想定した訓練を行うこと自体は不要どころか必須である。海外のテロでも、過去の日本国内のテロでも現実には連続で起きたり同時多発であったりするのは珍しくない。だがそうは言っても国民保護訓練のテロ想定は、あまりに現実離れして発生事案の詰め込めすぎと思えるものが多い。それもパターン化している。県内の多数集客施設やイベントの最中に爆弾テロが起き、化学剤、生物剤あるいは放射性物質も使用され、別の場所で人質も多数とられるなど、短時間の間に数件の大量殺傷もしくは重大テロが次々に起き、結果として 3〜4 桁もの死傷者が出る。参加者は自身の作業で手一杯で、全体的な動きなど考える暇も与えられないほど訓練が分刻みに進行する。

しかも、本当にそのようなことが立て続けに起これば、関係機関が対応するのは恐ろしく難しいはずなのに、訓練では問題なく対応できた、連携できたことにしてしまう。そういう訓練も筆者は目撃してきた。これでは訓練をやったというアリバイ作りにすぎない。

２　訓練における避難の場面

そして何よりも訓練の最大の問題は避難である。なぜならば、避難はそのやり方が生死に係わるからである。国民保護訓練における避難は、被災現場もしくはその周辺に居て、自ら動ける者多数を、行政機関が誘導してわざわざ別の場所に誘導するという形をとる。訓練の具体例を挙げておこう。

【例１】鉄道駅の構内で爆弾テロもしくは化学テロが発生する。その駅を中心に半径数百メートルを「警戒区域」（ここから出ない者には罰則を科すことができる）を設定して、その中にいる多数の者を区域外の避難場所（屋外の公園など）に徒歩で連れていき、そこからさらに避難所（屋根付きの体育館や公民館のこと）に搬送する。

【例２】野球やサッカーのスタジアムの観客席で爆発が起き、化学剤が散布され、多数が倒れている。その死傷者を遥かにに上回る何千何万人もの観客を、スタジアムの外に呼んだバスに乗せて、近くの避難所へ行政機関の者が連れて行く。（実働訓練では何千何万人も避難者役で動員できないので、あくまでそうするという想定）

【例 3】ショッピング・モールのなかで不審物が発見された。見つかっただけの段階でモールにいた多くの利用客を徒歩やバスでまとめて避難所へ行政機関の者が誘導する。

いずれも特異な例ではなく、このような想定は全国どこでもよく見られる。これらの想定ではいずれもテロリストは捕まっていないし、そもそも何人いるかもわかっておらず、１つ

の自治体の中で連続テロが起きることになっている。その中を、行政機関の職員（県庁や市役所の危機管理担当部署、警察官、消防吏員など）が被災現場で市民や利用客を誘導する形をとるのがパターンである。特別な警戒態勢下に置かれているようなイベントにおいては、その現場にも多数の警察官などが配置されているであろう。しかしそうでなければ、事件の一報を受けて現場に駆けつけ、それから避難誘導を始めることになるので時間がかかる。

集客施設でテロに遭遇した人は、負傷者でも自力で動ければ、一刻も早くそこから逃げ出すだけであろう。なぜ行政の職員が現場に到着するまで待っていて、避難所へ連れていかれなければならないのだろうか。負傷者は病院に行き、無症状者ならば帰宅する。

テロリストが何人で今どこにいるのか分からず、そのような中を、統制のとれない市民大勢に集団で道路を歩かせる、あるいは多数のバスに乗車させ（すぐに手配できるのか？）、避難所に連れていく。それは救急搬送や救護活動、捜査や検問の邪魔になるし、そういう避難は短時間、迅速にできない。そして何よりも危険である。

最近、交番で拳銃を強奪した者がそのまま逃亡したり（大阪・吹田市）、かつては寺で飼育していた虎が檻から脱走したりしたことがある（千葉・君津市）。その時、付近の住民多数を自宅から避難所へ連れていっただろうか。これらと、テロリストが徘徊しているケースとどこが違うのだろうか。どちらも屋内待避を呼びかけるのが常識である。諸外国のテロ事件をみても、テロリストが武器をもって移動しながら銃撃しているとか逃走していれば、外出禁止令が出るのが普通である。だが国民保護訓練では、人々を屋外に引っ張り出している。子供が考えてもおかしなことに全国で取り組んでいるのである。

３　避難実施要領パターン

消防庁は、自治体に対して「避難実施要領パターン」を作成させている。「避難実施要領」とは、避難経路、避難手段（徒歩か車両か）、職員の配置などについて細かく記載する書類であり、避難の指示が国から下された際には、市町村が作成しなければならないことになっている（国民保護法第 61 条）。だが、実際に事が起きてからそれをイチから作成するのでは避難に取り掛かるまで時間がかかりすぎるので、平素から「避難実施要領パターン」として、つまり雛形として作成しておくように国は自治体に要請している。

作成にあたってはまず事案を想定するのだが、イベント会場での爆弾テロなどから始めるように消防庁は「避難実施要領パターンのつくり方」を通じて奨励している[7]。このマニュアルは、自治体の実例を盛り込みながら、テロ発生地を中心に半径数百メートルの要避難地域を設定し、住民基本台帳をもとに避難人数を推計、そこから避難先、手段や経路を決めて素案に書き込む流れを紹介している。

---

[7] 消防庁国民保護室・国民保護運用室「避難実施要領パターンのつくり方」（平成 30 年 10 月、全 10 スライド）、消防庁国民保護室「避難実施要領パターン作成の手引き」（平成 23 年 10 月、全 66 頁）など。いずれも消防庁のホームページから全文をダウンロードできる。

『平成 30 年版消防白書』によれば、2018 年 4 月 1 日時点で「避難実施要領パターン」作成済みは全市区町村の 52%にすぎない。作成していない理由はノウハウの欠如と日常業務の多忙などとされている。だが、あらかじめ雛型を作っておいても、事が起きたときに依拠するマニュアルにはならない。想定したことと全く同じことはまず起きない。武力攻撃やテロは発生も事態展開も単純なパターン化を許さないほど多様である。どこに避難させるのが安全かは、事案が起きてからその性質と事態の推移を読み解かなければ判断できない。

避難自体の重要性は疑う余地がない。だが、避難といっても多様な方法があるし（次の 2 章で提示する）、それが必要か不要か、必要ならば実行のタイミングも判断しなければならない。

武力攻撃は国家が、テロは組織または個人が目的をもって引き起こす行為であり、それに対処する各機関の能力と意志があいまって、事態がどのように展開するかはパターン化しがたい。一か所に対する一回限りの攻撃なのか、二回目以降はどこであるのか、攻撃にはどの程度の威力の武器が使われるのか、被害の範囲がどこまで及ぶのかなどは、過去の内外の事案に照らしても予測できるものではない（4 章で詳述する）。

したがって、避難の要否やその方法の判断は、ケースバイケースとならざるをえない。特に避難のために外を移動している最中や避難先で被害に巻き込まれる可能性を考える必要がある。自然災害でさえ、警報の出し方から避難までを画一的にマニュアル化はできない。

武力攻撃や大規模テロは、自然災害以上に事態の展開を予測するのが困難なはずである。それにもかかわらず、国民保護の世界は、日常的に実施されている訓練やさまざまな計画の策定において、まず屋外避難ありきで、しかも行政機関の職員によって無症状で自宅が損壊しているわけでもない、偶然にもテロなどの現場に居合わせた不特定多数の施設利用客や周辺住民を避難所に誘導することが何の疑いもなく擦り込まれてしまっている。

第 2 章　避難方法の多様性

1　屋内・屋外間の動き

われわれは避難という言葉から、現在地 A を離れて、別の場所 B へ移動することを真っ先に想起するであろう。この動作は、現在地 A に留まるよりは B のほうが安全である、あるいは物理的に A には留まれない（例、自宅の損壊）という判断によって始められる。だが、移動するリスクの方が高いと思えば現在地に待避する。地震が起きてまずは机の下に身をかがめることも、爆発や銃撃に遭遇しその場でとっさに身を伏せるのも難を逃れる動作であるから、広義の避難に含まれる。

つまり避難とは、生命に係る災難、あるいは日常の生活や業務を阻害する災難から逃れて身の安全を確保する動作であると定義できる。

避難は【図１】に示したように、屋内・屋外を区分した移動種別によって４通りに分けられる。まずは、屋内から屋内への避難（同一建物の中での避難）がある。例えば、浸水が急迫しており同じ建物の上階に移動したり、空爆や砲撃から逃れるために逆に地階に移動したりするような「垂直避難」といわれる動作がある。また、複合施設やオフィスビル、学校の中などに銃で武装した者が侵入してきたことを感知すれば、むやみに部屋から出ずに、ドアに机などを積み立てて消灯し、音をたてず立て籠もりしばらく様子をみる。いわゆるロックダウンと言われる避難だ。新型コロナウィスルのパンデミックのおかげで、ロックダウンは大掛かりな都市封鎖を意味する用語として普及してしまったが、より日常的には部屋や建物から出ないことで、アメリカの学校でロックダウン・ドリルといえば武装侵入者対処訓練を指す。

他にも外で暴動が起きていたり、凶悪犯が脱走していたり、有害物質が漂っていたり、異常気象であったり、一時的に外に出られない事態はさまざまある。

【図１】避難の動き

→	屋内へ移動	屋外へ移動
屋内から	垂直（上下）避難 屋内退避 侵入者対策のロックダウン	避難場所・避難所へ移動 事件事故に遭遇し外へ出る
屋外から	爆風・衝撃波を回避 有害物質を回避 異常気象を回避	暴走車両､銃乱射から逃げる（その後、建物内に逃げ込む）

作成　宮坂直史

次に、屋内から屋外への避難がある。地震や火災、事件発生などで外に飛び出すということもあるし、自宅の損壊やライフラインの途絶によって、避難場所（例えば公園）や避難所（体育館など公共の建物）への移動を余儀なくされることもある。鉄道・バス・船舶・駐機中の航空機の中で異常が発生し、外に脱出することも屋内から屋外への避難の１つである。

逆に、屋外に居る者が屋内に入る避難もある。ゲリラ豪雨や竜巻の発生など突然の異常気象や、有害物質の大気中への流出、ミサイルの着弾や空爆がありそうだと察知したときも外を歩いているよりも屋内のほうが安全だから、目の前に建物があれば飛び込むであろう。

最後に、屋外から屋外への避難、つまり外に居る者がその場から逃げる。例えば、近年の欧米のテロ事件でよくあるが､暴走車両が向かってきたり､凶器を振り回して暴れていたり、銃の乱射に気づいたりしたときには、一目散に現場から逃げ出す。

２　避難誘導の主体

次に、誰が避難を促すのかという観点から３通りの避難があることを見ておこう。

１つ目は自らの判断で動く、自主・自力避難がある。テロや事故に遭遇して瞬時、反射的に身を伏せたり隠れたりその場から全力で離れる。危険回避の本能的な動作である。現場で多少負傷したが動ける者、現場にいても無傷の者、彼らにとって避難とは自主・自力避難に他ならない。中には「正常性バイアス」に駆られて自分は大丈夫だと現場で妙に冷静にしていたりすることもあるが、それでは助かるものも助からない。自然災害でも、避難勧告が出される前から自主的に避難を始めることもある。

２つ目は、事業者（施設の職員、管理者、そこに雇用された警備員）による誘導のもとに利用客、滞在者が避難する。不特定多数が集まる集客施設（ホテル、ショッピング・モール、駅・ターミナル、競技場、展示場、劇場、複合ビルなど）やイベント会場などでテロ、事件、事故が発生したときに見られる。利用者にとって出口までの経路が不明で右往左往したり、施設内で異常が起きていてもそれを知らない利用客がまだ中にいたりすることは規模が大きければありうる。そういう時に事業者の誘導が生死を分けるかもしれない。介護施設における避難も事業者誘導になるが、事件にせよ事故にせよ自然災害にせよ多くの犠牲者が出ることもままあり、常に難題になっている。

３つ目は、行政機関による誘導である。具体的には警察官、消防吏員、自治体職員、あるいは自衛隊員などが、計画的に大勢の市民の誘導に関わる。これは本来、特定の地域・場所に危険が及ぶことが予想でき、避難させる時間的猶予がある場合に限ってのことであろう。その例としては、人口密集地で不審物、あるいは不発弾が発見され（日本では第二次世界大戦中のそれが現在でも各地で見つかることがある[8]）、その処理の時程を決めてから、周辺住民に一時的に避難してもらうことがある。もう１つのケースは、すでに自宅などが被災している住民を避難所に収容する場合になる。これは行政が避難所の場所を通知するだけかもしれないが、それも含めて誘導としておく。さらに言えば、行政の施設内で異常事態が起きれば、そこの職員なり隊員なりが利用客の誘導避難に動くであろうし、市中でのイベントでも特別の警戒下にあればその場に大勢の警官などが詰めている。何かあれば警官がすぐに動くから行政誘導避難になる。

以上みてきたように、避難は屋内外間の移動をとっても、避難を促す主体からみても、さまざまな方法がある。ある１つの災害に対して１つの避難方法しかないというわけではない。建物に武装侵入者が入ってきた場合でも、それをいつ知覚したか、自分がいま居る場所などによっても、建物の外に逃げるか、それとも部屋でロックダウンするかの違いはある。各自が置かれた状況次第で、ある場合は本能的に、別の場合は総合的な考慮のもとに、各自が避

---

[8] 令和元年度の陸上での自衛隊による不発弾処理は 1441 件（うち沖縄県で 529 件）あった。『朝雲新聞』2020 年 7 月 30 日。

難方法を選択するのが自然である。

３　行政誘導避難への偏重

しかし、国民保護が想定している避難は、自ら動ける者を行政機関が誘導する避難に他ならない。国民保護を所管する総務省消防庁の見解を代弁する一般財団法人日本防火・危機管理促進協会は、全国の自治体に『武力攻撃への備えと対策　国民保護への対応』（2019 年 1 月、全 15 ページ）という冊子を配布しており、そこには武力攻撃や大規模テロがあれば、「市町村の職員、消防官、警察官等が誘導します」と冒頭に書かれてある。

突発的にテロや事故が生じた際に、偶然その場に居あわせながらも動ける身であるならば自力で脱出するか、事業者の誘導に従って現場から離れようとするだろう。自ら動ける者が、行政の職員が来るまでの間、恐怖の中、そこで待っているのか。行政誘導の避難ということは、上記したように、どこで何が起きそうなのかが前もって分かっていて、住民を避難させる時間的余裕がある場合ならば可能であろう。しかも避難所に連れていくのだから、道中も避難所も安全であると目途が立つ場合に限る。4 章と 5 章で後述するが、戦争やテロでそこまで見通せることはまずない。そもそも避難所の立ち上げにも時間がかかる。その間、多数を現場に留め置くのであろうか。それとも公園のような避難場所にまずは連れ出すのだろうか。いずれにせよ、そのようなことをしなければならない理由と、果たしてそのようなことができるのかが問われるのである。

第 3 章　国民保護法における避難

１ 避難の指示、退避の指示

（１）必ず避難指示、ではない

本節では 2004 年に制定された国民保護法において避難の手続きがどのように規定されているかを見ていこう。

まず、国の対策本部長（内閣総理大臣）によって警報が発令（44 条）される。その後、同本部長が「住民の避難（屋内への避難を含む。以下同じ）が必要であると認めるときは、基本指針で定めるところにより、総務大臣を経由し、関係都道府県知事に対し、直ちに、所要の住民の避難に関する措置を講ずべきことを指示する」（52 条、下線は筆者）。

つまり、警報の発令に続いて避難指示が発せられるとは限らない。避難指示はあくまでも避難の必要がある場合に限っている。52 条以下は避難指示が、国から都道府県、都道府県から市町村へ下される手順や内容、あるいは１つの都道府県を超えて避難の必要性がある場合の関係都道府県間の協議などが示されている。

そして 61 条以下が、避難住民の誘導について定めてある。まず、住民の避難を指示された

市町村は、「直ちに、避難実施要領を定めなければならない」。避難実施要領には「避難の経路、避難の手段その他避難の方法に関する事項」「避難住民の誘導の実施方法、避難住民の誘導に係る関係職員の配置その他避難住民の誘導に関する事項」を記載する（61 条）。本稿の１章３節で述べたように、これはいざ事が起きてから書くのでは避難させるのに間に合わないおそれがあるから、国は自治体に対して、平素からパターン化して準備しておくことを求めている。

次に、避難を誘導する者は次のようになっている。「市町村長は、その避難実施要領で定めるところにより、当該市町村の職員並びに消防長及び消防団員を指揮し、避難住民を誘導しなければならない」（62 条）。さらに「市町村長は、避難住民を誘導するために必要があると認めるときは、警察署長、海上保安部長等又は（中略）自衛隊の部隊等の長に対して、警察官、海上保安官又は自衛官による避難住民の誘導を行うよう要請することができる」（63 条）。

これ以下の条文には、誘導する者ができることや、市町村長の上位にあたる都道府県知事の権限、さらには避難にあたっての運送事業者による運送がなされるように規定されている。

繰り返しになるが、国民保護法では、必ず避難させることにはなっていない。同法を円滑に実施するために『国民の保護に関する基本指針』（平成 29 年 12 月最終変更）という文書がある[9]。ここには避難指示の発出の基準についても示されている。「対策本部長は、国民保護法に規定された要件を満たす場合であって、特に必要があると認めるときは、都道府県知事に対し、避難措置の指示、救援の指示及び武力攻撃災害への対処に関する指示を行うものとする」（17 頁）とある。国民保護法の条文の「必要であると認めるとき」に対して、『基本指針』では「特に必要であると認めるとき」とあるように、「特に」という強調的な副詞を追加して避難指示の発出には一層の慎重さを求めている。

さらに『基本指針』には、「対策本部長は、武力攻撃の現状や今後の予測、地理的特性、運送手段の確保の状況等を総合的に勘案し」（20 頁）たうえで避難が必要かどうか判断するとも明記されている。また、避難させるにしても、とくに大都市の場合は混乱の防止のために「まず近傍の屋内施設に避難するよう指示することとする」（21 頁）としている。

このように国民保護法や『基本指針』では、避難させるか否かの判断を求めている。国民保護法には必ず屋外避難させるなどとはどこにも書かれていない。

（２）国からの指示では間に合わない

本当に住民を避難させる場合、国から都道府県、都道府県から市町村への指示という段取りを踏んでいたら初動が遅れる可能性がある。現場の状況を最も把握し得るのは市町村のはずである。ということは、国が避難の指示を出す前に、市町村、都道府県からのアクションも必要になるだろう。そこで、市町村から都道府県への必要な措置の「要請」と、都道府県から国の対策本部長に対する「要請」（97 条）も規定されている。

---

[9] 「内閣官房国民保護ポータルサイト」から全文ダウンロードできる。

しかし、市町村から都道府県、そこから国への「要請」でも一定の時間はかかる。そこで、市町村町（16 条 3 項）と都道府県知事（11 条 1 項）は住民に対して「退避の指示」（退避先の指示も含めて）を出すことができるようになっている。

さらに、知事や市町村長の指示を待つ余裕がない場合には、現場に居る警察官または海上保安官も「退避の指示」を出すことができる。日本語として「退避」と「避難」は同義のはずである。字義からいえば「退避」はその場から離れる、逃れることなので、「避難」の一部（狭義の避難）ということにはなる。国が発すれば「避難」、市町村長や警察官が発すれば「退避」と法律上は用語を使い分けている。

この「退避の指示」、国に対する必要な措置の「要請」は、同法の審議中に都道府県知事や全国市長会、全国町村会との意見交換会を踏まえて同法に反映されたものである。もしこれがなければ、急迫していても現場は動けず、国からの指示を一方的に待つような仕組みになっていたであろう。

２　救援措置

国民保護法では、前節で概観したように第 2 章（第 44 条から 73 条）で避難に関する措置を扱い、続く第 3 章（第 74 条から 96 条）で避難住民等への救援措置について定めている。避難住民等の「等」には、武力攻撃災害による被災者が入る。本来、被災者こそ避難所が必要であることは言うまでもない。だが、運用にあたって、無症状で自力で動ける者や自宅が被災していない者も避難所へ誘導することになってしまっているところが問題である。

救援は避難とセットであり、同時になすべきとされている。救援措置は都道府県および市町村が実施するのだが、具体的には「収容施設の供与」「吹き出しその他による食品の供与及び飲料水の供給」「被服、寝具その他生活必需品の供与または貸与」「医療の提供及び助産」「被災者の捜索及び救出」「埋葬及び火葬」「電話その他の通信設備の提供」（75 条）などである。同条では、避難住民等の中であくまでも「救援を必要としているものに対し（上記の救援のなかで）必要と認めるものを行わなければならない」とされている。

従って法的に言えば、避難所を設営したならば、そこに収容した避難者役の人々からニーズを聞き出すなりして、例えば飲食が必要ならばそれを提供するという手順になるはずである。しかしそこは訓練。避難者役が避難所に到着すれば、すべての人に訓練参加協力への謝意だと思うが弁当と飲み物が提供されることが多い。

たとえ謝意であっても、訓練想定上、避難者役の人の家は破壊もされていない、帰ることができないわけではないのに、なぜ飲食まで提供するのか不思議である。吹き出しは防災訓練のときにやればよい。避難所に行けば弁当とお茶をもらえると思わせてしまうのはかえって良くない。国民保護事態ではもちろん、自然災害のときでも避難所に行ってもすぐには何ももらえない、それどころか入れないことさえある。

避難所で自治体職員が安否情報の収集訓練を行うこともある。それは、「市町村長は（中略）

避難住民及び武力攻撃災害により死亡し又は負傷した住民（中略）の安否に関する情報を収集し、及び整理するよう努めるとともに、都道府県知事に対し、適時に、当該安否情報を報告しなければならない。」（94 条）と規定されているからで、法律施行令（23 条）には、収集すべき情報（氏名、生年月日、男女別、住所、国籍など）も定められている。死者や病院に搬送される負傷者の安否情報ならばわかるが、訓練での避難者役の多くは負傷者ではない。自分で家族や職場に連絡すれば済むことだ。なぜ市町村の職員が、無症状者の安否情報を把握し、都道府県に報告しなければならないのか。94 条に忠実に避難住民全員を対象にしていたらとても人手が足りないし、より重要な業務に取り組めない。この 94 条があるからこそ、無症状者や自宅等が被災していない者をむやみやたらと避難所などに連れてきてはならないのである。

３　災害対策基本法の影響

国民保護法の起案にあたっては、災害対策基本法（以下、災対法）を参考にしたと伝えられている。災対法とは、1959 年に大災害をもたらした伊勢湾台風を契機に 1961 年 11 月に制定された自然災害に関する最も基本的な法律である[10]。防災に重点がおかれ、各機関・地方公共団体による防災計画の作成、災害予防（警報の伝達など）、災害応急対応（避難）などが規定されており、これらは国民保護法に引き継がれている。災対法の所管は総務省消防庁であり、国民保護法の起案も総務省の担当者が内閣官房に出向して中心となって関わってきた。

もっとも自治体にとって、災対法による防災と国民保護は業務上の位置付けが異なる。市町村にとって防災は「自治事務」であり、災害の応急対応の第一次責任は市町村が負うことになっている[11]。他方で国民保護は、国が本来果たすべき役割に係る事務であり、自治体にとっては法律・政令で事務処理が義務付けられる「法定受託事務」になる。

国民保護法は災対法と法律の構成まで似通っているわけではないが、いくつかの条文に至っては、行為の主体を書き替えた程度の違いでほぼ引き写しに他ならない。ここでは、武力攻撃やテロも自然災害と同じように見なしていたのではないかと思える条文を２例ほど取り上げたい。

（１）武力攻撃災害を発見したら通報する？

第１は、発見者の通報義務である。国民保護法では「武力攻撃災害の兆候を発見した者は、遅延なく、その旨を市町村長又は消防官吏、警察官もしくは海上保安官に通報しなければならない」（98 条１項）。これは、災対法の「災害が発生するおそれがある異常な現象を発見した者は、遅滞なく、その旨を市町村長又は警察官若しくは海上保安官に通報しなければならない」（54 条１項）が元になっている。「遅滞」を「遅延」に変えたり、通報相手に消防官吏

---

[10] 津久井進『大災害と法』岩波新書、2012 年、11 頁。なお、災対法には自然災害以外に、石油コンビナート事故や原子力発電所事故も対象に含まれている。全 10 章、117 条からなる。
[11] 同上、33 頁。

を加えたりしているが、引き写しであるのは容易に見て取れる。

「武力攻撃災害の兆候」を発見した者の中で、果たしてどのような人が市町村長に通報することを想定しているのかよく分からない条文であるが、それ以前に「武力攻撃災害の兆候」が何とも分かりにくい。武力攻撃災害とは「武力攻撃により直接又は間接に生じる人の死亡又は負傷、火事、爆発、放射性物質の放出その他の人的又は物的災害」（国民保護法第 2 条 4 項）であると規定されている。発見者は、このような災害現象を目の当たりにしてもそれが武力攻撃つまり他国からの攻撃によるものだと判断できるのか、ましてや「兆候」なるものを「兆候」だと認識できるのか。「兆候」をどのように定義しようと現実問題として適用不能である。敵国の軍事攻撃であることが明確であれば、市民が通報するまでもない。自衛隊もしくはしかるべき機関が覚知するであろう。武力攻撃かテロか事故かに関係なく、死傷者が出たり爆発や火事が起きたりすればどのみち消防と警察には通報される。

この点は災対法の方が分かりやすい。例えば、自宅前の河川が増水し堤防が崩れかかっているのに気づけば、それが「災害が発生するおそれのある異常な現象」（災対法 54 条）と思われるから通報対象になるであろう。だが国民保護法の「武力攻撃災害の兆候」では何を通報するのかさえ不明である。それゆえに「通報しなければならない」という努力義務規定が生きてこないのである。

（２）「警戒区域」が設定できる市町村長

第２の災対法からの引き写しは、市町村長に対して「警戒区域」を設定する権限が付与される条文である。ここは国民保護法の中でも唯一、首長が住民の行動に対して強制力を行使できる点であり注目しなければならない。

繰り返すが、自然災害を前提にした防災は自治事務である。その責務は市町村にあり、災害発生前から市町村長は消防機関や水防団に出動を命じたり、警察官、海上保安官の出動を求めたりすることができるし、必要があればそうしなければならない（災対法 58 条）。市町村長は、居住者に対しても避難のための立退きの勧告や指示も出せる（災対法 60 条）。さらに市町村長は「警戒区域」を設定して、そこへの立ち入り制限、禁止、そこからの退去を命じることができる（罰則規定付き）（災対法 63 条）。主たる責任を有する市町村長に「警戒区域」設定の権限が付与されるのは自然であろう。

一方、国民保護は自治体にとって法定受託事務であり、避難等の指示は国から発せられる。災対法とは違う。だが市町村長には災対法と同様に「警戒区域」を設定する権限が与えられている（国民保護法 114 条）。しかも従わなかった者に 30 万円以下の罰金又は拘留（193 条）という罰則まで同様に規定されている。市町村長による「警戒区域」の設定は、行政誘導の避難を強制することに他ならない。もし「警戒区域」を設定するならば、そこから出る（屋外を移動させる）ほうが危険が減じるという高度な情勢判断に基づかなければならないはずだが、武力攻撃や大規模テロの場合に、市町村長にそれを判断できる情報が地元の警察などから得られるものなのであろうか。結局、国が設定を要請するのであろうか。「警戒区域」の

外へ移動させることで、二次攻撃や二次災害に巻き込まれて訴訟を提起されたらどう対応するのであろうか。市町村は得られた情報から合理的な判断を下したと証明できるのか。国はこのような重大な結果に対する責任を市町村に負わせてよいのだろうか。

第４章　自然災害、事故、戦争、テロ[12]―それぞれの避難

前章では災対法の条文を参考にして国民保護法が起案されたことを述べたが、自然災害時の避難と、戦争・テロのときの避難では何がどう違うのかを整理しておくことは無駄ではないだろう。それは煎じ詰めれば、自然災害と、戦争やテロはいかに違うかということである。勿論それとは逆に、自然災害でも戦争やテロでも、それらが起きた後に取り組む措置には共通項がある。住民への情報提供、救命救急、被災者救援、消火、そして避難をどうするかを考えなければならない点などである。

１　シングル・ハザード・アプローチか、オール・ハザード・アプローチか

ある国がどのような危機対応をしているかについて、「シングル・ハザード・アプローチ」と「オール・ハザード・アプローチ」の分け方がある。前者は想定される事案、災害ごとに対処マニュアルを作っておくことである。一見するときめ細かく用意周到だが、想定外というものが必ず発生する。その隘路に陥ると柔軟性が発揮できない。想定外を口実にして、失敗を自己弁護しかねない。尤も想定通りに事が起こりマニュアル通りに対処できるのであれば、そのような事態は有事でも危機でもなんでもない、単なる平時の出来事にすぎない。

他方、後者は、各機関が有する人員、資機材などの資源をひとまとめにみなして、そこからいくつかの単位分け、モジュール化（標準規格化）をしておく。何か事態が発生したら、その規模に応じてその単位を組み合わせ動員、投入して対処しようとするものである。オール・ハザード（＝あらゆる災害）の名のごとく、細かく事案ごとにマニュアルを作るわけではなく、何にでも対処する構えなので柔軟対応であるともいえる。

日本の公的機関がどちらを採用しているかは言明していない。それでも実態をみると「シングル・ハザード・アプローチ」に近いと思われる。事態ごとに所管を分け、権限を分散し、そして何よりも事案ごとに想定をつくりマニュアル化する傾向があるからだ。

事態の違いばかりを意識するとどうなるか。自然災害での経験が、国民保護行政には反映されなかったりする。「あれは一般的な犯罪だからテロとは違う」と言って無意味に線引きしようとする。自然災害は多発しているから訓練が不可欠だが、国民保護は該当事案がないの

---

12 本章では、武力攻撃事態ではなく「戦争」、緊急対処事態ではなく「テロ」という用語を使用する。一般的な事象として戦争、テロを自然災害や事故と比較するからである。

だから訓練は不要ともなりかねない。国民保護法において、国民保護訓練は「防災訓練との有機的な連携が図られるよう配慮するものとする」（42 条）と書かれているのもその共通項を意識してのことだろう[13]。「オール・ハザード・アプローチ」の考え方を少しは取り入れることは、各種マニュアルの作成に走りがちの日本には必要なことであろう。

ただここで自然災害と戦争・テロの相違を強調しておくことは、「オール・ハザード・アプローチ」を否定したり、「シングル・ハザード・アプローチ」が良いと主張したりするわけではない。自然災害と戦争やテロは、事案の発生から終結まであらゆる局面で違いがあり、その違いこそが避難の在り方、避難の準備に影響を及ぼしていると考えるべきであろう。

まず危機関連の事態を、自然災害（地殻変動によってもたらされるものと、気象現象によってもたらされるもの）、大規模な事故（周囲の人々に避難を意識させる）、戦争、テロに分けてみる。次に、それぞれの「発生の予知」から「事態終結の予測」まで、何がどこまで見通せるのか、それによって避難の準備がどこまで可能なのか、あるいは合理的なのかを比較してみたいと思う。

２　自然災害の予測と避難

自然災害から見ていこう。まず、地殻変動である地震と一部の火山噴火に対しては、起きる前に避難の時間が十分にとれるほどの予知は未だに困難である。それでも、特定地域に将来起きる地震の可能性や、それがどの程度の被害をもたらすかまでは想定できる（例えば南海トラフ）。火山噴火も科学的見地および噴火の履歴から人々に同様の警戒をもたせることができる（例えば富士山）。つまり地震（や津波）、火山噴火に対して計画的に備えを進めることは可能である。

一方、気象現象（台風、豪雨、豪雪、竜巻など）ならば、観測によって特定の地域に予報、警報が出せる。豪雨の際の雨量予測の難しさがたびたび指摘されるなど予測には限界がある。それでも避難あるいは注意を向けさせる予測は可能で、特に台風ならばその勢力や進路をほぼ正確に予測して避難を促すことができる。

これら自然の威力は、マグニチュード、波高や伝播速度、雨量や風速など数値で表わされ、それらがどの程度の破壊力をもたらすのか、われわれは科学的知識として、また経験としても知っている。その威力と、土地の形状や開発状況、過去の災害の歴史の組み合わせで、津波や河川氾濫の場合でも、土石流や火砕流の場合でも被災の範囲を想定することができる。

こうして自然災害の多くの場合、どこが安全でどこが危険か、おおよその見当をつけることができるのである。災害の防止対策としては、治水や堤防などの土木や建築として対処すべきことと、１人１人がハザードマップを意識しておくなど、平時からなすべきことがあり、

---

[13] 衆議院修正で「有機的な連携」の一句が追加されたという。国民保護法制研究会編『国民保護法の解説』（ぎょうせい、平成 16 年）7 頁。

災害が予測されれば警報を出すなどする。自然が猛威を振るってもそれが一過性か、長くは続かないことをわれわれは知っている。以上の点から、自然災害用に前もって避難所を指定しておくことは可能であり、かつ理に適っている。

３　事故発生と避難

次に、事故の場合を考えてみたい。ここでの事故とは二次災害の虞から周辺の者が避難を考えねばならないようなケースである。例えば、化学工場や船舶からの有害物質の流出、コンビナート火災、危険物搭載車両・鉄道の衝突や横転などである。事故はその発生こそ予知できなくても、もし起きれば危険物質が何で、それがどこから出ているかなどは分かるので、天候、気象を加味して拡散の予測も立てられないわけではない。一部の原子力事故や、海底油田の掘削施設爆破事故のように事態の制御が非常に困難なこともあるが、多くの場合は鎮静化の見通しも立つ。事故からの避難は、多くのケースでは、その現場から一時的に離れるか、屋内にとどまるか、火災が迫ってきた場合のように避難所に身を寄せるかのいずれかになるだろう。平素から施設の事業者と自治体、周辺住民の間でリスク・コミュニケーションを積み重ねておくことが、いざというときの対応の良し悪しに影響するであろう。

４　戦争・テロの予測と避難

では、戦争やテロの場合はどうだろう。まず総じていえば、その発生点（攻撃される場所と時刻）までを予知することはできない。少なくとも、大勢の住民をどこかに移動、避難させるほどの時間的余裕があるとは考えられない。外国と緊張関係が高まり攻めてくるかもしれないという虞が昂じても、いつ、どこに、どのような攻撃を仕掛けてくるのかまでは事前に明らかにはならない。そのような中で、どこの住民をどこに避難させるのであろうか。敵対国が対岸で日本上陸のための艦隊を集結させ、九州とか沖縄とかどこに向かおうとしているかが数日前から分かるというならば（5 章で後述するが、国民保護の世界ではそれが分かるというのだ！）、被災地になり得る地域の住民を避難させることも可能かもしれない。

あるいは、将来の日本が国際的に悪事を仕出かし、1991 年 1 月 17 日（湾岸戦争開始日）以前や、2003 年 3 月 19 日（イラク戦争開始日）以前のイラクのような状況に置かれたというならば話は別である。いずれの時もイラクは多国籍軍に侵攻されるのは秒読み状態であったからだ。

だが、今日の戦争のほとんどは、そもそも上記したようには始まらない。5 章で再度述べるが、現代の戦争は「外国軍」が大挙して侵攻してくるような分かりやすいものではなく、そのＸデイに身構えて迎え撃つようなものでもない。

テロの場合はどうか。国民保護訓練ではテロリストからの予告がしばしば入る。それを受けて、いつ、どこが危ないと判断してプレーヤーが動きだすこともある。しかし、現実の世界において、テロリストがご丁寧に、いつどこを攻撃すると予告する（しかも、本当にその

とおりに実行する）ことはまずない[14]。本当に標的を破壊したり人々を殺傷したりしたいなら、無警告で突発的に起こすほうが理に適っている。

学校や市役所などへの爆破予告は無数にあり、退避や不審物の捜索には大変な労を要するが、ほぼすべてがフェイクである（何も発見されないか、ニセもの）。何らかの行事の中止、あるいは恨み、嫌がらせ、憂さ晴らしなどが動機である。

テロリストはどこを狙うのかという質問は一般的によくある。それに対して、今日のテロは「ソフトターゲット狙い」だから多くの人が集まる集客施設が危ないという回答がなされることが多い。この問答はナンセンスで、そもそもテロリストといっても目的や動機が千差万別だから、当然標的も違ってくる。同一組織でも同じような標的ばかり狙うとは限らない。現在の日本のようにテロが少ない国において、その危険地帯や危険施設をあたかも津波や洪水のハザードマップのように示して、警戒してもらうことなどできない[15]。

戦争やテロは、組織や人の意図によって引き起こされる。そこには目的や動機がある。それが攻撃方法や標的の選定に合理的に結びつく場合と、対策をとる側にとっては考えも及ばない攻撃方法や標的選定の場合がある。戦いの途中で目的や動機が変わることもある。

また、われわれは兵器、武器１つ１つの威力は分かる。地震で震度７だとどういう建物ならばどのようになるのか分かるのと同様に、TNT 換算でどの程度の被害になるのか計算はできる。しかし、武器に何を選ぶか、どう組み合わせるか、それはやられてみなければ分からない。いつ戦いが終結するのかも分からない。つまり避難所に行くのが安全なのか否かについて、戦争やテロほど見通しの立たない事態はない。

米国との太平洋戦争は 3 年 8 カ月に及んだ。本土での避難といえば、空襲時に防空壕に入ったり、あるいは長期にわたる集団疎開であったりした。次の戦争は、この 1940 年代とは技術的にも社会インフラ的にもまったく異なる次元において行われるのだから、このような避難の形になるとも思えない。ただはっきり言えることは、広範囲の地域で住居が破壊されるであろうし、一定地域が占領されるであろう。だから避難をするにしてもそれは決して一時的なものでは済まないということだ。

総じて戦争やテロは、その発生もその後の展開も、攻め手と守り手の意思と能力の衝突であり、どこが発火点となり、どこならば危険でないのかについて、単純なパターン化を許さない現象である。つまり避難先をあらかじめ指定しておき、事がおきたら無条件的にそこに避難させたりすることにはならない。以上をまとめたものが【図２】になる。

---

14 この例外はあるが、予告したといっても犯行の直前では避難が間に合わない。戦後日本で代表的な爆破テロ事件であった三菱重工ビル爆破事件（1974 年）では、犯人が爆破の 8 分前に予告の電話を代表番号にかけている。電話は途中で切られ 4 分前に再度かけた。電話交換手はそれを受けて庶務室に伝達しようとしていた矢先に、1 階に仕掛けられた爆薬が大爆発した。松下竜一『狼煙を見よ―東アジア反日武装戦線“狼”部隊』社会思想社、現代教養文庫、1993 年、158－159 頁。

15 ただしテロ多発国においては、一定の標的選定の傾向をマッピングすることは可能である。

【図２】　各事態の見通し

	地殻変動	気象現象	事　故	戦　争	テ　ロ
発生予知	直前不可 将来計画可	可 将来計画可	不可	時間・場所 とも不可	時間・場所 とも不可
破壊力	数値知り得る	数値知り得る	貯蔵・製造 積載物から 予見可能	予測不可 多種多様	予測不可 多種多様
被災範囲	被害予測可能	被害予測可能	有害物質拡散 予測可能	予測不可	予測不可
防止対策	警報、避難 土木的改良	警報、避難 土木的改良	安全操業 異常時対応	抑止・外交 情報活動	未然防止策 情報活動
災害因の制御	不可	不可	発生地の消火 など	反撃・鎮圧	捕縛・鎮圧
終結予測	可能	可能	可能	困難	困難

作成　宮坂直史

さて、国民保護法（148 条）は、国が地方自治体に予め避難所を多数指定させており、平成 30 年 4 月 1 日時点で全国 9 万か所以上になる。だがそのリストを見ると、自然災害時と同様に、小・中学校の体育館などが主なもので、戦時には重要になる地下施設の備わった所は少ない[16]。近所の体育館や公民館等への避難ありきの前提で、前述したように国民保護訓練が行われたり「避難実施要領パターン」が作成されたりしている。自然災害と戦争、テロが同一視されているとしか思えないのである。上空や地上での戦闘にも耐えられるような地下施設を予め避難所指定しておくならばともかく、日本の場合はそういう条件を付していない。

第５章　現実の戦争・テロと、想像上の武力攻撃事態・緊急対処事態

１　武力攻撃事態の 4 類型

16 内閣官房「国民保護ポータルサイト」では各都道府県が指定した全避難施設一覧を公表している。内閣官房副長官補付の「避難施設一覧の更新について」（平成 30 年 11 月 9 日）によると、同年 4 月 1 日時点で全国 91,973 か所が指定され、うち地下に避難可能な施設は 802 か所ほどである。

2004 年に国民保護法が制定された後、すべての地方自治体や指定公共機関はそれぞれ「国民保護計画」を策定することになった。これらは各機関のホームページ上で、あるいは冊子の形で全文公開されている。これを策定させるにあたっては、総務省消防庁国民保護室が『都道府県国民保護モデル計画』などを参考として示していた。そこには武力攻撃事態として①着上陸侵攻、②ゲリラ・特殊部隊による侵攻、③弾道ミサイル攻撃、④航空攻撃の 4 類型を示されていた。ほとんどの「国民保護計画」にはこの 4 類型が記載されており、モデルにすぎないのだが、武力攻撃イコールこの 4 つと見なされ、そのポンチ絵とともに全国的に浸透している。同法制定から約 15 年たち、平成 29 年 12 月の最新版『国民の保護に関する基本指針』(全 76 ページ。以下『基本指針』) においても依然としてこの 4 類型が示されたままになっている。そこでの記述から何が見えてくるだろうか。

（1）着上陸侵攻

まず着上陸侵攻について、『基本指針』(以下の引用はすべて 11 頁より）は、「上陸用の小型船舶が接岸容易な地形を有する沿岸部」や「大型の輸送機が離着陸可能な空港が存在する地域」が「当初の攻撃目標となりやすい」、「目標となる可能性が高い」と指摘する。東京や大阪をはじめ全国このようなところは多い。

ここで描いているような着上陸侵攻ではないが、領土を占拠されるかもしれないという点において最も防衛しなければならないのは尖閣諸島に他ならない。そこは無人島だから国民保護とは関係ないのか。いや、そんなことはない。もし尖閣諸島が占拠されれば、日中関係のみならずアメリカを含めて東アジア情勢は極度に緊迫し、軍事衝突が起きたり、戦線が開かれたりするかもしれない。そうなれば沖縄県の他の離島の住民の安全を真っ先に確保しなければならない。それが即、各島からの避難を要するのかは状況次第になるが、避難や救援措置を少なくとも検討せざるを得ないので国民保護と直接関係する。

離島ではなく本土に対する着上陸侵攻ということになれば、それを許す状況とは既に多数の死傷者が出ているのではないだろうか。制海権も航空優勢も失っているに違いない。『基本指針』では、「着上陸侵攻に先立ち航空機や弾道ミサイルによる攻撃が実施される可能性が高いと考えられる」、「主として、爆弾、砲弾等による家屋、施設等の破壊、火災等が考えられる」と書かれてある。もしそのような状況になれば、一部区域の長期的な占領を余儀なくされるだけでなく、最悪ならば降伏に持ち込まれるかもしれない。

ところが、この後『基本指針』には「武力攻撃が終結した後の復旧が重要な課題となる」と腰が抜けるほどの楽観論が飛び出てくる。これを書いた人は、侵略軍は何をしに日本に来ると思っているのだろう。まさか自国民救出作戦だろうか。それが終われば速やかに撤収するはずだと。しかし外国の軍隊が日本で、その国の国民の救出に着手するような事態は、日本が内乱か無政府状態に陥っている状況であろうから、日本としては国民保護どころではなく、国家としての秩序回復に取り組まねばならない。

着上陸侵攻について『基本指針』の記述で特に問題になるのは、軍用艦の方向や戦闘機の

配備状況などから前もってそれが予測でき、避難のための「事前の準備が可能」だと書かれてあることだ。インテリジェンス能力以前の問題として、これは前時代的な戦争観である。現代の武力紛争は、火砲を発することと同時に（それ以前に）、サイバー攻撃も使って銃後の国民生活を麻痺、混乱させる。あるいは、軍人なのか誰なのか所属不明の部隊に先乗りさせたり、無人機を投入したりして防御側の対応を鈍化させることもある。SNS による対外世論工作も決して侮れないばかりか雌雄を決する手段にもなり得る。いずれも「ハイブリッド戦」と言われる現在の戦いに観察できる現実である。戦時と平時の境界が曖昧になり、軍事と非軍事的手段が融合し、相手を騙し惑わす。「ハイブリッド戦」は現在の国際関係において非常に多岐にわたるのでその詳細をここで論じることは避けるが、中国、ロシア、北朝鮮といった日本の周辺国が最も得意とする戦術である。これこそが戦いの常態とみなければならない。専門家が考える尖閣諸島をめぐるシナリオでも軍隊が大挙して上陸するというものではない。南シナ海での領域拡大が示唆するように、東シナ海でもより巧みな複合的な侵略を想定しなければならない。『基本指針』が描くような、海から空から大軍が押し寄せてくるクリアカットな侵略は一昔前の事象である。

（２）ゲリラ・特殊部隊

次に、ゲリラ・特殊部隊による攻撃をみていこう。日本の周辺国に本来の意味でのゲリラはいないので、ゲリラと言っても国家に所属する兵士か国家の意を受けた集団が比較的少人数で上陸して、機動力を有し破壊工作を行うイメージになる。

『基本指針』（以下の引用はすべて 12 頁より）によれば、この攻撃では「都市部の政治経済の中枢、鉄道、橋梁、原子力関連施設などに対する注意が必要である」という。何が標的になるのかは敵の目的次第なのだから、このような列挙は意味がなく、事業者に対する警告にもならない。さらに何の根拠もなく唐突に「ダーティーボムが使用される恐れがある」と書かれている。なぜ、ゲリラ・特殊部隊がダーティーボムなのか。ここに理由は書いていないが書けるわけもない。そもそもダーティーボムが破壊工作にせよテロにせよ、あるいは戦闘行為の中でにせよ、実際に爆破までして使用が確認された事例は世界に１つもない[17]。

避難については、当初は屋内に一時避難、その後「避難地に移動させる」と記している。「警戒区域」の設定にまで言及している。武器をもった連中が移動している中でも、国は、住民を屋外に連れ出したいようだ。破壊工作の最中に住民を外に連れ出すなどは、道中の安全についての確実な情報がなければリスクが大きすぎる。

（３）弾道ミサイル・航空攻撃

---

[17] ダーティーボムは、セシウム等の放射性物質と爆発物を1つの容器の中に組み合わせるだけの簡易に作れる兵器なので世界のどこで使われても驚くようなことではないが、放射線検知がなされなかったのか使用の記録は残っていない。ただし、ダーティーボムの所有を誇示した事案は発生している（1995 年、モスクワの公園にチェチェン過激派がそれを埋めていた）。また、ダーティーボムではないが、核物質であるポロニウム 210 が暗殺用に使用されたことがある（2006 年、ロンドンでのいわゆるリトビネンコ事件）。

続いて、弾道ミサイル攻撃と航空攻撃についてだが、『基本指針』では、対応時間が少なく、目標の特定も困難だという。いずれも屋内避難を挙げており、この点に間違いはない。だがなぜか弾道ミサイル飛来時の訓練では、体育館などの近所の避難所に避難者役が集められる。訓練で避難所に行くのは、講話を聞いたり議論をしたりするためであって、本当に起きたときに行くのではないことを避難者役の人々に伝えねばならない（自宅が迎撃の際の破片で被弾したとか火災が起きたというのであれば話は別である）。身を守るにあたっては普通の体育館よりも、地下施設が望ましいことを『基本指針』に書くべきである。近所に地下施設がなければ、あっても移動できなければ、現在地で最善の危険回避動作をとるだけである。

近隣諸国の弾道ミサイルの新技術（滑空式の弾頭飛来など）や、ドローンをはじめとする経空攻撃の多様さ（ドローンは飛翔体とは限らないが）など近年の軍事技術の進展が国民保護の世界には反映されていない。行政の担当者にその知識がないままに住民を屋外避難させてよいものだろうか。国民保護のポンチ絵に印象づけられる放物線を描いて飛来する弾道ミサイルや、有人の戦闘爆撃機だけが脅威なのではない。迎撃の確率が減少するほど、国民保護の重要性は増すばかりである。

２　緊急対処事態

（１）化学テロが起きたら高台に行く！

国民保護は、以上の武力攻撃４類型以外に「緊急対処事態」（本稿の注１に定義）も対象になっている。要するに大規模テロのことなのだが、『基本指針』にはその例が挙げられており、危険性を内在する物質を有する施設（原子力事業所、石油コンビナート、危険物積載船、ダム破壊など）、多数の人が集合する施設（大規模集客施設、ターミナル駅、列車など）を攻撃対象とするテロであり、また、生物剤、化学剤、放射性物質を使用したり、航空機で自爆したりするテロなどとなっている（72～73 頁）。

避難に関係することに注意しながら『基本指針』を読んでみると、例えば、化学剤が散布されたら「住民を安全な風上の高台に誘導する等、避難措置を適切にする」（14 頁）と書かれてある。なお、これは『基本方針』の第２章、武力攻撃事態の想定に関する事項の中で言及されている。しかし化学剤の散布は、緊急対処事態の１例でも挙げられていることであり、ここでの記述は、緊急対処事態への措置にも準用されるはずである。

また、国民保護訓練では前述したようにテロリストによって化学剤が撒布されたという想定のもとに行われるものが非常に多い。これらの訓練では、屋内から屋外へ連れ出し避難場所まで連れていくのが定番でもあった。

武力攻撃でもテロでも、化学剤が散布された時でさえ人々を屋外に連れ出すとは驚くべきことだ。これはサリンなどの神経剤が風下に拡散し空気より重いからという理由なのだが、物質の性質だけをみており、状況を考慮しない高台避難案と言わざるをえない。高台が安全でもそこに行くまではどうなのか。テロリストは全員捕まっているのかも分からない。どこ

にサリンが付着、漂流しているのかも分からない。このような場合、屋内にいる人は屋内に留まるにこしたことない。国民保護の世界は、この例に限らず、個々の武器、危険物の特性から対処法が描かれるが、戦況とか事態の展開というコンテキストの中で国民の安全を考えることはしていないようだ。

（２）現実の化学テロ

国民保護訓練では化学剤のテロを想定した内容が多い[18]。しかし、いま化学テロが世界でどれだけ発生しているのか、どのような集団がいかなる動機でどの国で化学テロが起きているのか、化学テロといっても化学剤は何が使われることが多いのか。これらは国際テロのデータベースや関連論文から分かることだが（例えば Global Terrorism Database によると過去半世紀の間に全世界で 401 件）、それら基本的な動向が把握されていない。日本の訓練では数ある化学剤の中でもサリンが想定されることが多いが、オウム真理教事件のあとサリン製造については国内法で規制が強化されている。ならば訓練で登場するサリンはどこから持ち込まれたのか、あるいは国内でどのようにして製造されたのか。このようなことを考えずに訓練シナリオを作るから非現実的になる。諸外国のテロでサリンが使用され多数の殺傷に至った例は確認できない。神経剤は近年ではシリアやロシアや北朝鮮などの国家機関ならば使用した。テロリストが使ってきたのは、サリンや VX ガスやノビチョクのような製造や使用が難しい神経剤ではなく、より身近に存在し、民生品の原料にもなる血液剤や窒息剤である。

さらに日本の訓練では、テロリストの爆発物に化学剤が含まれているという想定が非常に多い。これも実際の事例に乏しい。1993 年に世界貿易センタービルを爆破した主犯のラムジー・ユーセフでも、それをやろうとしたができなかった（爆破だけで負傷者 1000 人にのぼった）。爆発と同時に散布するのは技術的に困難であり、化学テロならば化学剤だけを散布すればよいと普通のテロリストならばそう考えるものだ。

日本は、このような起こる可能性が低いことに神経を使い過ぎている。消防隊の標準作業手続きでは、爆発の起きた被災地に到着してもすぐに救急活動には着手せずに、化学防護・検知あるいは放射能防護・検知にとりかかり自身の安全を確かめてから有症者の救助、搬送に入るのだが、それが訓練でも繰り返される。そのような手順を「本番」でも繰り返していたら、多数の爆傷者は病院に搬送される前に死んでしまうであろう。爆傷者の中には四肢切断の重症者がいるのが普通である。一刻も早く病院に搬送して手術に着手すれば生命はとりとめるかもしれないが（2013 年のボストン・マラソン爆破テロ事件で 30 人の重症者の命を救った例が有名）、日本式ではまず助からない。

---

[18] 1 章 1 節で述べたように、国と都道府県の共同訓練は過去 226 回行われている。この中で化学テロ想定の事案は 185 件に上る。これは爆発物テロ想定の 309 件に次いで多く（1 度の訓練において平均 2 件以上の事案を盛り込むので、事案数は訓練回数よりも多くなる）、他の手段は桁違いに少ない（生物テロ 21 件、銃器使用が 13 件、放射性物質テロが 3 件）。

世界のテロの手法で近年3番目に多いのは、放火、発火装置の使用である（上記のGlobal Terrorism Databaseによる）。これは爆発物（1位）や銃器（2位）を使ったテロ以上に容易であり、大量殺傷も可能である。国民保護が行政誘導避難にこだわるのならば、訓練シナリオに放火、もしくは爆発後の火災を入れるべきであろう。今までその想定がなかったのが不思議なくらいである。住居にまで大規模火災が迫れば、避難所への避難が必要になる。ただし施設放火の場合、消防が現地に到着したときには、逃げられる人はすでに一目散に逃げており、行政機関による避難誘導は不必要ということもある[19]。

国民保護の所管は、総務省消防庁と内閣官房になる。戦争やテロについては業務上考える必要もなかった事務官が、人事異動でたまたま国民保護に携わることになる。そうすると、致し方ないのかもしれないが今日の戦争やテロには目を向けず、既にある法令や計画、過去の訓練などを業務遂行上の基準にしたりする。これでは国民保護の問題には気づかない。

担当者は総じて国際関係や軍事情勢に疎い。日本国内での過去のテロのことを知らなくても珍しくない。経歴上の畑が違うし、ましてや専門家でないから知らないことが沢山あっても当然だが、住民を避難させようとする人たちは住民の命を預かっているわけだから、その避難に関係する軍事やテロの知識、感覚が著しく欠如していてはやはりまずい。各機関の担当者と数多く接し交流してきた経験から言うと、例えば、ミサイル防衛についてごく基本的な知識に欠けている人がいることに驚かされる[20]。周辺国の最新の軍事動向や、現代の戦争がどのように始められるのか、あるいは爆発物テロが傍で起きると身体はどうなるのか、そのような国民保護の原点となるべき現実を担当者が学ばないでよいとは思わない。

第6章　避難に関する判断を求める訓練を実施すべき

1　多機関連携の問題

国民保護の最も根幹的な措置は避難である。その避難は2章で整理したように本来多様である。国民保護措置における避難にも屋内避難が選択肢にあるし、そもそも避難指示の発出に慎重さを求めている。ところがなぜか法律が意図することを端折って、行き着くところは行政誘導避難なのである。行政誘導避難が必要か否か、現実的か否かではなく、どのように

---

[19] 例えば、2019年7月に発生した京都アニメーション放火事件（36人死亡、33人重軽傷）における消防と避難の動きは、国民保護にも非常に参考になる。それは行政誘導避難の現実性を再考させてくれる。勿論、この事件はテロではないし国民保護事態ではない。しかし、犯行方法や大量殺傷という結果は海外での大規模テロに類似している。「京アニ放火事件から半年―京都市消防局資料などから見えた全容」『朝日新聞』2020年1月19日。

[20] 例えば、地上配備のPAC-3で迎撃に成功すれば落下物が落ちてくるから、家屋が壊れたり、火災が起きたり、運悪く命中したりするかもしれない。だがミサイル基地近傍でさえ、落下物が落ちてくることを考えもしなかったという自治体職員、消防、警察の人は少なくない。彼らはミサイル飛来時の訓練で住民の避難誘導をする役回りなのである。勿論、迎撃に失敗すれば被害は遥かに大きい。

平素からそれを準備するかに国も地方もその思考を囚われている。

国民保護訓練においても、避難実施要領の準備にせよ、屋外を移動させる避難が前提のようになっている。状況を考えもせずに屋外を避難させるのは国民の生命をかえって危険に曝しかねないし、行政誘導避難が場面によっては非現実的ですらある。

このような方向に引きずられている要因は、多分に人的なものである。国民保護に携わる人々が、４章で対比したような戦争・テロと自然災害における、発生予知から終結予測までの根本的な違いを意識していないことと、５章で論じたように変わりゆく戦争やテロの実態を捉えていないことに原因があるのではないだろうか。

加えて、日本の統治体制は、国民保護のように（国民保護だけではなく）多機関で取り組む問題において、とかく責任の所在を曖昧なままにしがちである。日本の法制では現場において多機関の要員を一体的に統括する指揮官などは決めない。警察、消防、自衛隊、医療機関、事業者、自治体職員など現場に赴いた要員がいわば自発的に連携して対処することになっている。被災現場では警察や消防の指揮所に加えて、現地調整所が立てられて情報共有をする。加えて自治体内にも（市役所、県庁）にも対策本部が立てられ、国にも対策本部が立てられる。避難のみならず救命救急においても人々の生命が係っているのだが、多機関連携という美名のもとに、現場で決定権を持ち従って責任を問われるべき者が存在しない。

この点を海外多数の国と比較したわけではないので、日本独特のものと即断するわけにはいかないが、どことなく日本の文化に合っている。しかし結果的に、各機関の失敗や不作為が見過ごされ、巧みに隠されてしまう仕組みになっているのだ。行政機関の措置によって損害を被り、事後に訴訟を起こそうにも、被告・被告機関がわかりにくく、法律、計画の手順通りに実行したという抗弁で済むようになってしまっている。

所管する内閣官房や総務省消防庁の担当者のほとんどが今日の戦争やテロに詳しくないうえに、法律施行後に国民保護措置を発動する事態が実際に起きていないとなれば、訓練でも前例踏襲的な取り組みになってしまう。訓練に参加する機関、関係者がおかしなことに気づいていても、自分たちの所管ではないし、もとより多機関連携で責任感を薄められ、おかしなことを正面から指摘して正そうとする者もいない。

２　訓練の在り方

非常に根深い問題であるが、こと避難については、国民保護法でも『国民保護の基本指針』でも慎重に考えるように求めているのであるから、その本筋に則って、平素の訓練でも、避難が必要か否かをプレーヤーに考えさせる局面を盛り込むべきである。

その訓練は、従来のように図上訓練にせよ実働訓練にせよ当日あわただしくやって終わりとしてはならない。まず訓練をやる前に、訓練で中心となる県庁もしくは市役所の危機管理担当部署が、参加機関を集めて検討会を開く。そこで訓練シナリオの概要を示し（いつ、どこで、いかなる事案が発生するか程度まで知らせる）、この訓練が避難の在り方を考える訓練

であることを周知する。そのポイントは、行政誘導避難が必要なのか不要なのか、必要ならばいつ、どこへ、誰を、どのような手段で、どれくらいの時間で避難させるのか、受け入れ側との調整などをどのように進めていくかがポイントになることをはっきり伝えておく。訓練目的は「避難の要否を判断する」の１点で十分であり、それに関連した目標はいくつか設定できるであろう。各機関は、被災地域の昼夜間人口（地区、丁目ごと）や介護施設、医療機関、教育機関、多数集客施設、避難施設、事案日時の交通状況などの統一資料を与えられイメージ準備をしておく。

訓練本番においては、事前検討会のときには開示しなかった細かな状況付与、例えば被害状況の細かい点に応じて、国と県と市の間での指示、要請、情報伝達、対策本部と現場との間、現場での各機関の情報共有を進めていく。事前にシナリオ概要を知らせておき予習を求めるのであるから完全なブラインド型の訓練でもないし、刻一刻なにが起きるのかまですべて事前に伝えて、対策本部では発言メモまで事前に準備しておく手順確認型の訓練でもない。完全ブラインド型は消化不良を起こすだけであり、手順確認型では何も考えず、ルーティーンを遂行する平時と同じになってしまう。その中間型を提案しているのである。

そして訓練が終わってから、避難の要否をどのように判断したのかを改めて議論する場を設ける。後日にアンケートをとったりするのではなく、熱気の冷めないうちに訓練会場で議論することが大切であり、できれば２～３時間はあてるべきである。多機関が集まる公的な場での議論は盛り上がらないのが相場だから、事前にいくつかの課題を与えておいたり、各機関の混成グループを編成したりすることで議論活性化の工夫をする。避難者役や被災者役として参加している市民の代表者も議論の場に招待すべきである。訓練後の式典で当たり障りのない訓示を垂れ、評価員からは社交辞令的な講評を述べてもらい、一方通行的に終わりとすることはあってはならない。このような進行では後に何も残らない。

従来の訓練のように、次から次へと事件が起きるようなシナリオだと、プレーヤーにとって目的がぼやけ、かえって散漫になってしまう。何が何だか分からないまま、ただ疲れたで終わってしまう。これでは意味がない。他国からの侵略でも大規模テロでも事案１つを入れることで十分である。実際には事案が連続して起きてもおかしくないのだが、ここで提案したい訓練は、避難の要否を考えてもらうことが中心なので、ただ事案を増やせばよいというわけではない。

また国（内閣官房、総務省消防庁）は、評価者のような立場で視察に来るのではなく、国の対策本部役として訓練プレーヤーになるべきである。国の対策本部長は警報を発し、避難の指示を出すか出さないか決める。つまり国から訓練に来た誰かが、対策本部長＝総理大臣役をやればよい。いままでの訓練はこの点が等閑視されてきた。本番では国が当事者になるにもかかわらず、訓練ではそれを避けてきた。国は訓練終了後にしばしば訓練評価、講評をするが、当事者たる国がやるのは適切ではなく、訓練評価は県外の担当者や外部の専門家に任せる領域であろう。

３　訓練シナリオの提案

では避難の要否を考えるには、いかなる訓練シナリオがよいのか。改めて、国民保護が前提としている行政誘導避難が本当に求められるのはどのようなケースなのか３つ挙げてみよう。①既に被災して住む家が損壊している、あるいは自宅周辺の状況からしても自分の家に居られないとき（火災が迫っているなど)。②ある場所で事態が起きたが、その現場から自力でも事業者誘導でも脱出できない人々がいるとき。救出と避難誘導がセットになるイメージである。③危険が迫っていることが確かであり、それまでに避難させる時間があるとき、あるいは周囲に害を及ぼすかもしれない何かが発見されそれを処分するとき（例えば、第二次世界大戦中に使われ、埋没されたままになっていた不発弾が見つかったとき。あるいは、現在進行中の事案のなかで不審物が発見されたとき。）

なぜか国民保護訓練では①のような住宅被災の想定がない。テロは鉄道駅や集客施設のようなところで起き、住宅街では起きないとでも思っているのだろうか。前述したようにそのようなことはないし、商業地と住宅が混在している地区も無数にある。ともあれ、①は該当する住民を避難所に収容しなければならない。既に着の身着のままで飛び出し路頭に迷っている人々だからである。被災地なので相当に危ない。彼らに対する連絡、伝達も一筋縄ではいかないはずだからこそ訓練で考えてもらう機会を作りやすい。

②の想定は、巻き込まれた人の生死が係っている場面である。武装立て籠り事件のこともあるし、爆破などで建物の一部が崩壊して自力で脱出できないこともある。実働訓練でやるならば発災、通報から、救急搬送までの時間を測ってやるべきだし、その際の現場は、模型の障害物などを置いてわざとスムーズな突入や搬送を困難にさせるのも一計である。スタジアムの観客席を被災現場とするときでも、一番近い出入口を封鎖したり、被害者が倒れている通路を止めたりして、容易にアプローチできないように現場レイアウトを工夫することもできる。実際におきれば観客席が崩落し、がれきの山になるかもしれないので、とにかく、倒れている被害者に接近するのに一番近い入口から入って、一番近い通路が使えるというような安易な設定はやめるべきであろう。

また、②の想定で実施するときには、事業者の参加が不可欠であろう。行政誘導避難が始まるまでに事業者として何がどこまでできるのか検証することも、訓練に含める。今までの訓練では、ある施設内で何かが起きる想定で、そこの事業者も訓練に「参加」しているにもかかわらず事案発生後に何もせずに（役割を与えないで)、ただ消防や警察が到着するのを待っているだけということがしばしばあった。その施設の従業員や利用客の全員が瞬時に倒れてしまっているならばともかく、実際には逃げまどう利用者もいるのだろうから、事業者が何もしないということはありえない。また、事業者誘導ですべて完了する場合もあるだろう。だから②の想定の場合、行政誘導避難が必要なのか否かを考えさせるような状況付与をすれば、実りある訓練になるだろう。

③の想定は、少なくともテロ発生の前に避難させるのは現実的にはあまりないだろう。武力攻撃も時間がなければ事前避難は無理で、攻撃がなされてかから①のような被災者対象の避難になる。

いずれのケースの訓練でも、避難に関する情報収集や判断をしなければならないプレーヤー側には、“不完全な状況”を付与し続けて、避難の要否や、避難させるならばいつ、どこで、誰を、どのように、を決めて手配させる訓練になる。“不完全”というのは、事が起きる直前も、事が起きてからも、どこが安全でどこが危険かはっきり分からない状況に置かれていることである。だから訓練の中で取り組む１手１手には必ずしも正解があるとは限らない。与えられた状況をどのように考えたか、足りない情報は何だったのか、それをどこから得ようとしたのか、これらを訓練終了後に議論するのである。避難（市町村が国に先だって判断するならば「退避」）の要否を判断させる訓練を今後は増やしていくべきではないだろうか。

おわりに　新型コロナウィルスと国民保護

2020 年、われわれは新型コロナウィルスによるパンデミック下におかれている。この災禍は一過性のものではなく、おそらく国民保護行政にも大きな影響をもたらすであろう。それはプラス面とマイナス面の両方が考えられる。

まずプラス面は、むやみやたらと避難所へ避難させることはなくなるのではないか。「３密」回避が至上命題であって、今夏は自然災害時における避難所の運営も大きな負担を強いられている。避難者間の２メートルの距離やついたての用意、入所者１人１人の体調チェックと手指消毒は必須になっている。いままでの避難所が難民キャンプ並みと揶揄されるほど酷すぎたので、この程度の距離取りや仕切りの設置などは人道的にも合格点に達したと言うべきなのだろう。体育館や公民館など全国共通の避難所の収容人数は従来よりも制限されるから、自治体はそれ以外の場所を「開拓」したり、知り合いのところへ行くことを奨励したりするなど避難先の多様化を言い始めた。このような状況になれば、誰かしらが気づくはずである。国民保護訓練で大規模テロの想定をしてきたが、鉄道駅やモールや競技場でテロが起きて、なぜ無傷の住民を避難所に連れていかねばならないのかと。こうして本稿で最も問題視してきた何でも避難、とくに屋外避難ありきの考え方が軌道修正される契機となるかもしれない。

同時に、コロナ禍によるマイナス面も考えられる。避難させることが厄介になり、避難させないのであれば、何のための国民保護訓練かという疑問がわき、訓練自体が敬遠されるのではないだろうか。図上訓練のように、多少広い空間でやるとはいえ、大勢が集結するのを「密だ」と言って嫌えば、訓練をやらなくなってしまう。

人々はいま起きていること、起きたばかりのこと、繰り返し起きることに関心を囚われがちにある。そうなると日本にとって戦争は 75 年前（1945 年に終戦）のことであるし、大規

模テロも 25 年前（地下鉄サリン事件）まで遡る。久しく起きていないと、想像力は低下するばかりである。国際的な大規模イベントは、テロ対策を推進する原動力であるが、延期された東京オリンピック・パラリンピックが来年開催できるのかも現時点では分からない。

国民保護を推進する追い風が国内で強いとは思わない。しかし、近年、東アジアでは戦争未満の国際緊張は幾度となく高まり、今後もその傾向は続くに違いない。日本国内でもテロ未遂事件や懸念すべき事案も少なくない。大規模な国際イベントがあろうとなかろうと、国民保護訓練は絶やしてはならない。国民保護措置を必要とする事態はいつ起きるかは分からないが、将来必ず起きるだろう。

【付記】本稿は、2019 年 12 月 23 日に警察政策学会・テロ安保部会で報告したものを土台にしています。質問やコメントを寄せていただき、誤りをご指摘いただいた会員各位に感謝申し上げます。また、本稿で示した意見はすべて筆者自身の責任で記載したもので、筆者の勤務先、及び勤務先が所属する機関の見解とは一切関係がないことをお断りしておきます。

「クリプト社」と NSA　～世紀の暗号攻略大作戦～

“The intelligence coup of the century”

日本大学危機管理学部教授　茂田忠良

＜目次＞

初めに

「クリプト社」は、世界的な暗号機メーカーであるが、その暗号機メーカーは 60 年以上にわたり秘密裡に米国シギント機関・国家安全保障庁 NSA など米国インテリジェンスと協力関係にあった。この協力関係については今まで何度も断片的な疑惑報道や研究がなされてきたのであるが、今回遂に協力関係の全体像が明らかになった。

以下、その協力関係の判明の経緯を見たのちに、クリプト社と米国インテリジェンスの協力の全体像（即ち、協力の経緯、協力の成果、協力関係の終了）を概観し、最後にインテリジェンスの世界においてこの協力関係が持つ意味について考察する[1]。

なお、米国インテリジェンスによるクリプト社から協力を得る作戦を、本稿では「クリプト社作戦」と記述する。

第１章 「クリプト社作戦」全体像判明の経緯

１ 「クリプト社」とは如何なる企業か？

（１）世界的な暗号機メーカー「クリプト社」

クリプト社は、もともと 1920 年代にスウェーデンにあった暗号機メーカーであるが、第二次世界後の 1952 年スイスに移設し、スイスを拠点として活躍した世界的な暗号機メーカーである。

そもそも、秘匿強度の高い暗号機を自力で製作するのは、それ程容易なことではなかった。そのため、第二次世界大戦後、多くの国々が欧州民間企業の販売する製品を使ってきた。その中でも、クリプト社の製品は「性能」が良く且つ会社が「中立国」スイスに所在することもあり、最も普及した製品であった。２０世紀後半から 21 世紀にかけて実に世界の 120 ヵ国以上で使用されたのである。

採用国は、アジア、中近東、アフリカ、中南米など多くの国々に及び、イラン、リビア、エジプト、ジョルダン、シリア、アルゼンチン、アイルランドも含まれていた。他方、ソ連及びその衛星国、中国、北朝鮮は、中立国といえども西側の国であるスイスの企業の暗号機は決して使わなかった。

（２）クリプト社と米国の秘密の協力関係（1950 年代～2018 年）

このクリプト社は、1950 年代から 2018 年に至るまで、秘密裡に米国に協力しており、クリプト社の販売する暗号機について、米国による暗号解読に協力してきたのである。

この間、クリプト社は、米国国家安全保障庁 NSA や独連邦情報局 BND と密接な関係を持ち、また、米モトローラ社や独シーメンス社とも協力関係を築いていた。特に米国とは、第

[1] 本稿の大幅な要約版を「クリプト社作戦」として、『治安フォーラム』令和 2 年 11 月号（2020 年 11 月 5 日、立花書房）に掲載している。

二次世界大戦中から関係を持っていたが、戦後、更に継続して密接な関係を保ってきた。即ち、NSA の支援を受け、且つ NSA による暗号解読が容易になるように協力していたのである。従って、このクリプト社の暗号機を採用してきた国々の外交・軍事通信は、一部の例外を除いて、全て米国 NSA によって解読可能であった。

２　米国との協力関係全体像の判明の経緯

（１）従来の疑惑報道

クリプト社と米（独）諜報機関の協力関係についての出版や報道は度々なされてきた。特に、1993 年と 1994 年元社員ハンス・ビューラーによる告発、1995 年米『ボルチモア・サン』紙による根拠を示した調査報道があった。

しかし、その度に、クリプト社幹部は断固とした否定会見などを行い、疑惑は有耶無耶にされてきた。また疑惑報道による顧客の流出も一部に止まった。

（２）2014 年ウィリアム・フリードマン関係文書の開示[2]

ウィリアム・フリードマンは、米国「暗号解読の父」とも呼ばれ、第二次世界大戦前から陸軍の暗号解読の中心人物であり、また、戦後の国家シギント機関 NSA の暗号解読の第一人者でもあった。2014 年にフリードマン関係文書の多くが（一部黒塗りながら）開示され、これによってフリードマンとクリプト社の実質的な創業者ボリス・ハーゲリンとの親密な交流が浮き彫りになった。そして、1950 年代に NSA とクリプト社との間に一定の協力関係があったことが明白となった[3]。

但し、開示されたフリードマン文書から明確なことは、クリプト社が新型の暗号機を NSA に販売したこと、高度な最新式暗号機の販売先の限定に合意したことなどであり、それ以上、米国による暗号解読に積極的に協力したか否か、また、1960 年代以降も協力関係が継続したか否かについては、明確でなかった。

（３）2020 年 2 月 WP 報道・独 ZDF 報道

ところが、2020 年 2 月 11 日『ワシントン・ポスト』紙とドイツの公共放送 ZDF は共同調査に基づく報道を行い、これにより、米国とクリプト社の協力関係のほぼ全体像が判明したのである。

---

[2] フリードマン開示文書は、現在 NSA, William F. Friedman Collection of Official Paper,https://www.nsa.gov/News-Features/Declassified-Documents/Friedman-Documents/でアクセス可能。

フリードマン開示文書の内、クリプト社関係の主要文書は次のウェブサイトにまとめられている。National Security Archive, *Hagelin and Friedman: The Gentlemen's Understanding Behind "The Intelligence Coup of the Century,"*accessed 3 March 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-02-19/hagelin-friedman-gentlemens-understanding-behind-intelligence-coup-century.

[3] フリードマン開示文書については次の分析がある。特に前者の分析は詳細である。

--"The gentleman's agreement," *Crypto Museum,* last updated February 2020, accessed 3 March 2020, https://www.cryptomuseum.com/manuf/crypto/friedman.htm

--Gordon Corera, "How NSA and GCHQ spied on the Cold War world," *BBC,* 28 July 2015, accessed 6 May 2016, http://www.bbc.com/news/uk-33676028

『ワシントン・ポスト』紙の報道（国家安全保障担当グレッグ・ミラー記者）[4]とドイツ公共放送 ZDF の報道[5]によれば、両者は、「クリプト社作戦」の経緯に関する米国中央諜報庁 CIA 秘密文書と BND 口述記録を入手し、これを調査分析した。

CIA 秘密文書は、CIA のインテリジェンス研究センターが 2004 年作成した「MINERVA[6]–A HISTORY」と称する「クリプト社作戦」の包括資料（96 頁）であり、BND 口述記録（オーラル・ヒストリー）は、BND の複数の職員が 2008 年に作成した記録であるとされる[7]。

同調査報道（以下「WP 報道」「ZDF 報道」と呼ぶ）は、これら秘密文書の分析と付随調査[8]に基づくもので、その内容は従来の疑惑報道やフリードマン文書と斉合性を有しており、信憑性は極めて高いと評価できる。

なお、WP 報道は CIA 文書提供者の意思であるとして CIA 文書全体は開示していないが、同文書から 22 箇所を抜粋しており、その記述（以下「CIA 文書抜粋」と呼ぶ）も情報価値の高い資料である。

3　クリプト社と米国諜報機関の協力関係を見る意味

CIA 文書抜粋[9]によれば、「クリプト社作戦」は、「世紀の諜報成功事例である（the intelligence coup of the century）」「外国政府は米国と西独両国に費用を払った上で、少なくとも２ヵ国（多ければ５又は６ヵ国））の外国政府に機密通信を読ませる特権を付与していたのである」[10]。

このような、米国（及びドイツ）インテリジェンスの大成功事例を研究することは、それ自体が意味あることであるが、それと同時に、それを通じて、インテリジェンスの本質、その実態と論理について、また「供給網工作」（supply chain operation）など現下の課題につ

---

[4] Greg Miller, "The intelligence coup of the century," *Washington Post,* 11 February 2020, accessed 14 February 2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/. 以下、「WP 報道」と呼ぶ。
次の豪州ラジオ局によるイタビューも興味深い。Greg Miller, interview by Phillip Adams, *ABC Late Night Live*, 17 February 2020, accessed 3 March 2020, https://www.abc.net.au/radionational/programs/latenightlive/intelligence-coup-of-the-century:-the-cias-private-spying-busi/11972630

[5] "Operation Rubicon: How BND and CIA eavesdrop on the world," by Eomar Thevessen, Peter Mueller and Ulrich Stoll, aired 11 February 2020, on ZDF, accessed 5 March 2020, https://www.zdf.de/politik/frontal-21/operation-rubikon-100.html. 本放送の内容は、次の記事に記載されている。Eomar Thevessen, Peter Mueller and Ulrich Stoll,*"#Cryptoleaks: How BND and CIA Deceived Everyone," ZDF*, 11 February 2020, accessed 5 March 2020, https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html. 以下、「ZDF 報道」と呼ぶ。

[6] MINERVA とは、クリプト社に付されたコード名である。

[7] クリプト社と関係を持った米側インテリジェンスは、NSA と CIA 両機関である。今回の報道は、CIA 側資料のみによっており、NSA 側資料がないので、全容解明とまでは言えないが、ほぼ全体像が判明したとは言える。

[8] 付随調査には、現職や元職の諜報機関員やクリプト社社員のインタヴューが含まれるが、事案が機微な内容であるため、多くは匿名を条件として応じたということである。

[9] 抜粋内容は、全て註３の WP 紙記事に添付されている。

[10] WP 報道によれば、「クリプト社作戦」について、当事者である米独２ヵ国の他、少なくとも英国、スウェーデン、スイス、イスラエルはその存在を知っていたか、情報成果の分け前に預かっていたとされる。

いて、理解を深めることができる。

以下、WP 報道、CIA 文書抜粋、ZDF 報道、フリードマン文書、その他の現在までの開示資料や報道を基にして、本作戦について見ていくこととする。

第２章 クリプト社と米国の協力の経緯

１　クリプト社創設者ボリス・ハーゲリンの生立ち

CIA 文書抜粋によれば、ボリス・ハーゲリンは、1892 年にロシアの石油生産地として有名なアゼルバイジャン・バクー市近郊で、スウェーデン人実業家の家に生まれた。父親カールは有名なノーベル家の友人で、当時欧州最大の石油会社ノーベル兄弟社のバクー油田の経営を任されていた。ハーゲリンは、幼少期をロシアで過ごした後、大学教育を母国で受けるため帰国、スウェーデン王立工科大学で機械工学を専攻し 1914 年に卒業した。やがて父親の役割を引き継ぐ前提で、経営を学ぶためにストックホルムの総合電機企業に勤務していたが、ロシア革命が勃発したためロシアへの帰還が出来なくなった。

ボリス・ハーゲリンは、その後スウェーデンや一時米国で働いていたが、暗号機会社（スウェーデンのクリプト社。ハーゲリン家が以前から出資していた。）を 1925 年頃から経営するようになった。

２　M-209 暗号機の開発と米国陸軍の採用：フリードマンとの友情

CIA 文書抜粋によれば、ボリス・ハーゲリンは 1930 年代に C-36 という機械式暗号機を開発した。これは電力不要で軽量可搬型であり、秘匿強度は必ずしも高くはなく時間をかければ解読可能であったが、戦場での使用には最適の暗号機であった[11]。ハーゲリンは、この暗号機の売込のため、米国を 1937 年と 1939 年の二度に亘り訪問したが、その際に、米国「暗号解読の父」ウィリアム・フリードマンの知遇を得て友人となった。（フリードマンはロシア生れで幼少期に米国に移住したユダヤ人である。暗号研究家であり、1920 年代以降米陸軍の暗号責任者であった。）

WP 報道によれば、1940 年にドイツがノルウェーを占領すると、ハーゲリンは米国に亡命したが、暗号機 C-36 を改良して米軍の戦術通信用暗号機 M－209 を開発した。M-209 は米陸軍が採用するところとなり、大戦中 14 万台も生産された。ハーゲリンは、特許料で 860 万ドルを得たという[12]。このためハーゲリンは米国に恩義を感じることとなった。

３　ハーゲリンとフリードマンの（不文の）紳士協定時代（1950 年代）

ハーゲリンは大戦後、クリプト社をスイスに移転し、暗号機の開発を続けた。WP 報道に

---

11 戦術通信用の暗号機としては、秘匿強度よりも、戦場での使用のため電力不要で軽量可搬型であることが重要であった。戦術通信では、仮に一定時間後に解読されたとしても、既に通信内容は情報的に無価値となっている場合が多いからである。

12 ハーゲリンは、暗号機で百万長者になった世界初の事業家とされる。

よれば、ハーゲリンは 1951 年には CX-52 という新製品を製造したが、これは従来の暗号機と比して秘匿強度が高く、米国シギント機関の軍安全保障庁 AFSA（NSA の前身組織）でさえ解読が困難なものであった。本製品が世界に幅広く販売されると、米国としては世界各国の情報収集に支障を来すことになる。

そこで CIA 文書抜粋によれば、ハーゲリンが 1951 年に米国を訪問した際、フリードマンはハーゲリンと会食をした。その際フリードマンは、クリプト社の最新の暗号機の販売対象国を制限するように申し入れ、ハーゲリンは交渉に応じる意向を表明した。

フリードマン文書（1955 年の出張報告書[13]）によれば、その後 1954 年 1 月にフリードマンとハーゲリンは協力関係に関する紳士了解（gentlemen's understanding）に至った。

その了解を基に、米国諜報コミュニティでは協力関係について検討が進められてきたが、米国コミント委員会（当時）は 1954 年 12 月漸く正式提案[14]を決定した（提案内容には英国のロンドン・シギント委員会も同意している）。

フリードマンはその提案を持って 1955 年 2 月にクリプト社を訪問し、ハーゲリンは米国の正式提案に即座に同意し紳士協定が成立した。合意内容そのものは現在でも不開示であるが、フリードマン出張報告の開示部分から分かるのは、クリプト社が、次の方法によって NSA による暗号解読が容易になるように協力していることである。

- （開発中を含む）暗号機やその技術情報の提供
- 暗号機の世界各国への販売状況についての情報提供
- 最新式暗号機の販売時期の調整（必要に応じて販売延期）
- 特定国への販売は（解読容易な）旧式暗号機に限定

これに対して、NSA はハーゲリン一族に対して多くの便宜を図ってきた。ハーゲリンは、NSA の働き掛けにより娘婿コンラディの米空軍での継続勤務が可能になったことや NSA が妻の従妹バースを採用してくれたことについて、感謝を述べている。他方、ハーゲリンは NSA に対する協力に関して、特別に何かをする（例えば、積極的に暗号機に弱点を挿入する）訳ではないとして、金銭報酬の受領には拒否感を示していた。ハーゲリンの NSA への協力の動機は、米国に対する恩義・親近感とフリードマンとの友情を基礎にしたものであったと見られる[15]。

しかし CIA 文書を基にした WP 報道によると、1955 年の合意ではクリプト社は協力の代償として 70 万ドルの支払い[16]を受けることとなっていた。米国政府内の調整に手間取りなか

---

[13] 2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G.（Adapted Final Draft）*, 28 March 1955, accessed 31 August 2015, https://cryptome.org/2015/07/nsa-crypto-ag.pdf. --2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G. (Final Draft）*, 28 March 1955, accessed 3 March 2020, https://www.cryptomuseum.com/manuf/crypto/files/19550328_VisitToCryptoAG.pdf --2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G. (Second Draft),* 15 March 1955, accessed 31 August 2015, https://cryptome.org/2015/07/nsa-crypto-ag-draft.pdf.

[14] USCIB: 29.14/29 dated 27 December 1954.　内容は現在も非開示である。

[15] フリードマンは、1955 年や 1957 年のクリプト社訪問の際は、1 週間以上もハーゲリン家に宿泊して滞在している。ハーゲリン家との交流は家族ぐるみのものである。

[16] 代償としての 70 万ドルという金額は既に 1951 年の米シギント機関 AFSA 内の議論で言及されている。具体的な協力内容としては、コミント（この場合は暗号解読）面に加え、通信保全（米軍用暗

なか支出に至らなかったが、その間も、ハーゲリンは紳士協定を守り、最新式暗号機は特定の国にしか販売しなかったとされる。ハーゲリンの拒否感の表明にも拘らず、1955 年合意には（最新式暗号機の販売機会の損失補償《逸失利益の代償》などの）何らかの名目で金銭的対価が含まれていたと見られるが、ハーゲリンは元々金銭的対価を重視していなかったので、支出が遅れても不満がなかったのであろう[17]。

なお、フリードマン文書（1957 年の出張報告書[18]）は、クリプト社が 1950 年代に、ドイツ企業シーメンス社とも取引し交流していたこと、スウェーデン政府とスイス政府の意向を汲みながら経営を行っていたことも示している。

4　特許契約による販売制限協定時代（1960 年代）

CIA 文書抜粋によれば、1950 年代の協力関係は不文の紳士協定によってきたが、1960 年にはそれが特許契約という形で文書化された。それによれば、クリプト社は NATO 諸国とスイス、スウェーデンには最新式の解読困難な暗号機を自由に販売できるが、他の諸国に対しては国別に販売できる暗号機の種類（即ち性能）が制限されていた。その代償に、米国はクリプト社の全ての暗号機に対して特許料を払うという取決であった。WP 報道によれば、特許料は 1970 年に一時払いで 85 万 5 千ドル、加えて、毎年、契約更新料として 7 万ドル、クリプト社の（NSA にとって解読可能な）暗号機の販売促進費用として 1 万ドルが支払われる

号機開発への協力）面も含まれているようである。参照：2014 年 NSA 開示資料 William Friedman, *Negotiations with Mr. Hagelin,* 22 May 1951, accessed 4 March 2020, https://www.cryptomuseum.com/manuf/crypto/files/negotiations_1951.pdf

[17] 1950 年代の協力関係については、従来ハーゲリンは金銭的対価を得ていないという解釈が一般的であったようである。（“The gentleman’s agreement,” *Crypto Museum* 中の “The Hagelin Deal 1955” の記述を参照）。その理由は、①本文中に記載したように、フリードマンの 1955 年出張報告によれば、ハーゲリンが金銭的報酬に拒否感を示していたこと、②協力内容に関する米国コミント委員会の提案自体は今以て情報開示されていないこと、以上二つから導かれた推論であろう。

しかし、実際は金銭的対価 70 万ドル支払の約束と実行はあった判断するのが妥当である。その根拠は、①1951 年 5 月フリードマン自身がシギント機関 AFSA 内部での検討で 70 万ドルの支払いを積極的に主張していること（参照：Friedman, *Negotiations with Mr. Hagelin,* 22 May 1951）、②今回の WP 報道が、CIA 秘密文書（MINERVA－A HISTORY）に基づき（関係部分は公表していないものの）1950 年代の協力の対価として 70 万ドルが支払われたとしていること、③米国側の事情で対価の支払が遅れてもハーゲリンは不満を示さなかったという展開は、正に 1955 年フリードマン出張報告の内容と斉合性があること、以上三つである。

こうして見ると、2014 年のフリードマン関係文書の開示自体に、一つの情報作戦が含まれていたと考えることができる。即ち、1955 年フリードマン出張報告の開示により、クリプト社の協力は、①最新式暗号機の販売対象国の制限という消極的な協力に過ぎないこと、②協力は金銭的対価の伴わないハーゲリンの自発的協力であって、フリードマンとの個人的関係によるところが大きいというイメージを流布させることに成功している。つまり、クリプト社の暗号解読における対米協力は、過去のものであるという印象創出を意図したものであろう。即ち、フリードマンもハーゲリンも故人となって久しく両者の個人的関係も終了し（協力の基礎は既に消滅し）、且つ 2014 年現在で関係フリードマン文書を開示できる位に秘密保持の必要が低下した、従って現在は協力関係は継続していないという暗黙の主張である。

[18] 2014 年 NSA 開示資料、William F. Friedman, *Memorandum for the Record; Hagelin Negotiations (Draft),* 18 December 1957, accessed 3 March 2020, https://nsarchive2.gwu.edu//dc.html?doc=6779397-National-Security-Archive-20-Draft-of-William

こととなった。

この段階でのクリプト社の協力は、いわゆる「拒否作戦」であり、クリプト社の（NSA が解読不能な）高度暗号機を販売しないという、NSA の暗号解読に対する消極的な協力であった。

５　NSA によるクリプト社暗号機の回路設計の始まり（1967 年）

1960 年代半ばには電子回路が発達し、暗号機も従来の機械式暗号機から電子式暗号機への変換が迫られた。

しかし、WP 報道によれば、必ずしもクリプト社には電子回路に関して十分な技術力がなかった。他方、NSA は電子式暗号機で秘匿強度が増大して解読不能となることを危惧していた。

折しも NSA の専門家ピーター・ジェンクスは、一見無限乱数を生成しているように見えて実は有限乱数を生成するに過ぎない電子式暗号機を製造することが可能であることを発見した。勿論この有限乱数は、NSA のコンピュータで解読可能なものである。

その結果、1967 年にクリプト社は最初の電子式暗号機（テレプリンター型）H-460 の販売を開始したが、その電子回路は NSA の技術者が設計したものであった。勿論、NSA にとって、電子式暗号機 H-460 でも通信を傍受して且つ解読する手間はかかったのであるが、それまでの機械式暗号機よりも遥かに迅速に解読できるようになったという。

クリプト社の一見高性能に見える電子式暗号機に対して、諸外国政府の需要は高く売上は急増した。同時に、クリプト社は益々NSA に依存するようになった。クリプト社は、暗号機は常に 2 種類以上製造し、1 種類は解読困難な友好国用であり、その他は解読可能な機種とした。

NSA による暗号機の回路設計の開始により、クリプト社製暗号機販売は、弱点を仕込んだ暗号機を販売するという「積極工作」の段階に入ったのである。

６　米独によるクリプト社共有時代（1970 年～1993 年）

（１）米独によるクリプト社買収

WP 報道によれば、1960 年代末には、ハーゲリンも 80 才近くと老齢に達し、クリプト社の事業承継を考えるようになった。他方、CIA はハーゲリンの突然死やクリプト社の売却を危惧するようになった。そこで、クリプト社の買収が検討されたが、CIA と NSA 間の調整が進まず具体的な動きにまでは進まなかった。

そうこうする内に、仏独諜報機関がハーゲリンの引退希望を察知して、クリプト社への接近を始めた。仏独と幾つかの欧州諜報機関は、同社と米諜報機関との関係について、米国から知らされ、或いは自ら探知して知っており、かねてからクリプト社と同様の関係を築きたいと模索していた。そこで 1967 年には、仏諜報機関が独諜報機関と共同で、ハーゲリンに同社買収を持ち掛けたが、ハーゲリンはこれを拒否して CIA に通報した。次に 1969 年初に、独 BND のシギント部門 ZfCh[19]責任者ヴィルヘルム・ゲーイングが、CIA に対して米仏独共

[19] Zentralstelle fuer das Chiffrierwesen。現在のドイツの BSI（Bundesamt fuer Sicherheit in der

同によるクリプト社買収を提案したところ、CIA はフランスを排除した米独共同による買収を逆提案し、ドイツはこれに同意した。

（２）米独によるクリプト社経営の構造

CIA 文書抜粋によれば、1970 年 6 月に秘密裡にクリプト社の全株式が米国政府とドイツ政府に譲渡された。同月締結された CIA と BND の覚書によれば、両組織が費用を折半して合計 2500 万スイス・フランで全株式を取得し、両者の合意の下に運営することとされたが、形式上は BND のフロント企業が所有する形を取った（WP 報道によれば、会社の登記他の文書作業にはリヒテンシュタイン公国の法律事務所 Marxer and Goop が関与して、所有者の正体隠匿に協力した）。このクリプト社の秘密共同経営作戦は、暗号名「シソーラス作戦」と命名された（1980 年代末には「ルビコン作戦」と改名。以下「ルビコン作戦」と呼ぶ）。

WP 報道によれば、クリプト社の運営について、CIA はミュンヘンに秘密事務所を設置して、独 BND と定期会合を持った。クリプト社では、取締役の内唯一人、ハーゲリンから経営を引き継いだシュトゥーレ・ニイベルグ（Sture Nyberg）のみが、米独諜報機関との関係を知っていた。また、諜報機関は、企業経営には疎いので、民間企業も巻き込んでいた。ドイツはシーメンス社を引き込み、売上の５％の顧問料でクリプト社の営業と技術問題について助言を得るようにした。また、米国は後にモトローラ社を引き入れ、大型製品について技術支援を得るようにした。

CIA 文書抜粋によれば、クリプト社の運営に関係した組織は、政府機関では米国は CIA と NSA、ドイツは BND と傘下シギント部門 ZfCh、民間会社では独シーメンス社と米モトローラ社である。

クリプト社は、米独諜報機関と両民間大企業の支援を得て成長して、1970 年の売上高 1500 万スイス・フラン、従業員数 180 人以上から、1975 年の売上高 5100 万スイス・フラン、従業員数 250 人以上となった[20]。

（３）クリプト社従業員に対する協力関係の秘匿

クリプト社の社員で米独諜報機関との関係を知っていたのは、ごく少数であった。当初は、取締役ニイベルグ唯一人であり、彼が 1976 年に引退するとその地位は Heinz Wagner に引き継がれ、更に後に Michel Grupe に引き継がれた[21]。

一般の従業員に対しては、協力関係は秘匿されており、外部（実は NSA）から提供される暗号機の設計アルゴリズムは、協力関係にあるシーメンス社から提供されていると説明されていた。従業員の中には、暗号設計の欠陥に気付いて、勝手に改良して NSA が解読不能の製品を製造する者も現れたが、解雇されたり、改良を中断させられたりした。開発部門の幹部に対しては、暗号アルゴリズムの秘匿強度には規制が掛かっている旨の説明をして、ドイツ政府による規制のため已むを得ないものと思わせたりした[22]。

Informationstechinik）の前身組織である。

[20] CIA 資料抜粋。同抜粋によれば、1970 年から 1975 年までの 6 年間の純益合計は 1711 万スイス・フランであり、当時の為替相場で 20 億円近くの利益を上げていた。その後も 1990 年前後までは純益を上げ続けていたと見られる。

[21] WP 報道

[22] WP 報道

（4）暗号学の大家ヘンリー・ウィドマン招聘 1979 年

しかし CIA と BND は、このままでは秘密保持が難しいと考え、1979 年にスウェーデンの数学教授で暗号学の大家であるヘンリー・ウィドマン[23]を技術顧問に招聘した。その役割は、クリプト社の開発部門が納得する（即ち、気が付かない）高度な弱点を暗号アルゴリズムに仕込むことであり、スウェーデン諜報機関の推薦による人選であった。この後、クリプト社の暗号アルゴリズムはウィドマンが設計することとなったが、その設計目的は通常の統計学的解読手法では探知不可能な弱点を仕込むことであり、万が一弱点を発見されても製造段階或いは使用段階での人為的ミスと言い訳できるものを設計することであった。ウィドマンは不可欠の人物となり、その招聘は「ルビコン作戦」の歴史で最重要な人事であったという[24]。ウィドマンは 1994 年まで技術顧問を務めた。

7　米国単独のクリプト社経営時代（1993 年～2018 年）

1993 年、後述する経緯で、ドイツ BND はクリプト社の経営から手を引いた。同年 9 月ドイツ駐在の CIA 代表と BND は合意に達し、CIA はクリプト社の BND 所有株を 1700 万ドルで購入した[25]。この後は、米国単独でのクリプト社経営となる。

1990 年代には新たな暗号通信方式が発達し、次第にクリプト社製暗号機の販売は減少した。その結果、赤字に沈み込んだが、インテリジェンス収集プラットフォームとしては 21 世紀に入っても依然有効であった。それは、各国政府の官僚制の惰性によるもので、特に発展途上国ほどクリプト社製品を惰性で使い続けたとされる[26]。

しかし、暗号技術市場がハードウェアからソフトウェアに移行すると、遂にクリプト社も追随が困難となり、2018 年に会社を分割譲渡して解散した。

なお、米国 NSA は、クリプト社経営で蓄積した利益を使って、他の暗号機メーカーも買収したとされる。それは、同じくスイスの暗号機メーカー「グレターク社」である。同社は 1995 年に形式上元 NSA 職員が設立した会社が買収したが、2004 年に解散している。

第３章 クリプト社の協力による情報成果

1　米国にとっての全体的成果

クリプト社の暗号機は多くの政府によって使用され、その暗号機の殆どは NSA にとって解読可能であったので、米国に大きな情報成果を生み出した。クリプト社製暗号機の使用国は、1950 年代から 2000 年代にかけて 120 ヵ国以上に及んでいるとされる[27]。

---

[23] 本名は Kjell-Ove Widman であるが、学生の頃米国に交換留学した際に発音し難いので、Henry Widman を通称としていた。留学経験もあり親米派であった。
[24] WP 報道
[25] WP 報道
[26] WP 報道
[27] WP 報道。ZDF 報道によれば、クリプト社の最盛期には、世界の 130 を超える政府（軍、諜報機関の通信を含む）を顧客にしていたという。

WP 報道によれば、使用国には次の各国が含まれる。

○　米州：　アルゼンチン、ブラジル、チリ、コロンビア、ホンジュラス、メキシコ、ニカラグア、ペルー、ウルグアイ、ベネズエラ

○　欧州：　オーストリア、チェコスロバキア、ギリシャ、ハンガリー、アイルランド、イタリア、ポルトガル、ルーマニア、スペイン、トルコ、バチカン市国、ユーゴスラビア

（註:旧共産国がクリプト社製暗号機の使用を始めたのは、ソ連の崩壊後の事と考えられる。ユーゴスラビアは戦後初期にも購入したことがある。）

○　アフリカ：　アルジェリア、アンゴラ、エジプト、エチオピア、ガボン、ガーナ、ギニア、象牙海岸、リビア、モーリシャス、モロッコ、ナイジェリア、コンゴ共和国、南アフリカ、スーダン、タンザニア、チュニジア、コンゴ民主共和国（ザイール)、ジンバブエ

○　中東：　イラン、イラク、ジョルダン、クウェート、レバノン、オマーン、カタール、サウジアラビア、シリア、UAE

○　アジア：　バングラデシュ、ビルマ、インド、インドネシア、日本[28]、マレーシア、モーリシャス、パキスタン、フィリピン、韓国、タイ、ヴェトナム

なお、ソ連や中国はクリプト社製暗号機を使用せず、米国はそれらの国の暗号通信は解読できなかったが、クリプト社製暗号機を使用する諸国の在モスクワや在北京大使館と本国間の通信を解読することにより、ソ連と中国について相当の情報を入手することが可能であったという[29]。

２　米独協力期間中（1970 年～1993 年）の成果

（１）全体的な成果

CIA 文書抜粋によれば、米独協力期間中、米 NSA にとって、その暗号解読の 40%以上が「ルビコン作戦」の成果であり、代替不可能な重要な情報源であった。更に独 BND にとっては、その外交関係情報報告の 90%本作戦の成果であり、本作戦が米独諜報協力の根幹であったという。

NSA はシギント機関であり、その通信暗号解読の 40%以上が本作戦由来であったということは、米国諜報コミュニティにとって極めて大きな意味がある。ところが更に、BND はオールソース・インテリジェンス機関であり、ヒューミントを含む全外交関係情報報告の 90%がシギントの本作戦由来であったということは、BND の外交情報源の殆どが本作戦であったということであり、ドイツにとって如何に大きな位置を占めていたかを示すものである。

（２）地域別、個別国の成果

地域別では、1980 年代、NSA の G グループ（ソ連圏とアジアを除く全世界担当）の情報報告の 50%以上は、クリプト暗号機解読由来であった[30]。

クリプト社の暗号機の使用国は世界中に及んでいるが、1981 年時点で、大口購入国は、サウジアラビア、イラン、イタリア、インドネシア、イラク、リビア、ジョルダン、韓国の順

---

[28] 日本について、使用組織と使用台数については特定できなかった。
[29] WP 報道
[30] WP 報道

であった[31]。

国別で成果が大きかったのはイランである。「ルビコン作戦」のお蔭で、イランの諜報対象の 80～90%の通信は解読可能であった。1988 年にはイラン通信 1 万 9 千件が解読され情報化された[32]。

３　個別の情報成果

「クリプト社作戦」の情報成果を、個別具体的な事例で見てみよう。

（１）1978 年キャンプ・デービッド会談（エジプト通信解読）

1978 年 9 月、米カーター大統領の仲介で米国の大統領別荘キャンプ・デービッドで、エジプトのサダト大統領、イスラエルのベギン首相を迎えて、両国の和平交渉が行われた。

この交渉では、サダト大統領とカイロ間の（クリプト暗号機を使用した）通信を米 NSA が傍受して、エジプトの立場に関して情報を入手した[33]。

（２）1980 年イラン米大使館員人質の解放交渉（アルジェリア通信解読）

イラン革命防衛隊に指導された学生達は、1979 年 11 月テヘランの米国大使館を占拠して大使館員 52 人を人質に取った。

人質の解放交渉ではアルジェリアが仲介した。アルジェリアはクリプト社の暗号機を外交通信に使用していたので、米国はアルジェリア本国と大使館間の秘密通信を解読できた。当時の NSA 長官ボビー・インマンによれば、この解読情報は、当時のカーター大統領にとって、イランの状況を把握して人質解放交渉を管理するために絶対的に重要な情報であり、カーター大統領は頻繁に NSA 長官に電話をしてアルジェリアの通信情報を要求したという[34]。

（３）1982 年フォークランド戦争（アルゼンチン通信解読）

アルゼンチン沖のフォークランド諸島は、19 世紀以来英国が海外領土として実効支配していたが、領有権を主張するアルゼンチンが 1982 年に軍事侵攻し占領した。これに対して、英国は米国や EU 諸国の支援を受け、軍事作戦を展開して同諸島を奪回した。

その際、アルゼンチン海軍はクリプト社の暗号機を使用していたため、米国 NSA が解読情報を提供し、英国が情報優位に立ち戦勝に貢献した[35]。なお、アルゼンチンは、クリプト社の暗号機が解読されていることを疑い、クリプト社の技術顧問ヘンリー・ウィドマンを召喚して詰問したが、ウィドマンはクリプト社の暗号機は解読不能であり、秘匿強度の低いアナログ秘話装置が解読されたのではないかと主張して切り抜けた。その結果アルゼンチンはその後もクリプト社の暗号機を使用し続けた[36]。

（４）1986 年西ベルリンのディスコ爆破事件（リビア通信解読）

1986 年 4 月西ベルリンのディスコ「ラ・ベル」が爆破された。同ディスコは駐留米国兵が良く集まる場所であり、米兵多数が負傷し 2 人が死亡した。

---

31 WP 報道
32 CIA 抜粋資料
33 WP 報道
34 CIA 資料抜粋
35 WP 報道、ZDF 報道
36 CIA 資料抜粋

これに対して、レーガン大統領（当時）は、米国はリビア関与の証拠を握っている、その証拠とは事件１週間前に東ベルリンのリビア大使館が攻撃命令を受け、事件翌日にはトリポリに任務達成の報告をしていることであると述べた。そして同月、米軍が報復措置としてリビアの首都トリポリを爆撃した。

リビアもクリプト社の暗号機を使用しており、米国 NSA がリビアの首都トリポリと東ベルリンの外交通信を傍受解読していたのである[37]。

（５）1989 年パナマの独裁者ノリエガ将軍の所在把握（バチカン市国通信解読）

パナマの独裁者ノリエガ将軍は 1989 年 5 月の選挙で敗北したにも拘らず、そのまま居座ろうとしたが、米国は米海兵隊員の殺害等を理由にパナマに軍事侵攻した。ノリエガ将軍はバチカン市国大使館に逃げ込んだが、その所在を把握され投降した。

ノリエガ将軍がバチカン市国大使館に逃げ込んだ事実は、バチカン市国と同大使館の間のクリプト社暗号機による通信の解読によって判明した[38]。

第４章 困った情報成果の副産物

クリプト社の暗号機解読による情報成果は、関係国に大きな情報成果をもたらし、国益増進に貢献したのであるが、時には必ずしも好ましくない情報をももたらした。

その典型は、南米諸国による「コンドル」の通信システム「コンドル・テル」の傍受解読である。

1974 年、南米４か国の左翼革命組織が「革命調整会議」という協力組織を設立した。参加組織は、アルゼンチン人民革命軍、ボリビア民族解放軍、チリ革命左派運動、ウルグアイ民族解放運動ツパロマスであり、これら組織はキューバの支援を受け、革命を目指して、国内だけではなく欧州においてもテロを敢行している。

これらのテロ・革命運動に対抗して 1976 年に発足したのが「コンドル」である。参加国は、アルゼンチン、ボリビア、チリ、ウルグアイ、パラグアイ、ブラジルであり、1977 年末にはエクアドル、ペルーが加わった。「コンドル」はこれら南米諸国の国家諜報機関の調整機関である。チリのサンチャゴに情報センターを設置してテロ・革命勢力に関する情報交換を行うと共に、関係機関の秘匿通信システム「コンドル・テル」を導入し、通信用暗号機にクリプト社製を採用したのである[39]。

---

[37] WP 報道

[38] WP 報道

[39] 開示資料、CIA, *Counterterrorism in the Southern Cone*, 9 May 1977, accessed 8 March 2020, https://nsarchive2.gwu.edu//dc.html?doc=6773840-National-Security-Archive-Doc-2-CIA-report
--開示資料、CIA, *Communications System Employed by the Condor Organization,* 1 February 1977, accessed 8 March 2020, https://nsarchive2.gwu.edu//dc.html?doc=6773841-National-Security-Archive-Doc-3-CIA-cable
—開示資料、DIA Intelligence Appraisal, *Latin America: Counterterrorism and Trends in Terrorism*, 11 August 1978, accessed 8 March 2020, https://nsarchive2.gwu.edu//dc.html?doc=6773842-National-Security-Archive-Doc-4-DIA-

ところで、南米諸国の軍事独裁政権の多くは、革命勢力に対抗して、拉致、暗殺、拷問その他の超法規的な対抗措置を取り、多大な人権侵害をもたらしていた。その超法規的対抗措置は、国内にとどまらず欧州など国外にも及んでいた。当然のことながら、その関連通信が、関係諸国の諜報機関間の通信システム「コンドル・テル」でなされており、米独両国は、クリプト社暗号機による通信解読を通じて、その人権侵害を知り得る立場にあった。

独 ZDF 報道によれば、BND がその北ドイツの施設で傍受解読した情報には、アルゼンチンやチリにおける人勧侵害事態が含まれていたという。アルゼンチンでは 1970 年代は軍事政権で、政権に対する反対者を誘拐、拷問、殺害していた。軍用機から数千人を大西洋上に突き落として殺害するなど合わせて 3 万人以上を殺害したという。米独ともこのような人権侵害の事態を知っていたにもかかわらず、これを放置していたのである[40]。

第５章 「クリプト社作戦」の終了

１　疑惑報道による打撃

クリプト社と米独諜報機関の協力関係についての出版物や報道は度々なされてきたが、次の報道は協力関係を阻害する影響を及ぼした[41]。

（１）1993 年、1994 年元クリプト社社員による告発

クリプト社社員ハンス・ビューラーはイラン担当の営業員であったが、クリプト社暗号機による通信内容の漏洩に疑問を持ってきたイランが 1992 年に同人を拘束して厳しく訊問をした。ビューラーは米独諜報機関とクリプト社との協力については全く知らず、9 か月後 1993 年初めにクリプト社が 100 万ドルの身代金を払って解放された[42]。

しかし精神的外傷を負って帰国したビューラーは、クリプト社と米独諜報機関の協力を疑うようになり、疑惑を語り始めた。1994 年には更に別の匿名の元社員と共にテレビに登場して米独諜報機関との協力疑惑を告発した[43]。

Intelligence

[40] ZDF 報道。

--Greg Miller and Peter Mueller, “Compromised encryption machines gave CIA window into major human rights abuses in South America,” *Washington Post*, 17 February 2020, accessed 25 February 2020, https://www.washingtonpost.com/national-security/compromised-encryption-machines-gave-cia-window-into-major-human-rights-abuses-in-south-america/2020/02/15/bbfa5e56-4f63-11ea-b721-9f4cdc90bc1c_story.html

[41] 本文に述べた報道の前にも、1977 年出版のウィリアム・フリードマンの伝記（ロナルド・クラーク著）は、1957 年のフリードマンのクリプト社ハーゲリン訪問を記述、また、1982 年出版の『パズル・パレス』（ジェームス・バムフォード著の NSA 研究の古典的名著）は、フリードマンとハーゲリンの協力関係の存在について記述したが、影響は殆ど無かった。

[42] CIA 資料抜粋によれば、身代金は BND が支払った。米国は身代金の支払いは国策に反するとして支払わなかった。

[43] WP 報道。CIA 資料抜粋によれば、1994 年ビューラー等のテレビ告発の際は、当時のクリプト社取締役 Michael Grupe が反論のテレビ会見を行ったが、なかなか上手な対応であり、疑惑を有耶無耶に終わらせた。

（2）1995 年『ボルチモア・サン』紙による疑惑報道

米国の『ボルチモア・サン』紙は、クリプト社と NSA の協力関係の具体的証拠を入手したと報道した[44]。同紙によれば、1975 年に NSA 暗号専門家ノラ・マカビーがクリプト社における暗号機の詳細設計に関する議論に参加しており、これは同紙が入手した資料[45]と同席したモトローラ社技術者ボブ・ニューマンの証言があるとした。更に、クリプト社の元社員ユルグ・スポルンデリは 1970 年代後半に秘匿強度を下げるようにアルゴリズム変更を指示されたと述べ、同元技術者ルディ・フグは技術顧問ウィドマンが暗号機の秘匿強度には制限がある旨を述べたと、協力関係の根拠を示して報道した。

（3）一部顧客の流出

これらの疑惑報道に対して、クリプト社は断固として否定したが、これら報道の影響を受けて、少なくとも半ダース程の顧客がクリプト社製品の使用を停止した。それらの国は、アルゼンチン、イタリア、サウジアラビア、インドネシア、エジプトが含まれる。ところが、驚くべき事に、イランはクリプト社製暗号機の購入を直ぐに再開したのである[46]。

2　1993 年ドイツの離脱

ビューラー事件によって協力関係の暴露の虞もあり、ドイツは 1993 年「ルビコン作戦」を離脱したが、その基本的原因は米独の国益の違いである。

CIA 文書抜粋によれば、米独共有時代の煩わしい問題は、解読困難な暗号機の販売可能対象国の範囲であった。ドイツとしては NATO の同盟諸国には解読困難な暗号機を販売したいと考えていたが、他方米国は、解読困難な暗号機の販売対象をできるだけ限定しようとした。当初 NATO 諸国は全て販売対象であったが、初めにギリシャとトルコが除外され、スペインやイタリア他の国々も次々に販売対象国から除外されるようになったのである。この点について米国 NSA は極めて執拗であって、最終的には、解読困難な暗号機の販売対象国は、「ルビコン作戦」に直接又は間接に関与する一部の NATO 諸国[47]とスウェーデンとスイスのみとなってしまったという。

ところが、冷戦が終結して 1990 年にドイツ再統一が実現すると、ドイツにとっては、欧州諸国との友好関係がより重要となってきた。万が一「ルビコン作戦」とドイツ関与に EU

---

44 Scott Shane and Tom bowman, “RIGGING THE GAME Spy sting: Few at the Swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup—perhaps the most audacious in the National Security Agency’s long war on foreign codes; NO SUCH AGENCY,” *The Baltimore Sun,* 10 December 1995, last accessed 3 March 2020, https://www.baltimoresun.com/news/bs-xpm-1995-12-10-1995344001-story.html なお、本記事は、NSA による暗号解読手法として、他に、スーパーコンピューターによる純理論的暗号解読、米国国内での FBI 要員の外国施設侵入による暗号の入手、米国外での CIA の協力者工作による暗号の入手、米国企業に対する輸出許可権限をテコにした協力取付け（秘匿強度の制限、バックドア設置）などを挙げている。

45 資料自体は 2020 年 2 月 11 日に Scott Shane がツイッターで公表している。
”CIA/IA/Motorola Meeting—August 19-20, 1975,” in Scott Shane, Twitter post, 11 February 2020 (11:14pm), accessed 3 March 2020, https://twitter.com/ScottShaneNYT/status/1227242088057565190

46 CIA 資料抜粋。

47 これら一部の国とは、直接関与しているドイツの他、UKUSA シギント同盟の一員として情報成果の分け前を得ている英国、カナダ程度と推定できる。

諸国が気付いた場合、その政治的悪影響は大きく懸念が広がった[48]。NATO 加盟の友好国といえども躊躇なく標的とする米国の方針にドイツが附いていけなくなったのである。

また、1970 年代は、クリプト社は優良企業であり、純益を生み出していたが、1990 年代に入ると、電子機械式暗号機への需要が減少[49]して赤字体質となり、資金援助が必要となった。米国にとっては赤字補填をしても得られる情報に価値があったが、再統一後のドイツには財政的余裕が失われて、関与を嫌うようになったという[50]。

以上の事情で、1993 年ドイツ BND はクリプト社の経営から手を引いた。同年 9 月ドイツ駐在の CIA 代表と BND は合意に達し、クリプト社の BND 所有株は CIA が買い取り、この後は、米国単独でのクリプト社経営となる。

３　2018 年クリプト社の持株会社 AEH の解散

1993 年以降は、米国（CIA と NSA）が単独でクリプト社を経営してきたが、その後インターネット通信の発達、Pretty Good Privacy など公開鍵方式の普及によって、世界の暗号通信に占めるクリプト社製暗号機の重要性は急速に低下してきたと見られる。その結果、CIA と NSA にとって諜報源としてのクリプト社経営の重要性が低下し、遂に「クリプト社作戦」も終了を迎えた。

即ち、2018 年にクリプト社の持株会社 AEH（リヒテンシュタインに登記）は解散し、2 社がクリプト社の資産を買収した。一つは、CyOne Security 社であり、経営陣買収によってクリプト社元経営者が設立したもので、専らスイス政府にセキュリティ・システムを提供するスイス政府御用達専門企業である。もう一つは、Crypto International 社であり、クリプト社の国際事業を引き継いでいる。CyOne Security 社 CEO の Giuliano Otth は 2001 年以来クリプト社の CEO であり、米国インテリジェンス機関との協力の事情を良く知っていると見られるが、Crypto International 社の新経営者は、事情を全く知らないようである[51]。世界の顧客を相手とする Crypto International 社にとって、NSA との関係を暴露する報道がなされた現在、その将来展望は暗く、新経営者はとんだ不良資産を掴まされてしまったと言えよう。

第６章 教訓：インテリジェンスの実態と論理

以上、「クリプト社作戦」の全体像を概観してきたが、最後にインテリジェンスの世界において同作戦の持つ意味、同作戦から読み取れる諜報世界の実態と論理について考察してみよう。

---

48 CIA 資料抜粋

49　例えば、現在でも使用されている公開鍵暗号 Pretty Good Privacy は 1991 年に開発され、前世紀中に世界中で使用可能となった。本暗号は、NSA 文書を漏洩したウィリアム・スノーデンも 2013 年漏洩準備のための秘密通信に使用している。

50 CIA 資料抜粋

51 WP 報道

１　暗号解読・暗号攻略におけるヒューミント手法の役割

通信諜報の世界では、暗号解読・暗号攻略は主要な情報入手手法である。

その暗号解読・暗号攻略の歴史では、第二次世界大戦時の米国による日本外交暗号や海軍暗号の解読、或いは英国によるドイツ・エニグマ暗号の解読が有名であるが、ともすると暗号解読は数学的天才や異才の活躍の結果であるようなイメージが流布している。また、現代の NSA による解読手法として、スーパーコンピューターと高等数学を活用した純粋理論的な解読が知られている。

しかし、暗号解読では、天才や異才或いはスパコンと高等数学よりも、実は広義のヒューミントによる貢献が大きいのである[52]。その中には、在米外国公館への侵入[53]、協力者工作による暗号の入手、民間企業への働掛け（民間暗号技術の政策・規準への影響力行使、民間の暗号システムやネットワークへの弱点挿入）、配送途中の製品に対する工作などが挙げられる[54]。

そして、今回の「クリプト社作戦」の全体像の判明により、そのヒューミント的手法の暗号攻略に占める大きさが再確認されたのである。通信の秘密保全に関心を有する者は、このことを肝に銘じて、ヒューミント的手法による攻撃可能性も含めて広汎な通信保全措置を構築することが重要である。

２　友好国に対するインテリジェンス

「クリプト社作戦」では、単に第三世界の諸国だけではなく、米英の友好国も情報収集の標的とされていた。この背景にある友好国に対する諜報の在り方に関するインテリジェンスの論理は如何なるものであろうか。

その論理を明白に示した資料が NSA の開示資料[55]にある。それは友好国を含む第三国[56]との関係について述べたものであるが、表題「サード・パーティ諸国：パートナーにして標的」

---

52 グレゴリー・トレバートンはインテリジェンス専門家であり、2014～2016 年に亘って米国の国家諜報会議（National Intelligence Council)議長を務めた人物であるが、NSA による暗号解読は、多分高等数学やスパコンによるよりも暗号書の窃取の方が多いと、2001 年に記述している。Gregory Treverton, “Intelligence Crisis,” *Government Executive Magazine,* 1 November 2001, last accessed 9 March 2020, http://www.govexec.com/magazine/magazine-national-security/2001/11/intelligence-crisis/10254/

53 実際、NSA の開示文書によって、第二次世界大戦前の 1920 年代と 1930 年代に米国当局（この場合は海軍情報部であるが）は少なくとも 3 回、在ニューヨーク日本領事館に侵入して暗号書を複写したことが明らかにされている。

54 茂田忠良『米国国家安全保障庁の実態研究』（警察政策学会資料第 82 号、2015 年）第 2 部第 3 章３「暗号対策」中 126－130 頁参照。

55 開示資料、NSA、”Third Party Nations: Partners and Targets,” *Cryptologic Quarterly, Vol.7 No 4,* winter 1989, accessed 9 March 2020, https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/third_part_nations.pdf.

56 NSA にとってセカンド・パーティは、UKUSA シギント同盟を構築している英加豪ニュージーランド 4 ヵ国であるが、UKUSA 同盟は極めて密接強固な特別関係であり、この同盟諸国間では互いを標的にしないとされている。しかし米国 NSA は、これにも例外を設定し、国益が要求するならば UKUSA 同盟諸国であろうと標的とすることが許されるとしている。茂田『実態研究』第 3 部第 1 章１「英 GCHQ 概観と NSA との協力関係」188 頁参照。

が本質を明確に示しており、友好国も標的であることが前提とされているのである。同資料は更に「国家には友人も敵も存在しない、在るのは国家利益だけであると言われる」「今日の友人や同盟国も、いつまでも友人や同盟国である訳ではない」と記述しており、冷厳な国益追求が国家関係の基礎とされている。即ち、インテリジェンスでは、国益が合致する限りで協力し、一致しない範囲では互いを標的として諜報対象とすることが前提とされているのである[57]。

実際、米国の友好国であるイスラエル、フランスや韓国は、米国に対する積極的な諜報活動を行っている国として、米国 NSA の監視対象とされている[58]

なお、ドイツ BND は、「クリプト社作戦」が NATO 同盟諸国を標的としていたこともあって、同作戦から離脱したが、それもソ連崩壊とドイツ統合という世界の歴史的構造変化に伴う政治判断であって、離脱前は友好国に対する諜報成果を享有していたのである。

何れにしろ、インテリジェンスの世界における冷厳な国家関係を忘れるべきではない。

3　供給網工作～現代の「クリプト社作戦」

「クリプト社作戦」は、当初 NSA が解読困難な暗号機の販売時期と対象国を制限する「拒否作戦」から出発して、やがて解読を容易にする弱点を仕込んだ暗号機を販売する「積極工作」に至った。同作戦は 2018 年に終了したが、このように製品に弱点を仕込んで標的組織に届ける作戦は他に実施していないのであろうか。

実は、NSA は供給網工作（supply chain operation）の名の下に現在も同様の作戦を実施しているのである[59]。

---

[57] 茂田『実態研究』第 3 部第 2 章 1 「サード・パーティ関係とは」219-220 頁参照。

NSA 渉外局の資料でも、サード・パーティとの協力関係は無条件のものではなく、常にギブ・アンド・テイクの関係であり、協力関係の進展は、あくまで米国の国家諜報要求が相手国の国家諜報要求と交叉する場合に限られるとしている。

「米国と相手国の国家諜報要求が交叉する場合」とは、筆者の解釈では、シギント協力がそれぞれの国の国家諜報要求の充足に貢献する場合ということである。即ち、シギントに関する国家諜報要求の充足という面においてギブ・アンド・テイクの関係が成り立つ場合にのみ協力するし、シギント協力関係が進展するということである。

なお、危機的状況に於いては一方的なシギント支援があり得るとしている。これは、危機的状況にある国を支援することに米国の国益が合致する場合は、シギント面だけを見ればギブ・アンド・テイクの関係は成り立たないが、国益全体の立場からシギント支援をすることがあり得るということである。

何れにしろ、ここには、博愛主義もなければ、一方的なインテリジェンスやサービスの提供も存在しない。インテリジェンス活動が、国民からの付託を受けて且つ国民の負担の上に成り立っている以上（そして場合によっては構成員の人命の犠牲の上に成り立っている以上）、これは当然のことであり、世界のインテリジェンス業界の常識を述べたものである。

この点に関して元 NSA 長官マイケル・ロジャースの次の発言は味わい深い。「ファイブアイについてよくある勘違いは、全ての情報が一方的にもらえるということです。情報をもらいたいなら、出す覚悟も必要です。」マイケル・ロジャース、土屋大洋によるインテヴュー。『朝日新聞』2020 年 1 月 29 日付「サイバー監視は正義？」

[58] 茂田『実態研究』第 2 部第 1 章 2 「戦略的任務リスト」31 頁参照。

[59] 以下の本文の記述は、次を参照。

茂田忠良『サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～』（情報セキュ

即ち、供給網工作は製造段階での工作と製品配送段階での工作の二つに分けられる。「クリプト社作戦」は製造段階での工作であるが、スノーデン漏洩資料で判明したのは、後者の配送経路介入である。これは、標的組織がサーバーやルーター等のコンピュータ・ネットワーク関連製品を発注した場合、その製品を配送途中で一旦確保して、これにマルウェアを注入し或はマルウェア入りハードウェアを装入した上で、配送経路に戻して発注元に届ける方法である。具体例としては次の例が挙げられている。

○　シリアのインターネット基幹部品への工作

2010 年 6 月の NSA 内部資料によれば、「シリア通信事業機構」のインターネット基幹部分の製品（中枢ルータと推定される）に対して配送経路介入を実施した結果、シリアのインターネット通信の基幹部分に侵入できた。同基幹部分は携帯電話通信にも使用されていたため、極めて大きな情報成果を挙げたという。

○　中国製 VoIP 通信機材への工作

2013 年 4 月の NSA 内部資料によれば、NSA は中国から輸出される暗号化 VoIP 通信機材に対して配送経路介入を計画し、ヒューミント機関と第三国当局の協力を得て、海外において物理的介入を行った[60]。

４　米国以外の国は紳士か　～他の諸国による供給網工作

それでは、米国・UKUSA 諸国以外の国々はどうであろうか。他の国は紳士であってこのような「汚い」作戦は実施していないのであろうか。

既に、「クリプト社作戦」で見たように決してそんな事はないのである。そもそも、フランスもドイツも、クリプト社に食指を動かしていたのである。「クリプト社作戦」以外にも次のような例が判明している。

（１）ドイツ諜報機関 BND[61]

2005 年 10 月時点で、供給網工作を行うために幾つかのフロント企業を設立していた。（情報源：公式の渉外情報）

（２）フランス諜報機関 DGSE[62]

2002 年にセネガルのセキュリティサービスにコンピュータとファックスを提供したが、その結果 2004 年までにこれらのシステム上の全情報にアクセスできるようになった。（情報源：間接的に情報アクセスのある協力者）

（３）オランダ海軍情報部[63]

リティ総合科学第 11 号、2019 年 11 月）22－23 頁。

[60] NSA は海外における配送経路介入作戦のため、「海外遠征チーム（Expeditonary Access Operations）」という専門部署を設置しており、作戦実施においては、在外公館に設置した「特別収集サービス（SCS）」拠点なども活用している。

[61] 茂田『サイバーセキュリティとシギント機関』23 頁

[62] 茂田『サイバーセキュリティとシギント機関』24 頁

[63] Huib Modderkolk, “Nederland luisterde jarenlang landen af dankzij superchip,” *de Volkskrant*, 20 February 2020, accessed 25 February 2020, https://www.volkskrant.nl/nieuws-achtergrond/nederland-luisterde-jarenlang-landen-af-dankzij-superchip~bc9a9ce4/　本報道によれば、本文の事実が、今回漏洩された CIA 秘密文書「MINERVA

オランダ諜報機関も「クリプト社作戦」と同様の、製造段階における供給網工作を実施していた。

1970 年代末、オランダのフィリップス社とドイツのシーメンス社は共同で、テレックス暗号機「アロフレックス」を開発した。アロフレックスは暗号強度の高いことで知られ NATO 諸国に販売されていた。暗号強度が低い機種 T1000CA はその他の諸国に販売されていた。T1000CA は当時スーパーコンピューターで解読可能であったが、それでも 1 か月半を要したという。

そこで 1977 年、オランダ海軍諜報部は解読容易な特別のマイクロチップの開発に着手し、フィリップス社の協力を得て 1979 年春には完成させたという。特別なマイクロチップを挿入した T1000CA 通信の解読所要時間は半時間と大幅に短縮された。オランダは解読用機材を米 NSA と独 BND に販売したが、アロフレックスはクリプト社製品の競合製品であり、且つ、米独が解読のためオランダ製の特別機材を購入する必要があったのは、NSA にとっては面白くない展開であったであろう。

（4）中国、ロシアによる工作[64]

さて、では西側民主主義国家以外の国はどうであろうか。

当然、中国もロシアも取り組んでいるのである。

詳細は不明であるが、スノーデン漏洩資料によれば、2012 点時点では、中露両国とも、コンピュータ部品のバイオスを工作対象として注目しており、米企業の American Megatrends(AMI)と Phoenix Technologies の製品が攻略されていたとされる。

供給網工作は、世界の諜報機関が取り組んでいる標準的な情報収集手法であるということである。

5　華為、カスペルスキーとの関係

米国は近年、中国の巨大通信企業華為と中国政府との関係やサイバーセキュリティ会社カスペルスキー社とロシア政府との関係に疑惑の目を向けている。

例えば華為について、米国政府は中国政府の供給網工作などの情報収集に協力しているとの証拠は掴んでいないようである[65]にも拘らず、5G における華為製品の普及を抑制しようと、友好国に圧力を加えている。

米国が、何故、これら企業に危惧を持つのであろうか。それは米国自体がクリプト社など企業の協力を得て、或いは供給網工作を行って、諜報工作活動を成功させてきた歴史があるからである。

しかし、米国政府の危惧が自己のミラーイメージに基づく単なる杞憂かと言えば、そうとは言えないであろう。ソ連共産党によるロシア革命以来ソ連崩壊に至るまでの世界を対象にした 70 年間を超えるインテリジェンスの歴史、中国共産党による結党以来 100 年間に及ぶインテリジェンスの歴史を振り返れば、ロシア、中国両国のインテリジェンスは米国に勝る

– A HISTORY」（CIA インテリジェンス研究センター、2004 年）の内容から読み取れるという。

64 茂田『サイバーセキュリティとシギント機関』58 頁

65 茂田『サイバーセキュリティとシギント機関』＜補論＞ 対中国サイバーセキュリティ対策の話題 2 華為問題（中国による Supply Chain Operation）86-91 頁参照。

とも劣らない実績を誇っているのである。インテリジェンスにおける民間企業利用において、ロシア中国両国が米国より劣ると判断する根拠は全く存在しないのである。

これがインテリジェンスの世界である。

「クリプト社作戦」は、これらインテリジェンスの実態と論理を再認識できるケーススタディの教材なのである。

警察政策学会資料　第 113 号

テロ対策に見る我が国の課題
国民保護における避難
「クリプト社」と NSA（暗号攻略大作戦）

令和 2（2020）年 11 月

編集　テロ・安保問題研究部会

発行　警察政策学会

〒 102-0093
東京都千代田区平河町 1-5-5　後藤ビル 2 階
電話（03）3230-2918・(03-3230-7520)
FAX（03）3230-7007