JCLU創立70周年記念

ナショナルセキュリティ法に関する
アメリカ調査報告書
テロ対策と監視・テクノロジー

2017年10月

公益社団法人 自由人権協会

JCLU
公益社団法人 自由人権協会
Since1947

アメリカ調査報告書発行によせて

公益社団法人自由人権協会
代表理事　喜田村　洋　一
同　　紙　谷　雅　子
同　　芹　澤　　齊
同　　升　味　佐江子

公益社団法人自由人権協会（Japan Civil Liberties Union・ＪＣＬＵ）は、日本国憲法が施行された１９４７年１１月に、人権擁護を唯一の目的として設立されたＮＧＯです。憲法が、自由と人権は、国民の不断の努力によって保持しなければならないと定めていることを受け、その実現を目指す様々な市民が参加しています。

ＪＣＬＵは、政治的・社会的問題について、人権擁護の観点から取り組み、調査研究、講演会、出版などを通して、市民の立場で提言を行い、政府機関などに対して声明や意見を発表し、人権侵害を受けた人びとの裁判支援なども行っています。

現代は、目覚ましい技術革新により本格的なデジタル時代に突入し、ＩＴを活用した新しいサービスが次々と生まれ、私たちの生活はたいへん便利になりました。しかし、技術革新がもたらすのは、メリットだけではありません。一昔前には想像もつかなかったやり方で、個人に関する詳細かつ膨大な情報を収集し利用することが可能となり、プライバシーなどの人権が侵害されるおそれが拡大しています。それにもかかわらず、このような人権侵害を防ぐための法的な議論は、全く不十分です。

アメリカでは、９．１１以降、テロ対策を名目とする政府の監視活動が大幅に強化されていましたが、エドワード・スノーデン氏の内部告発があるまで、政府が市民のプライバシーを脅かす大量監視を行っていたことは顕在化しませんでした。今年４月に新たに公表されたスノーデン・リーク文書からも明らかになったように、アメリカの監視活動は日本とも密接に関係しています。また、日本でも、新しい技術を用いた捜査手法が進展しており、「共謀罪」法成立による捜査名目の監視活動の強化が懸念されています。

本調査報告書は、ＪＣＬＵ創立７０周年記念事業の一環として、アメリカの市民団体や学者からＪＣＬＵの会員が「テロ対策と監視・プライバシー」について聴き取りをした結果をまとめたものです。この問題に関するアメリカでの最前線の議論を紹介するものとして、今後、日本でこの問題に取り組む際の示唆に富むものと自負しています。

今後もさらに発展していくデジタル時代の中で、次々に新しい人権問題が生じ、それに対応する新しい法的枠組みや制度、運用が必要となっていきます。ＪＣＬＵは、当会の唯一の目的である「人権擁護」を、時代に即してこれからも考え続けていきます。

本報告書の意義──憲法学の観点から

千葉大学大学院専門法務研究科
准教授　　大　林　啓　吾

今回の報告書は、「テロ対策と監視」の問題について、アメリカの法制度、実際の運用、課題などを総合的に分析したものである。テロ対策は市民社会にとってきわめて重要な政策の一つであることは間違いなく、その手段として監視が重要であることも疑いない。しかし同時に、監視はプライバシーを侵害するおそれがあり、行きすぎた監視社会をもたらしてしまうのではないかといった懸念を抱える。そこで今回の報告書は、テロ対策の先端を行き、かつそれに対する議論も豊富なアメリカを素材に、実際の監視システムを解明しながら、その課題を考えるという内容になっており、今後の日本のゆくえを考えていく上でも重要な資料を提供するものと考えられる。

本報告書は、今後の議論に資するように、法制度や運用といったプラクティカルな側面を中心に検討しており、あえて抽象論は捨象している。そのため、ここでは報告書の内容を踏まえて、憲法学の観点から若干の補足を試みたい。

テロの時代においては、テロを防ぐことと、いきすぎたテロ対策を防ぐことのバランス（自由と安全のバランス）が重要であることは言うまでもない。そのバランスをどのようにはかるのかを考えるにあたり、場当たり的に考えるのではなく、そもそも憲法はどのような対応を求めているのかという根源的な問いに思考をよぎらせることが必要である。

かかる問題意識を踏まえ、アメリカでは、予防的立憲主義と最適化立憲主義という二つのアプローチが存在する。予防的立憲主義は立憲主義の瓦解を予防するのが憲法の中核にあるとする見解であり、このアプローチからすると自由と安全のバランスは自由に重きを置くことになる。テロ対策がいきすぎるとプライバシーを中心とした自由や権利を損ねるだけでなく、テロ対策の実働を担う執行権（行政権）の権力を拡大させてしまい、立憲主義が崩壊してしまうおそれがあるので、それを予防することこそが立憲主義であると考えるからである。これに対して、最適化立憲主義は予防的立憲主義のように自由の天秤を重くしすぎると、現実的対応ができなくなるおそれがあるので、自由と安全のバランスは個別に考えていくべきとする。

予防的立憲主義が憲法の理念を重視するという特徴を備えるのに対し、最適化立憲主義は現実を踏まえた対応をはかるという特徴を有している。テロの時代は最適化立憲主義でなければ対応できないのではないかと思える反面、そういう時代だからこそ予防的立憲主義が必要であるともいえる。いずれのアプローチも一長一短があるが、立憲主義の維持と現実的対応を考えると、最適化立憲主義を採用しつつ、バランシングが安全に偏らないように法制度や法理によって一定の法的枠組を備えていくことが肝要である。

それを踏まえると、本報告書が重要になってくる。なぜなら、法制度、運用、判例法理を分析しているので、法的枠組を検討するのに格好の素材を提供するからである。たとえば、FISA がどのような内容を定めているのか、FISC はどのように機能しているのか、第三者任意提供の法理はいかなる内容のものかなどの分析はまさにテロ対策の枠組であると同時に、テロ対策のいきすぎを防ぐための法的枠組でもある。まずはこれらの内容を理解し、その課題を検討して、日本にも応用可能な場面があれば、それをいかすことになろう。

テロの問題は、テロ対策とテロ対策のいきすぎの両方を同時に検討することが欠かせない。それは憲法の要請でもあり、法の役割と機能に不断の検討を迫るものでもある。

目　　次

はじめに …… 1
１．調査の目的と内容など …… 1
　Ⅰ．ナショナルセキュリティ法とは …… 1
　Ⅱ．テロ関連情報の収集、テロの予防、テロリスト及びその予備軍の摘発活動に関する法分野 … 1
　　①　情報収集としての大量監視の是非 …… 1
　　②　ムスリムに対する監視 …… 2
　　③　テロ支援活動の規制をめぐる法的議論 …… 3
　　④　テクノロジーとテロ対策をめぐる法的議論 …… 3
２．調査の日程と訪問先・ヒアリング内容の概観 …… 4
３．調査団の構成 …… 5
４．小括 …… 6

第１部 Center for Constitutional Rights（CCR） …… 7
１．CCR について …… 8
　Ⅰ．ヒアリング先 …… 8
　Ⅱ．CCR の組織・運営等について …… 8
２．政府のサーベイランス（監視活動）に対する CCR の活動 …… 9
３．現在 CCR が関わっている個別訴訟（ムスリムコミュニティに対する監視） …… 9
４．監視に対する訴訟の困難性 ……10
５．電子的監視の問題（スノーデンの告発を含む） ……11
６．パブリックな場での監視の問題 ……12
７．テロ対策についての CCR の立場 ……13

第２部　American Civil Liberties Union（アメリカ自由人権協会） ……15
１．アメリカ自由人権協会について ……16
　Ⅰ．ヒアリング先 ……16
　Ⅱ．アメリカ自由人権協会の組織・運営等について ……16
２．ナショナルセキュリティ分野の取り組みについて ……16
３．スピーチ、プライバシー及びテクノロジー分野の取り組みについて……17
４．プライバシーと国家安全保障のバランス ……18
５．政府のテロ活動に関する監視をいかに統制するか ……19
６．ディスカバリー制度等で得られる情報について ……20
７．ナショナルセキュリティ分野の情報公開に向けた努力 ……20
８．警察による監視捜査 ……21
９．EZPASS について……21
10. 新しい監視技術についての取り組み ……22
11. ロケーションプライバシーに関する議論 ……24
12. アメリカ自由人権協会の弁護士の仕事やキャリアについて ……25

第３部 Brennan Center for Justice（BCJ） ……27
１．BCJ について ……28
Ⅰ．ヒアリング先 ……28
Ⅱ．BCJ の組織・運営等について ……28
Ⅲ．自由と国家安全保障プログラムについて ……28
２．政府からの情報の開示について ……29
３．監視捜査について ……30
４．捜査・諜報活動とプライバシー、現状の手法が抱える問題……30

第４部 Professor Stephen Schulhofer（シュルホーファー教授） ……33
１．シュルホーファー教授のプロフィール ……34
２．FISC・FISA を利用した活動の拡大と濫用 ……34
３．FISC・FISA の活動が秘密にされることの是非 ……34
４．捜査機関による監視活動が正当か不当かを分けることができるのか……35
５．監視活動を秘密にする手続 ……36
６．FISC の存在意義　～日本等の諸外国との比較～ ……36
７．現行法制度の限界　～アメリカと日本の通信傍受に関する法律の規制の不十分性～ ……36
８．アメリカの現行法制度の状況 ……37
９．現行法制度の改正に関するアメリカ議会の動き ……37
10. 捜査機関及び諜報機関が取得した情報の管理・利用 ……38
11. データマイニングの問題　～連邦最高裁の展望～ ……39

第５部　Adjunct Professor and Executive Director of the Center on Law and Security
Zachary K. Goldman（ゴールドマン教授） ……41
１．ゴールドマン教授のプロフィール ……42
２．米国のインテリジェンスについて ……42
Ⅰ．インテリジェンスと捜査（刑事法） ……42
Ⅱ．情報の収集と利用 ……42
Ⅲ．データの種類ごとの規律、特にメタデータについて ……43
Ⅳ．政府と民間の関係性 ……44
３．外国人の保護と外交的な懸念 ……44
４．FAA702 条改正論議について ……45
５．データ使用のルールについて ……46
６．テロ対策の諜報活動とプライバシー保護のバランス ……47

参考資料
「プリズムの衝撃」大林 啓吾（JCLU Newsletter 387 号～389 号所収） ……50
「テロとアメリカ」井桁 大介（JCLU Newsletter 399 号～402 号所収） ……62

はじめに

本報告書は2016年４月から５月にかけて実施したナショナルセキュリティ法に関するニューヨーク現地調査の内容を報告するものです。

１．調査の目的と内容など

Ⅰ．ナショナルセキュリティ法とは

ナショナルセキュリティ法は、環境法や社会福祉法と同じように、特定の関心領域にまたがる法分野を横断的に理解するために用いられる概念です。用語の直訳のとおり国防・軍事に関する法制度も対象の一つですが、それにとどまらず、治安維持に関する分野であるテロ対策やスパイの摘発に関する法制度、さらにはこれらの分野から派生した捜査手法を規律する分野なども対象となります。

アメリカではかねてより確立されていた法分野ですが[1]、９．１１後に大いに発達しました。テロ対策に関する部分について言えば、その内容は大きく、①テロリスト集団（アルカイダや IS）やテロ支援国家に対する軍事活動をめぐるものと[2]、②テロ活動に関する情報を収集し、テロを予防し、テロリスト及びテロリスト予備軍を摘発するための捜査手法をめぐるものに区別することができます。

今回の調査研究はこのうち②に対象を絞って行われました。ニューヨークは９．１１により直接被害を受けた街であり、以後もしばしばテロの対象として名指しされるため、ニューヨーク市警は連邦政府と連携して最先端のテロ対策を追い求めています。そのため多くの NGO や研究者がその効果や弊害について分析しており、ナショナルセキュリティ法の議論が活発にかわされています。

Ⅱ．テロ関連情報の収集、テロの予防、テロリスト及びその予備軍の摘発活動に関する法分野

この分野は、さらに大きく以下の４つに区分することができます。

①　情報収集としての大量監視の是非

アメリカ政府の情報収集権限を飛躍的に広げたとされるのが、愛国者法（USA Patriot Act）と FAA（FISA Amendment Act）という２つの法律です。

愛国者法は 16 の章からなる膨大な法律で、９．１１から 45 日後に成立しました。テロ対策のために捜査機関の権限を広げたり、裁判所の監督を緩めたりする規定がいくつか含まれています。とりわけ捜査機関がきわめて緩やかな要件で民間会社の保有する個人情報を収集できるようにする規定（215 条など）は制定当時から

---

[1] アメリカにおけるナショナルセキュリティ法の代表的教科書である Stephen Dycus, et al., *National Security Law* は、現在六版が出版されていますが、その初版は 1990 年に出版されています。

[2] その詳細はさらに３つに分類することができます。第１に連邦政府が行うアルカイダや IS を相手方とする軍事活動を正当化する法的根拠、第２にロボットや戦闘ドローンの取扱い、拷問、暗殺などの可否といった、個別の戦闘行為をめぐる法律論、第３にグアンタナモに象徴される捕虜をめぐる法律論です。

物議をかもしていました。

FAA はアメリカ史上初めて裁判所の事前審査なしでの通信内容の傍受を認めた法律です。原則として国外にいる外国人を対象とする場合に限られてはいるものの、事後的に通信の相手方がアメリカ市民であることが分かった場合でも傍受内容の保有が許される場合があるなど、令状主義の潜脱となる危険があるとして批判されていました。

これらの法律によってアメリカ政府は、電話、メール、インターネットの検索履歴、SNS でのやり取りといった通信情報を取得する権限を有し、これを用いて膨大な通信情報を収集するようになります。しかし、いずれの監視捜査についてもほとんど情報公開がなされず、単発的な調査報道を除き、市民がその全貌を知ることはありませんでした。その状況を一変させたのが 2013 年６月から始まったいわゆるスノーデンリーク（スノーデン氏による暴露）です。これ以降、アメリカ政府による監視捜査をめぐる議論はナショナルセキュリティ法の筆頭分野となりました。

リークによれば、アメリカ政府は愛国者法を根拠としてアメリカ国内のすべての電話のメタデータ（メタデータとは「データのデータ」と言われるもので、例えば電話のメタデータの場合であれば、電話での通信がなされた「日時」「通話時間」「受信者番号」「発信者番号」等を言います）を毎日集めていました。また、FAA を根拠としてフェイスブック、ヤフー、グーグル、マイクロソフトなどの世界的なインターネットサービス企業に命じて、メール、ネット電話、SNS、インターネットの検索履歴といったあらゆるタイプのネット上の通信を提出させていました。アメリカ市民の情報収集に当たっては法律上最低限の歯止めがかけられていましたが、実際にはほとんど機能せず、多くのテロや犯罪と無関係の通信情報が収集されていました。アメリカ国外の外国人については何の保護もありません。ネット会社から提出させる情報だけでなく、スパイウェア（利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム）などを利用して、世界中の人々のコンピュータ内の情報を取得していたとされています。

この監視活動は激しい反発を招きました。2015 年には９．１１後、初めて捜査機関の監視権限を弱める方向の法改正がなされるなど、議論は現在進行形で発展しています。

この監視権限に関する法的根拠や憲法・国際法との整合性などを研究する分野が、一つ目の大きなテーマです。

② ムスリムに対する監視

９．１１テロはムスリム過激派であるアルカイダによって行われました。アルカイダはその後壊滅させられますが、そのあとを受けて IS やボコハラムなどが反アメリカ・反異教徒を旗印に活動を続けています。

そのためいくつかの国ではムスリムをひとからげに対象として、信仰の深さなどにも着目する徹底的な監視捜査を行っていますが、ニューヨーク市警はその筆頭でした。2011 年８月には AP 通信の調査報道により、ニューヨーク市警がニューヨー

ク州やニュージャージー州などにおいて、テロと全く無縁にもかかわらずただイスラム教と関係があることのみを理由として、ムスリム個人の個人情報を集めたり、モスクを監視したり、学生団体にスパイを送り込んだり、商店やレストランの情報を細かく集めてデータベースを作っていたことが暴露されました。日本政府も同様です。2010 年 10 月にインターネット上に流出した内部資料によって、日本の警察が日本全国に住むすべてのムスリムを対象として詳細な個人情報を集めてデータベースを作成したり、モスクに監視カメラを設置して 24 時間体制で監視していることなどが明らかにされました。

このように一つの宗教を信じていることのみを理由とする監視活動は、人権侵害や差別ではないのか、またそもそもそのような監視活動に効果はあるのかといったテーマが、社会学や宗教学などと連携しつつ、活発に議論されています。

③　テロ支援活動の規制をめぐる法的議論

テロリスト予備軍の摘発や、テロ団体の力の削減のために、様々な規制が取られています。例えば、ツイッターに過激派の思想内容をつぶやいたり、IS が実効支配する地域への渡航を SNS で予告したりすることを理由に逮捕される例がおきています。またテロリスト団体に対して法的な助言をすることなどを処罰する法規制もなされています。

このようにテロ対策の一環として様々な活動が犯罪として取り締まられるようになりましたが、その定義が曖昧であるなど[3]、表現の自由と抵触する可能性があることを理由に様々な議論がなされています。

④　テクノロジーとテロ対策をめぐる法的議論

この分野で最も重要な議論はサイバーセキュリティに関するものです。現代生活はインターネットやコンピュータ処理に大きく依存しており、ひとたび大規模なサイバーテロが起きれば軍事的テロに勝るとも劣らないほどの人的・経済的・社会的被害が生じるといわれています。他方でサイバーテロの予防はインフラ（ネット通信網、サーバ、検索システム、メールシステム、SNS を運用する会社など）を提供する民間会社に大きく依存しています。政府が民間会社に任意の連携を求める場合もあれば、警察の申請に基づく裁判所の令状により強制する場合もあります。テクノロジーの進化に即して、これらの法的関係を整理する分野が大いに発展しています。2016 年に裁判で争われた FBI 対アップル[4]は記憶に新しいところです。

また、テクノロジーの進化は捜査手法にも影響を及ぼしています。精巧な顔認証システム、DNA データベース、GPS 捜査、データマイニング[5]など、一昔前では

[3] *Holder v. Humanitarian Law Project et al.*, 561 U.S. 1(2010)では、助言等を犯罪化する条文について、漠然不明確ゆえに無効であるという主張を原告がしましたが、最高裁によって退けられました。

[4] 詳細は末尾参考資料・JCLU Newsletter 399 号 井桁大介「テロとアメリカ 第 1 回 アップル対 FBI」参照。

[5] 統計学、パターン認識、人工知能等のデータ解析の技法を大量のデータに網羅的に適用することで知識を取り出す技術のこと。

SF の世界にしか存在しなかったような捜査手法が現実のものとなっています。他方、その捜査手法を規律する権利論・手続論はいまだ発展途上です。新たな技術が世に出るにつれ、新しい議論が繰り広げられています。

２．調査の日程と訪問先・ヒアリング内容の概観

調査日程及び主な訪問先は以下のとおりです。

日　付	訪　問　先　な　ど
4/29(金)	CCR 訪問 アメリカ自由人権協会訪問
5/2(月)	シュルホーファー教授訪問 BCJ 訪問 ゴールドマン教授訪問

今回の調査では次の５か所でヒアリングを行いました。各ヒアリング先の組織や人物の詳細は後記第１部から第５部に記載しています。ヒアリング先はいずれも最先端のナショナルセキュリティ法に精通した実務家・研究者です。

第１部 Center for Constitutional Rights（CCR）
第２部 American Civil Liberties Union（アメリカ自由人権協会）
第３部 Brennan Center for Justice（BCJ）
第４部 Professor Stephen Schulhofer（シュルホーファー教授）
第５部 Adjunct Professor and Executive Director of the Center on Law and Security Zachary K. Goldman（ゴールドマン教授）

ヒアリングの概要を、上記の分類（①情報収集としての大規模な監視の是非、②ムスリムに対する監視、③テロ支援活動の規制をめぐる法的議論、④テクノロジーとテロ対策をめぐる法的議論）に応じて整理すると以下のとおりです。

第１部 CCR

CCR では、主に「②ムスリムに対する監視」についてヒアリングしました。AP 通信の報道の後、ニュージャージー州に住むムスリムらが原告となって、ニューヨーク市警を相手取る訴訟（Hassan 事件）が提起されましたが、CCR はその訴訟を中心となって支援する NGO です。Hassan 事件は、ヒアリングの数か月前に連邦高裁において勝訴的な破棄差戻し判決が出されています。ヒアリングでは、この事件を担当する弁護士に、訴訟の展開や法律上の争点などの詳細を伺いました。

第２部 アメリカ自由人権協会

アメリカ自由人権協会では、主に「①スノーデンリークによって暴かれた大規模な監視」、「②ムスリムに対する監視」及び「④監視に用いられる最新技術」につ

いてヒアリングをしました。

アメリカ自由人権協会ニューヨークオフィスにはスノーデン氏の代理人であるベン・ワイズナー氏が所属しており、スノーデンリークをめぐる政府との攻防の最前線ともいうべき事務所です。その他政府の大規模監視をめぐる訴訟をいくつも手掛けています。

ムスリム監視に関しても、ニューヨーク州に住むムスリムらが原告となって提訴した訴訟（Raza 事件）を中心となって支援しており、こちらの事件もヒアリングの数か月前に、ニューヨーク市と画期的な和解を勝ち取っています。

さらに、ニューヨーク市警は最先端の科学技術を監視捜査に用いているとされており、その全体像を明らかにするための情報開示請求や、プライバシー侵害の恐れのある技術の差し止めを求める訴訟の提起など、進行形の議論を伺いました。

第３部 BCJ

BCJ では、主に「①大規模な監視」に関する議論として、政府が監視の根拠とする法がはらむ問題点や、大規模監視の有効性などをヒアリングしました。また、ナショナルセキュリティ分野に特有の情報公開に関する問題についても実務的な問題点を伺いました。

第４部 シュルホーファー教授

シュルホーファー教授は、「①大規模な監視」の法的根拠とされた FISA（Foreign Intelligence Surveillance Act）などの法制度を研究対象としており、その制定の経緯や全体像などについて詳細な解説を伺いました。

第５部 ゴールドマン教授

ゴールドマン教授はナショナルセキュリティ法の専門家として、政府（テロリズムの資金調達に関する情報収集部門や防衛省）と民間の法律事務所での勤務経験があり、実務的な観点から①大規模監視の法的評価を中心にヒアリングを行いました。

３．調査団の構成

今回の調査には、自由人権協会の以下のメンバーが参加しました。

藤本　美枝　（理事・現事務局長・７０周年ＰＴ座長）
二関　辰郎　（理事・前事務局長）
牧田　潤一朗（会員）
出口　かおり（同上）
藤原　大輔　（同上）
井桁　大介　（理事・NYU 客員研究員（当時））

４．小括

今回のヒアリング調査はスノーデンリークの衝撃が色濃く残る中、メンバーの関心もあって大規模監視の法的問題について多くの時間が割かれました。テーマが絞り込まれたことにより、多角的な視点からヒアリングすることができ、この重要な問題について重層的な全体像を浮かび上がらせることができたと感じています。

今回のヒアリングによる成果は、テロ対策を名目とする政府の権限行使にどのように対抗していくか、どのように情報を公開させ、どのような法制度により濫用を防ぐかといった普遍的な課題に大いに役立つものと確信しています。各ヒアリング内容をご一読いただければ大変嬉しく思います。

2017 年 10 月　調査団一同

第 1 部

Center for Constitutional Rights (CCR)

（CCR ホームページより転載）

（CCR 事務所にて）

１．CCR について

米国憲法及び世界人権宣言が保障する権利の実現を目的とした非営利組織。公民権運動の代理をしていた弁護士によって１９６６年に設立された。貧困層、有色人種のコミュニティなどを、訴訟、教育、啓発活動等によって支援している（ホームページより：https://ccrjustice.org/）。

Ⅰ．ヒアリング先

・Omar Farah 氏

以前はホワイトカラーの犯罪や国際的な仲裁事件を取り扱う法律事務所に勤務していた。プロボノとしてグアンタナモ案件を扱うにつれて関心が移り、CCR に移籍した。過去の経歴を生かして CCR をはじめとする NPO と通常の法律事務所の橋渡しもしている。

・Shayana Kadidal 氏

以前は商事取引や起業支援、海外の金融案件などに携わっていた。９．１１の際ボランティアとして CCR に関わりそのまま移籍した。「海外金融案件から海外抑留案件に移籍したわけだ」（本人談）。CCR では主にグアンタナモ案件を手がけており、その他監視の問題も扱っている。

Ⅱ．CCR の組織・運営等について

事務所はビル[6]の２フロア。他の地域に支部などはない。発足時から現在にかけて、年間予算は 100 万ドルから 800 万ドルに[7]、専属弁護士数は５人から 16 人に増加した。収入の大半は、会員からの会費である。多くの会員がいるとそれぞれの関心事がばらばらなので議論のある案件を抱えると資金が枯渇するリスクがある。CCR の寄付者には富裕層が少ない。その分あまり変動がなく、活動内容も一貫している。

グアンタナモやテロ関与者の弁護は様々な意味でリスクが高い。アメリカ自由人権協会がこのような問題を手がけようとして、国民からの反発などで寄付金が集まらず解散・縮小することになったら大変なこと。このような議論を呼ぶ分野は大きな組織が手を出しにくい。他方で CCR が解散することになっても影響は小さい。小規模であることが重要である。

取り扱う事件の選択やメンバー編成の際は、官僚的にならないよう気をつけている。個々の弁護士が判断する体制になっている。

弁護士以外にファンドを集める担当が５人いる。シリコンバレーの資産家は市民的自由に関心があり、政府がプライバシーに立ち入ってくることを嫌う。プライバシー問題に関心がある。９．１１のテロ以降、サンマイクロシステムやアマゾンの設立メンバーの一部が大口寄付者となっている。

大手事務所の弁護士に事件を振り分けることもしている。グアンタナモの案件は、

[6] マンハッタンのダウンタウンの目抜き通りに位置するオフィスビル。１フロアは 100 坪ほどか。
[7] なお当初の 100 万ドルのうち３分の１は借り入れでまかなっていたとのこと。また、比較としてアメリカ自由人権協会は１億ドルの年間予算、３億ドルの年間寄付金がある。

当初は死刑専門弁護士も含めて誰もやりたがらなかった。CCR が支援した事件で 2004 年に最高裁で勝ってから[8]、600 人いる抑留者の多くから依頼を受けて事件数が激増したので、外部の弁護士 500 人くらいに割り振った。

割り振る際には訴訟戦略などに関して外部弁護士に研修している。これらを通じて外部の弁護士とつながりができたのは大きい。グアンタナモのほかフライリスト問題[9]も大手事務所の弁護士と一緒にやっている。彼らとは収入や隣人、ライフスタイルも異なるが、このような事件を共同して受任することはお互いに財産である。

CCR は憲法上の問題が含まれる事案を主に取り扱う。グアンタナモを除き、個人の単独の事案は取り扱わない。アメリカ自由人権協会などの別の人権団体とも密にコミュニケーションを取り、情報を得ている。こちらから原告候補者にアプローチすることもある。

訴訟提起には謙抑的である。訴訟により原告となる人の身を危険に晒す可能性を承知しているためである。

２．政府のサーベイランス（監視活動）に対する CCR の活動

訴訟は政策形成的に意味がある場合に行う。市民の自由や社会正義に関する独立したキャンペーンは行っていない。グアンタナモ案件については、訴訟と啓発活動を両方行っている。９．１１以降は、国内の国家安全保障、対テロ施策にどう対応していくかが活動の中心になっている。

ムスリム監視の問題は、以前から関心をもって対象の人たちといろいろコンタクトをとって関わっていた。そういうところから訴訟になることもある。

３．現在 CCR が関わっている個別訴訟（ムスリムコミュニティに対する監視）

2011 年、AP（アソシエイトプレス）通信社によりニューヨーク市警察（NYPD）のムスリム監視プログラムが暴露された。ニューヨーク、ニュージャージー、コネチカット州等のムスリムのコミュニティを対象に、監視をしてマッピング（地図ないし分布図の作成）をするという特殊な部門が作られていることが明らかになった。ムスリムであることのみを理由とした監視、マッピングは、合衆国憲法の修正１条（信教の自由)、修正 14 条（平等）に違反すると主張して、ニューヨーク市などを相手取りニュージャージー連邦裁判所に提訴した。特定の人種、信教のみを対象とし、他は対象としないという取扱いの差別が違憲であると考えている。

プライバシー違反の主張はしていない。監視プログラムは公道など公の場所で行わ

---

[8] Rasul v. Bush, 542 U.S. 466 (2004)。キューバのグアンタナモ米軍基地に抑留されたイギリス人とオーストラリア人の家族が申立人となり、抑留の違憲性を理由に人身保護令状の発布を求めた事件。CCR が支援した。グアンタナモの外国人抑留者に人身保護令状の申立適格があるかが争われた。この訴訟で 申立適格を認める最高裁判決を勝ち取ったことにより、その後多くの抑留者に裁判で抑留の違法性を争う道が拓けた。

[9] アメリカにはテロ関係者であることなどを理由に飛行機への登場を禁止するリスト、いわゆるフライリスト（ノーフライリスト）があり、このリストに掲載されるとあらゆる飛行機に搭乗できなくなる。しばしばテロと全く関係がない市民がリストに掲載され、多大な不便を被ることが社会問題となっている。

れていたためである。個人情報を大量に収集して利用している事実が明らかになれば完全な抹消を求めたいところだが、本件では NYPD が大量の個人情報を収集したかどうかわかっていないためその点は主張していない。

原告は、ムスリムが運営する会社、モスクの連合体、ムスリムの学生団体、ムスリム個人等である。NYPD を相手に訴訟を起こす勇気を原告にもってもらうことは容易ではなかった。監視対象であるならばあまり目立ちたくないというのが自然だろう。監視の詳細が分からない中で原告をどのように選択するかは、この種の訴訟の一般的に難しいところである。本件では AP 通信の報道で個人名、ビジネス名が明らかにされていたので、原告の選択は比較的容易であった。

この訴訟は地裁で却下されたが、控訴審で勝訴し、現在地裁に破棄差戻審が係属している。

AP 通信が、報道するにあたり本件の具体的な情報をどのように得たのかは不明であるが、きっかけは NYPD の内部告発だったようである。その後、かなり多くの書類が開示されている。マッピング、監視の報告書等が開示されているが、それ以上詳しいことは分かっていない。報道がなければ NYPD は秘密裏に継続していただろう。

私たちは訴訟を通じてさらなる情報開示を求めている。アメリカの法的システムでは、開示は原則として法廷で勝ち取らなければならない。ニューヨーク市は示談による決着を目指しており、開示には消極的で、未だ証拠開示を得られていない。

今後、秘密裏に行われた監視について、原告らがどのようにして自らが監視対象であることを認識したか、どのように感じたかという点を立証していく必要がある。これらは容易ではない。ただ、控訴審判決により、NYPD が特別な監視対象として分類した時点で、現実の危害として、憲法の平等保障条項の問題が発生するとされた。そうすると、モスクで監視されていたからモスクに行けなかったなどの具体的な監視行動による不利益（萎縮効果）を立証できなくてもよいということになる。

４．監視に対する訴訟の困難性

ムスリムに対する監視と NSA（アメリカ国家安全保障局）による監視とは問題の次元が若干異なる。

NSA の監視はスノーデンリークの以前から単発的に報道されていた。最初に 2005 年 12 月に報道され、訴訟が提起された[10]。NSA が通信内容を監視すると、弁護士やジャーナリストがクライアントと秘密裏にコミュニケーションをとることができなくなる（例えば、グアンタナモの抑留者の海外の家族や海外の同僚弁護士と秘密裏に連絡が取れなくなる）ことが主張の骨子であった。2013 年、最高裁は原告らの主張は憶測に基づくものであり、現実の危害が生じたとは言えず、訴訟要件を欠くとして訴えを却下した[11]。明言されたわけではないが、自らがターゲットであることを具体的

[10] CCR v. Bush (later, CCR v. Obama)。この訴訟は第 9 区連邦巡回控訴裁判所が第一審裁判所による却下を支持し、2014 年に連邦最高裁が申立てを棄却して終了している。

[11] Clapper v. Amnesty International, 568 U.S. 398 (2013)のこと。外国諜報監視法（FISA）による NSA の監視の違憲性を争った訴訟。同法は当初、アメリカ国内の政府の諜報監視活動を規制するもので、原則として政府にアメリカ人の通話や電子メールでの通信を監視する前に令状を取ることを求

に立証できなければ監視の是非を問う訴訟を提起できないと言っているに等しい。

しかも、監視に関する訴訟にはさらなる困難がある。たまたま証拠を入手しても、機密情報を理由に訴訟での利用を制限される点である。例えば 2007 年、イスラムの慈善団体が政府から突然テロ支援組織として指定され資産を凍結されたため、政府を相手取り訴訟を提起した。政府は訴訟においてテロ組織であることの根拠として８０頁ほどの資料を提出した。その中に、NSA が当該団体の理事と顧問弁護士との間の電話の内容を傍受したものが含まれていた。この資料をもとに NSA の監視をめぐる訴訟を提起しようとしたが、機密文書であることを理由に証拠として提出することは許されなかった。現実に監視の被害を受けていることを明らかにする資料があり、かつ、その資料を入手した経緯に何ら違法な手続が含まれていないにもかかわらず、証拠とすることができない。証拠がなければ、訴訟を起こせず、また監視プログラムの内容を証明することができない。ACLU v. Clapper 事件[12]は、政府がスノーデンリークの内容を真実と認めたために訴訟を提起することができた稀なケースである。

５．電子的監視の問題（スノーデンの告発を含む）

裁判所は、外国を対象とする電子的な監視については、テロ対策としての効果をある程度認めているように感じる。他方でムスリム監視はあまり効果がないと考えたのではないか。

実際は全てを対象とした電子的監視は当局のフォーカスがぼけてしまい効率的でない。本当の脅威に注意が向かない。伝統的な令状主義（裁判所に証拠を提出して嫌疑に基づく捜査）アプローチが効果的である。

電子的監視に関しては、前述のとおり Clapper v. Amnesty 事件で最高裁が訴訟要件を認めていないため訴訟を起こすのは無益と判断した。もちろん CCR が、訴訟として勝ち目が薄い場合でも政治的な運動を盛り上げるために提訴することはある。活動家やマイノリティに、支援していることをメッセージとして届けることに意味がある場合である。ただ、電子的監視はこの限りでない。政府、議会、司法府の三権で電子的監視を評価する判断が出ているので、CCR としては、これを覆すための活動より

めていた。しかし、2001 年、ブッシュ大統領は、NSA が令状なしに盗聴を行うことを承認し、2008 年に議会は FISA 修正法でそれを承認して延長し、NSA が監督をほとんど受けずにアメリカ人の国際電話及び国際メールを傍受することを認めた。ブッシュ大統領が同修正法成立のサインを行った直後に、アメリカ自由人権協会は、外国の市民と電話及び電子メールで、機微で時には守秘義務のあるやり取りをすることが要求される仕事をしている弁護士や組織など多くの利害関係者を代表してこの訴訟を提訴した。2013 年２月、連邦最高裁は５対４の僅差で、訴訟要件を欠くとして訴えを却下した。

[12] ACLU v. Clapper 事件。2013 年６月 11 日、アメリカ自由人権協会が NSA（アメリカ国家安全保障局）によるアメリカ人の通話記録の大量収集の合法性を巡って提訴した事件。原告はその手法は憲法修正１条で保障されている表現の自由及び結社の自由のみならず、憲法修正４条で保障されているプライバシー権の侵害になると主張した。原告はまた、その計画は愛国者法 215 条で議会が与えた権限を越えているとも主張した。2015 年５月、控訴審裁判所は、通話記録計画は愛国者法 215 条に違反していると判断した。数週間後の 2015 年６月１日、2001 年に愛国者法が成立してから初めて一時的に愛国者法 215 条の期限が切れた。次の日、議会は USA 自由法を成立させ、215 条をアメリカ人の通話記録の大量収集を禁止する内容に修正した。

も、むしろ暗号化などで自己防御することに注力している。

先ほど述べた Clapper v. Amnesty 事件は、プリズムプログラム[13]を認める立法に異議を唱えるものであったが、スノーデンリークの５か月前に敗訴判決となった。もう少し経てばスノーデンリークが起きて判決の内容が変わっていたかもしれず、タイミングが悪かったともいえるが、逆にこの判決を受けてスノーデンが告発した可能性もある。

６．パブリックな場での監視の問題

アメリカにおいてプライバシーを保護する法的根拠は合衆国憲法修正４条[14]である。しかし過去の判例法理により、一般の目に触れる場では基本的にプライバシーは保護されないとされている。2012 年の Jones 判決[15]はこの流れを変える可能性がある。

この事件は、警察が麻薬密売人の車に無断で GPS を取り付け、非常に長い期間車の動きを監視したというケースである。この捜査が修正４条に違反すると判断されたが、連邦最高裁判決の多数意見は、個人の車に GPS を取り付けた行為自体が、個人の財産に対する不法侵入（トレスパス）に当たることを理由とするもので、従来の判例法理に依拠しており射程は短い。他方で同判決の補足意見は、監視の期間や内容によっては、公共の道路であっても、修正４条違反になるというもので、デジタル時代のプライバシーの特殊性を踏まえたものとなっている。ただ多数意見ではないので判例変更はされていない。

データマイニング（大量のデータを集めて保存し分析することで、そこから何らかの法則性など価値のある情報を引き出す取り組み）についてご質問を受けたが、この点は CCR が手がけるムスリム監視の問題が参考になる。ニューヨーク市は、1980 年代に交わされた和解によって、個人の政治活動に関する情報を収集し利用することを制限されている。モスクへの出入りを政治的な活動と捉えれば、これに抵触する可能性がある。NYPD がそのようなデータベースを作成していたということがあれば、CCR の訴訟でも主張していく。

一般的に政府がデータマイニングを用いる目的は、大量の監視により大規模なデータベースを作成し、裏切りの心配があるうえ高価な人間のスパイ（を使わなくても、テロ容疑者を探索できるようにすることと理解している。しかし、どのアルゴリズムが効果的かを判断することは容易ではない。例えば、アフガニスタンを発信場所とする電話番号から、１時間でアメリカ国内にいる 10 人に電話をしていると分かったとしよう。確かに怪しいとも言えるが、家族が結婚することがわかり舞い上がって親戚や友人に電話しているだけかもしれない。テロ計画という極めてレアな状況は滅多に

---

13 アメリカ国家安全保障局（NSA）が運営する秘密の通信監視プログラム（後出参考資料「プリズムの衝撃」参照）。

14 合衆国憲法修正第４条

「不合理な捜索および押収に対し、身体、家屋、書類および所有物の安全を保障されるという人民の権利は、これを侵してはならない。令状は、宣誓または確約によって裏付けられた相当な理由に基づいてのみ発行され、かつ捜索すべき場所、および逮捕すべき人、または押収すべき物件を特定して示したものでなければならない。」

15 United States v. Jones, 565 U.S. 400 (2012)

起こらない。そうすると何でもない情報を誤ってテロ計画としてピックアップしてしまう可能性がある。実際、無実の人を含んでしまう可能性がかなり高い。NSA が実施していた電話の大量監視プログラムは 10 年以上実施されていたが、テロ予防に役立ったという報告は１件もない。

データマイニングの効果検証が重要である。そのためには、テロが起きた後に事後的に検証し、データベース内のどの情報が関連していたかをトラッキングする必要がある。

７．テロ対策についての CCR の立場

マイノリティの監視は安全保障にとってもマイナスである。警察から監視されていると、マイノリティの人達はテロや犯罪に関する情報を得ても、災難に巻き込まれる可能性が高まるため警察に通報しなくなる。貴重な情報を得られなくなる点で逆効果である。信教の自由、プライバシーを保障することこそ安全保障にプラスである。

メディアは市民の自由と安全保障がトレードオフの関係（一方を得るためには他方を犠牲にする必要のある関係）にあるかのように報道するが、これは誤りである。アメリカ人口の 10%はアメリカ人ではないので、これらのマイノリティが犠牲にされてしまう。

有効なテロ対策は、伝統的な警察のアプローチしかない。足で情報を集めて、裁判所から令状を得る。そうすれば警察の行動は裁判所によって監督される。真摯に努力して情報を集めることが重要である。

テロは歯止めをかけることが困難である。重要なことは、簡単に攻撃できるような対象（100 階建ての建物など）を作らないなど、ダメージを最小限にするための努力だが、一般市民にはなかなか受け入れられにくい。９．１１のダメージが大きく、また技術が進み破壊力が大きいテロが起きていることが原因だろう。確率論的には雷に打たれて死ぬよりテロで死ぬ方が少ない。そもそもテロというのは極めて例外的な出来事なのだが、９．１１後に大きなテロ攻撃が起こっていないことについては、テロが稀だからではなく、ブッシュのテロ対策が奏功しているためだと捉えられてしまう。

大規模なテロ攻撃の事例を見ても、多くの場合で当局は攻撃が起こる前から犯人に関する情報を掴んでいる。９．１１についてもパリの事案でも同様である。しかし、９．１１のインパクトが大きすぎて、人々の正常な判断が失われてしまっているし、これを政治的に利用しようとする動きもある。

人々が恐怖心にあおられて正常な判断ができない理由は、昔のテロは人質をとってテレビで長く報道されるようなタイプだったが、最近のテロ攻撃は大量の人が無差別に攻撃され被害が大きくなるようになったところにもある。

第 2 部

American Civil Liberties Union
(アメリカ自由人権協会)

(アメリカ自由人権協会ホームページより転載)

(アメリカ自由人権協会事務所にて)

１．アメリカ自由人権協会について

アメリカ自由人権協会（ACLU）は、1920 年に設立された。米国内のあらゆる人の権利を守ることを目的とする、非営利、無党派の人権擁護団体である。

LGBT の人々に対する完全な平等の実現、デジタル時代における政府による広汎な監視に対する新たなプライバシー保護の確立、大量投獄の是正、選挙権や妊娠中絶の権利の保持など、アメリカ自由人権協会は困難な人権課題や、政府の濫用や行き過ぎから全ての人を守ることに取り組んでいる（ホームページ https://www.aclu.org/）。

Ⅰ．ヒアリング先

・Hina Shamsi 氏

ナショナルセキュリティープロジェクトのディレクター。同プロジェクトのテーマは、米国の安全保障政策や実務を憲法や市民的自由、人権と整合させること。

・Alex Abdo 氏

スピーチ・テクノロジー・プライバシープロジェクトのスタッフ弁護士。同プロジェクトのテーマは、合衆国憲法修正１条の定める表現・結社の自由の拡充と保護、プライバシーの権利の拡充や自己情報コントロール権の拡大に関する調査研究活動など。NSA 等による監視の問題を担当している。

・Nathan Freed Wessler 氏

スピーチ・テクノロジー・プライバシープロジェクトのスタッフ弁護士。FBI や国家安全保障庁など、警察組織の監視の問題を担当している。

Ⅱ．アメリカ自由人権協会の組織・運営等について

ほとんどの資金は民間の財団や資産家から。政府の援助は一切受けない。これは鉄則である。政府から資金を得るのは、勝訴の際に法律に基づいて弁護士費用の支払を受ける時だけである。

２．ナショナルセキュリティ分野の取り組みについて

ACLU ではどのプロジェクトでも、注力するテーマに関する優先順位を戦略的に決めている。ナショナルセキュリティ分野の優先的なテーマは以下の４つである。

①宗教・人種をめぐる差別の是正
②グローバルな戦争をめぐるパラダイムの制御、グアンタナモでの違法な抑留、ドローンを使った対象者の監視など
③アメリカ政府による国外での不法な拘禁・拷問
④NSA の監視、ウォッチリスト、ノーフライリスト（搭乗拒否者リスト）[16]の是正

[16]アメリカにはテロ関係者であることなどを理由に飛行機への登場を禁止するリスト。ただし９頁注９参照。

３．スピーチ、プライバシー及びテクノロジー分野の取り組みについて

プライバシーとテクノロジー分野の中心テーマは、21 世紀にふさわしい新たな合衆国憲法修正４条を築くこと。新たなテクノロジーによるプライバシー侵害に対応することである。

スピーチ分野の中心テーマは、オンライン上の言論に対する検閲など。近年、連邦政府や地域の学校がオンライン上の表現を監視しており、その対応がテーマである。また、自由な言論が引き起こすコンフリクト（ヘイトスピーチなど）にも取り組んでいる。

NSA による監視の手法に関心が強い。長年にわたり NSA の監視手法を明らかにすべく活動してきたが、政府が情報を隠すため、これまではそもそも戦う土俵に立つことができなかった。スノーデンリーク以前は、ほとんどの訴訟が本案審理にすら入れず、却下されていた。

スノーデンリークにより状況は大きく変わった。政治家や裁判所が監視の適法性について真剣に検討するようになった。

NSA は毎日、米国内のすべての電話のメタデータを集めて、疑わしいと判断した対象者の情報を別のデータベースに移していた。ACLU はスノーデンリークから数日後にこの監視捜査を対象として訴えを提起し、控訴裁判所からこの監視プログラムは違憲・違法であるとの判断を得た。その後、連邦議会が 1970 年以来初めて、政府の監視権限を弱める法律として米国自由法（Freedom Act）[17]を成立させた。これは大きな成果だ。この法律には透明性を高める規定がいくつかある。これにより将来の監視活動を構造的に阻止することが可能になるはずだ。ただ、対象はアメリカ国内における情報収集に限られてしまった。国外の通信を対象とする監視捜査に関する透明性も高められる必要がある。その他様々な問題に取り組んでいる。他にもいくつかの訴訟を手掛けている。

リーク後、多くの人がプライバシーに関して議論するようになった。皆が関心を持つテーマになった。これは非常に勇気づけられることだ。

今後検討されるべきこととして二つの問題がある。

一つは、電話のメタデータの収集プログラムのような、米国内における大量監視に関する問題だ。メタデータの収集プログラム以外の NSA の活動内容にも焦点を当てることが重要である。この中には海外・アメリカ間の通信をめぐる監視も含まれる。

もう一つは海外における監視である。この点は今回のリークでもあまり情報が明らかになっていない。原則として、政府は海外ではほとんど制限なく監視活動を行っている。どのような形で侵略的な大量収集プログラムが行われているのかを明らかにする必要がある。例えばスノーデンリークによれば、バハマ国内においてはアメリカ政府が全ての電話の会話を録音しているとされている。メタデータのみならず、通信内容まで 30 日分ほど録音して、保存している。アフガニスタンなど合わせて５カ国ほど同様の監視プログラムがあるとされている。これは非常に深刻な人権侵害だ。中期

[17] 米国自由法は NSA による電話のメタデータの収集にあたり、一定の嫌疑を要件とする外国諜報活動監視法（FISC）に基づく連邦裁判所の命令を要求するようになった。

的にはデジタル時代のプライバシーの問題として取り組んでいきたい。

４．プライバシーと国家安全保障のバランス

プライバシーと国家安全保障の的確なバランスをどう考えるか。二つの視点があると考えている。

一つは、アメリカ合衆国憲法修正４条の視点。監視は嫌疑ある者に限定し、一般市民を対象としてはならないというものである。

もう一つは人権論。自由権規約 17 条[18]を根拠として、監視は適正な範囲に限られるべきというものである。大量監視は政府にとって魅力的だが、効果がない。スノーデンリーク以降、政府の二つのグループが大量監視を調査した[19]が、大量監視が対象を限定した監視（ターゲット監視）捜査よりも効果的だという証拠は一つも報告されていない。我々はターゲット監視でなければならないと考えている。

ご承知のとおり、アメリカにおける自由権規約の位置付けは複雑だ。政府は、条約への署名を認めながら、国内的な法的拘束力を認めていない。自由権規約 17 条はアメリカ国外において実施される監視捜査に適用されないというのがアメリカ政府の立場だが、我々はこれに反対しているし、多くの国が反対している。もっとも、17 条の国内法的効力が疑問視されているため、これまでのところアメリカの裁判所でこの問題を問うことはしていない。

我々は訴訟、政策提言、ロビー活動など、様々な態様の活動を行っているが、アメリカの法解釈や法制度は他の国にも影響力があるので、自由権規約 17 条における通信内容の保護に関する原則論を海外における監視にも適用されるよう解釈すべきであると考えている。

もちろん、条約を米国内の裁判所で直接援用するためには議会の承認が必要であり、現時点では困難だが、他の手段、例えば IACHR（Inter-American Commission on Human Rights）[20]においてアメリカの自由権規約上の義務に関して意見を述べたり、他の国や国際機関の裁判所でイギリスの GCHQ[21]の監視プログラムに関して証言したりするなどの活動を行っている。

ナショナルセキュリティとプライバシーをめぐるもうひとつの旬な話題として暗号化に関するものがある。そもそもナショナルセキュリティとプライバシーを対立構造と捉えるのは適切ではない。プライバシーを保護することがセキュリティを守ること

---

18 自由権規約（市民的及び政治的権利に関する国際規約）17 条

「１．何人も、その私生活、家族、住居若しくは通信に対して恣意的に若しくは不法に干渉され又は名誉及び信用を不法に攻撃されない。

２．すべての者は、１の干渉又は攻撃に対する法律の保護を受ける権利を有する。」

19 PCLOB（Privacy and Civil Liberties Oversight Board、プライバシーと市民権監視委員会）と NSA の OIG（Office of Inspector General、査察官事務所）の２つの組織のことを指すものと思われる。

20 OAS（Organization of American States; 中南米の３５の国からなる組織）における人権の推進と擁護を目的とする機関。

21 The Government Communications Headquarters のこと。イギリスの NSA と呼ばれる。

になる。この視点は暗号化において顕著である。消費者がどのような暗号を使えるべきかについて、プライバシー対監視の問題ではなく、セキュリティとセキュリティの枠組みで考えるべき問題である。

多くのテクノロジーカンパニーも消費者は強力な暗号化手段を手にするべきであるとする考えをサポートしている。暗号化は政治的な言論の自由、特に抑圧的な国家で反政府的な意見を表明する際にはとりわけ重要である[22]。

政府によるビッグデータの利用も重要な課題だ。シリコンバレーがビックデータの効果的な利用法を客観的に明らかにして、ユーザーの利便性を示している。民間会社が利用するテクノロジーを政府が利用できないことを疑問視する向きもあるだろう。しかし、歴史を踏まえるならば、政府を信用してこのような権限を全面的に与えてはいけない。

5．政府のテロ活動に関する監視をいかに統制するか

情報機関内部における統制、情報機関の外部だが政府内部の統制、そして議会や裁判所を通した統制のいずれも必要である。ただ、政府内部や議会による統制は、それだけでは効果がない。それがスノーデンリークで得られた教訓だ。

1970 年代、議会は FISA を制定し、議会による監視や内部統制を要求した。それから 25 年間は、監視対象が絞られていたこともあり、この枠組みがうまく機能していた。2001 年に大量収集が始まって、従前の内部統制がうまく機能しなくなった。唯一独立した統治機構である裁判所の監督が重要であることを強く裏付けている。

ただ、裁判所だけでは十分ではない。市民による監督が重要だ。透明性を高めることで、市民に情報を提供し監督させるべきだ。もちろん、どの情報を公にし、秘密にするか、その線引きは非常に難しいが、透明性を高めることは政府機関の利害にも一致する。スノーデンリークを経て市民の信用が失われ、NSA は危機的な状況にあると思うが、近年は監視プログラムの概要に関し多くの情報を公開するようになってきた。

ナショナルセキュリティの問題に関し、目標を設定して戦略を立てることは、全ての政府機関が関係するうえ、一般市民の理解とサポートを得る努力も必要となるため、数年に及ぶ作業となる。

今回の大統領選挙のように、政府や候補者が恐怖をあおる発言をする際、現状よりも強力な政策を打ち出さなければ安全が確保できないといった「神話」を持ち出すことがある。

機密指定に関しては、不必要に多くの情報が機密指定されることで、民主主義、市民に対する説明責任がうまく機能しなくなるという問題がある。我々は裁判で不要な情報の機密化と闘っている。勝てることもあれば、負けることもある。

アメリカの裁判所は、機密指定された情報の開示を躊躇しがちである。インカメラで情報を見られる点は大きな違いかもしれないが、裁判所が行政府の意見を尊重する

22　政府が監視捜査のために暗号通信の脆弱性を放置したり、バックドア（利用者に気づかれないうちに遠隔操作で暗号解読ができるソフトウェア）を設けたりすれば、世界全体の通信におけるセキュリティレベルを下げ、ひいてはサイバーハックなどナショナルセキュリティ上の危機をもたらすとされている。ブルース・シュナイアー『超監視社会』（草思社）など。

ことはある。９．１１から時間が経ちそのインパクトが薄れるほど、裁判所が独立した監督機能を果たす可能性は高くなるとは思うが、まだそこまで行っていない。長期的な目標としては米国情報公開法（FOIA）をもっと強化すべきと考えている。いくつかの裁判で勝利してはいるものの、期待するほどではない。苦労している分野だ。

ウィキリークスが数年前に、何十万というアメリカの国務省が利用するファイバーケーブルについてリークしたことがある。そのうちあるケーブルが特定の人権問題（ターゲットキリング〔対象者を定めて行う政府による殺害〕や拷問など）と関係があることがわかった。リークにより存在が公になったにもかかわらず、米国政府は機密性を強硬に主張したので、FOIA に基づき正式に開示請求をした。訴訟において、米国政府は真正な情報でないためウィキリークスの情報を我々（原告側）が利用することは許されないと主張し、この主張が認められたため、我々は敗訴した。

政府は訴訟においてリーク情報を真正な情報と認めない。我々はメディアを通じてこの主張が論外であることを訴えている。市民がどう見るかが重要だ。市民が政府の説明に懐疑的になることで、裁判所の立場も変わることを期待している。いかに根深い問題があるかについて、一般市民の意識を高めたい。

６．ディスカバリー制度等で得られる情報について

情報公開に関して、FOIA 訴訟とは別に訴訟におけるディスカバリー制度（米国の訴訟法上認めれる証拠開示制度）の利用がある。FOIA よりも機密情報にアクセスできる可能性は高いが、そこで得られた情報を訴訟外で活用できるとは限らない。例えば、訴訟を通じてグアンタナモの被抑留者に関する情報を得たが、それを公にすることはできない。機密情報を理由に訴訟でも開示できないとして拒まれるものもある。

ACLU は、12 年にわたり拷問に関する情報の開示を求めている。CIA を相手に初めて拷問に関する説明を求めた訴訟で、先日判事が訴訟を進める決定を出した[23]。その背景には、多くの情報について機密指定が解除されたことがある。ただ、政府は、機密情報を開示することなく訴訟を進めると主張しており、さらなる機密情報の開示は期待できない。

政府はあらゆる拷問に関する訴訟などで State Secret Doctrine という原則を有効に活用している。これは、「この訴訟で原告が勝訴するためには国家機密の開示が必要だが、安全保障が害されるためそれは出せないから、この訴訟は却下されなければならない」とする抗弁である。非常に問題がある法理であり、訴訟を早々に打ち切られてしまう。

７．ナショナルセキュリティ分野の情報公開に向けた努力

基本的には情報公開訴訟を利用するが、他の手続もある。議会に対する政策提言などあらゆる手段を活用している。CIA のレポートなど何か月も働きかけた結果、開示されたものもある。

---

[23] CIA の拷問プログラムを開発した心理学者らを被告とする Salim v. mitchell のこと。2017 年８月、勝訴的和解が成立した。

ノーフライリストの訴訟も同様だ。この訴訟はデュープロセス（適正手続）条項違反を主張の骨子に据えている。憲法上保障された旅行する権利について、理由を知らされることなく、また、リストに含められた理由を有効に争う手段を与えられることなく奪われてはならないというものである。

従前、政府は機密情報と主張していたが、裁判所が違憲と判断し、政府の手続が改定された。ただ、我々は改定された手続も違憲と考えており、現在も引き続き係争中である。

８．警察による監視捜査

警察が新たな技術を用いてどのような監視捜査を実施しているか。その一つとしてロケーショントラッキング（居場所の追跡）がある。

EZPASS[24]、自動化したライセンスプレートリーダー（＝ナンバー読み取り機）、Spot on Location Tracking（携帯基地局から発信される電波の追跡）、ＧＰＳなどの技術を転用し、警察は車の移動を追跡して、人々のロケーション情報に関する大量のデータを収集している。

ACLU 自身が直接にクライアントの代理人として訴訟活動をすることもあるが、多くの場合は、刑事事件において、憲法上の問題、例えば合衆国憲法修正４条違反を根拠とする違法収集証拠の排除の主張など、法廷に提出する意見書（Amicus Brief）という形で助力して、成果を上げている。

監視に関する訴訟はスタンディング（当事者適格）を確立するのが難しい。多くの監視技術は機密情報とされている。またそもそも秘密裏に監視されているため、トラッキングされている事実を立証すること自体が難しい。刑事事件ではこの問題を回避できる。刑事事件の被告人であれば当事者適格はクリアできる。トラッキングによる証拠が提出されるので立証も問題ない。彼らに助力することで有効に問題提起できる側面がある。

調査報告も行っている。ナンバー読み取り機について、なぜこのような装置が実際に使われているのか、データベースの情報保管規定はどうなっているか、アクセス権者や手続はどうなっているか、連邦政府、州政府、都市など全米の情報を調査して公表したところ、マスメディアが大きく取り上げて、警察の利用を制限する州レベルでの立法措置に繋がった。嫌疑がない人についても情報を一律で保管し、数か月後に検索して過去にどこにいたかがわかるというのは、プライバシーの観点からは問題がある。そのため、情報の保管期間を７日や１か月などに制限する立法が出来ている。

９．EZPASS について

2014 年、NY 州と NY 市に、EZPASS の読み取り機がどこに設置されているかを問い合わせたところ、マンハッタンのほとんどの交差点に設置されていることが判明した。高速道路の料金徴収のためのシステムが、全く関係のないところに設置され、交差点を通る全ての車の位置情報を集めているということになる。この問題を報道機関

[24] 日本における ETC のようなシステム。高速道路の利用を記録し料金所を自動で通過できる。

に公表して、かなりの関心を集めた。

EZPASS の問題を争うことは携帯電話のトラッキングほど簡単ではない。ナンバー読み取りも EZPASS も、公道で自発的に情報を発信していると考えられるため、合衆国憲法修正４条の問題として主張しても勝訴しにくいためだ。

ただ、場合によっては、州政府の情報管理規定の問題としてとりあげられることもある。例えばバージニア州では、特定の目的がなければ州及び地元警察が読み取り機のネットワークにアクセスして情報を収集したり保管したりしてはいけないと州法で規定している。特定の容疑者や盗難車に関する情報であれば EZPASS を用いて情報収集することも許されるかもしれないが、あらゆる情報を集めていつか役に立つだろうという運用は州の法律に違反すると考え、ACLU の協力組織が提訴している。

法的な異議申立てはこの事件くらいで、まだ違憲と判断されたものはない。ただ、技術にもよるし、このような装置をもっと使うようになると、ＮＹ州のあらゆる交差点で、いつ、だれがそこを通っているかという情報を集めれば、それだけでも違憲だという主張ができるかもしれない。詳細かつ膨大な情報が収集されるようになれば、法的な異議申立ても可能かもしれない。

10. 新しい監視技術についての取り組み

NYPD のドメイン・アウェアネス・システム（Domain Awareness System）[25]は新たなテクノロジーの一つだ。将来的に、多くの市民がこのシステムで追跡される可能性があり、非常に懸念している。高度化した技術が法律のはるか先を進んでいる例である。

ほかに、顔認識及びビデオサーベイランス（ビデオによる監視）の仕事も手がけているが、これらの問題は立法により短期的に解決したいと考えている。現時点で訴訟の提起は考えていない。顔認識に関して、政府の建物の入口で容疑者を認識するために利用される場合は問題ないが、あらゆる場面で全ての人が認証されデータベースを作られるとすれば大きな問題である。

利用目的を制限し、収集された情報の保管期限、使用期限を限定する州もある。ロケーションデータベースは、それがどのような技術によるものであっても、たとえ警察が独自に作成したデータベースであっても、捜査に使う際には裁判所の承認を求めるべきである。

（質問）

日本にＮシステムがあると言われてから、実際に警察がこれを認めるまでかなりの期間がかかった。新しい技術について、たとえ捜査に利用していたとしても警察はこれを明らかにせずに、違う理由で発覚したとして逮捕する場合などが指摘されている。EZPASS についても同じ問題があるのではないかと思うが、どのような方法で新たな技術についての情報を得る働きかけをしているか。

---

[25] ニューヨーク市街に設置された多数の監視カメラ映像と、警察のテロリストデータベースとを照合させる仕組み。

（Alex 氏）

非常にいい質問で、私たちもいつもこのことで苦労している。警察が監視技術を利用する時期と、市民がこれを認識するまでの間にタイムラグがある。利用に気付いたときには既に別の強力な技術が使われていて、いたちごっこになってしまう。

一つの例として、携帯電話のトラッキングデバイス（追跡装置）である IMSC（International Mobile Subscribe Identity）の事案がある。警察が、携帯の基地局のごとく振る舞うデバイス（Cell Tower と呼ばれる小さなボックス）をパトカーの中に設置して、定期的に信号を発して、特定のシリアル番号（個々の携帯電話に割り振られている識別用の番号）が応答すると、どのアパートの部屋に当該携帯電話があるかを特定できるというものである。

警察が 20 年以上もこの技術を利用していることが明らかとなり、また携帯電話の技術の進歩とともにこの技術も進歩しているが、市民はこの技術について４、５年前まで全く知らなかった。ここ２年でかなり情報が開示され、いくつかの裁判所で検討され、州政府でこれを規制しようという動きが出てきた。

この技術が発覚することとなった刑事事件を紹介しよう。アリゾナ州にいる男性が、いつもは森の中に住んでいて、たまに都市に出てきたときにラップトップＰＣを利用して、死んだ人の SSN（社会保障番号）を用いて税の詐欺行為をしていた事案があった。彼はセキュリティにとても注意を払っており、自分をトラッキングするのは不可能だと考えていた。ホテルに偽名でチェックインしていたところ警察が部屋に来て逮捕された。彼は裁判を通じて、警察は秘密のデバイスを利用して自分が携帯電話のエアカードにタッチした情報を感知したに違いないと弁護士に訴えたが、弁護士はそんなことはあり得ないと言って取り合わなかった。彼は弁護士を４人も変えたがどの弁護士もこれを信用しなかったため、自分で弁護することになった。彼は巧みに弁護して、ついに予備審理のディスカバリー手続でこの技術についての情報を開示させることに成功した。

こうして彼はつかんだ証拠を元に ACLU に援助を求め、我々が裁判に関与することとなった。警察は様々な弁明を試みた。この技術を実際に利用する意図はなかったとか、携帯電話会社との合意に基づき携帯電話の場所を特定するためだけに使ったとか、秘密の情報源の情報で被告人の潜伏先が分かったなどと説明したが、次第にこの技術が組織的に利用されていることが明らかになり、１か月ほど前の初めての控訴裁判所（メリーランド州の裁判所）で有利な判決が出された。裁判所も警察の秘密主義ぶりに憤っており、このような技術を用いる際には令状を得なければならない、令状審査においてどのような技術を使用し、それがプライバシーにどのような影響があるかを説明しなければならないと述べた。この技術は容疑者の電話のみならず、あらゆる携帯電話を識別することができるうえ、当該地域の全員に網をかけることができるもので、このことを裁判官すら全く知らなかったのである。

11. ロケーションプライバシーに関する議論

ロケーションプライバシー（居場所に関するプライバシー）に関して、二つの理論がある。

一つは、ある人がプライベートスペース（オフィスや家）にいる場合。この場合、議論は簡単である。最高裁判例により、家の中で携帯電話を使っても、プライバシーは守られるべきとされている。

もう一つが公共の場所にいる場合。これは原則としてプライバシーの保護が及ばない。ただ、長期的に追跡された場合、公共の場所でも問題となるとされる。これが2012 年の Jones 判決であるが、この事件では意見が分かれて、多数意見はＧＰＳデバイスを設置する際にトレスパス（不法侵入）があったことを違法の理由としている。他方、多数意見のうちの１人の判事と少数意見を述べた４人の判事は、長期的に特定の人物の詳細な情報を集めるのはプライバシーの合理的な期待に反すると述べた。これはモザイク理論と呼ばれている。特定の人に関するあらゆる情報を細切れに集めると、結局は人生すべてに関する情報を集めることとなり、プライバシーの侵害になるという理論である。我々はこちらの考え方が正しいと考えており、実際にいくつかの訴訟でもこの理論を主張して成功を収めている。

なお、携帯電話のトラッキングに関しては、捜査を実行する時点で対象者が自宅にいる可能性がある以上、セーフガードとして事前に令状を取得しなければならないという主張が、モザイク理論に寄らずとも可能である。

EZPASS やナンバー読み取り機の場合、車は家の中に入らないためこのような立論はできない。一定期間の情報を集めることでプライバシーの期待・権利が侵害されると主張しているが、これを認める裁判所もあれば、認めない裁判所もあり、様々だ。

合衆国憲法修正４条は、憲法制定以来、家庭内のプライバシーに関してはコモンロー的に強力に保護する。自宅は城であり、政府が侵入することは許されない。自宅は最もプライベートであり、保護されるべきであると裁判所は述べてきた。

しかし、家の外に出ても、あらゆる情報をすべて集められ政府から監視されるとなれば、顔認証であれ、携帯電話や他のトラッキングなどの他の技術であれ、プライバシーを侵害するのではないか。サーベイランス・ドローンという、小型の強力なカメラを搭載したドローンもある。都市の上空から誰がどこを歩いているかを詳細に捉えることができる。このような機械の利用も同じ問題があると考えている。

第三者提供の法理は合衆国憲法修正４条に関するもので、情報を第三者に提供した場合には、当該第三者だけでなく、警察にも提供したものと考えてよいから、令状なしに情報を取得しても問題はないというものである。

この法理は、例えば私が「誰かを殺したい」と誰かに話し、それを聞いた人が政府に通報するという場面であれば妥当するかもしれないが、携帯や電子メールによるプライベートな情報が増えている現代においては非現実的な法理である。携帯電話のトラッキング情報は数年にわたって保管して、のちになって当時の場所がわかるなどというのはロケーションプライバシーを脅かすものだ。第三者提供の法理の見直しの問題提起として適していると考えている。

その他現在係争中のものとして、病院の処方箋のモニタリングシステムがある。規

制薬物が含まれる鎮痛剤やテストステロン、ステロイド、睡眠薬などに関して、薬局で購入記録を残さなければならない。警察はこのデータベースが大好きで、しばしば利用している。医者に行くときには自分の病気に関する情報を開示し、薬局では処方箋とともに薬に関する情報を開示する。州の法律で、薬局は州のデータベースに登録しなければならないとされる。この制度を争うものとしてオレゴン州で裁判が係属している。

12. アメリカ自由人権協会の弁護士の仕事やキャリアについて

全米の多くの訴訟で ACLU の弁護士が関わっている。刑事被告人の弁護人が ACLU にアクセスしてくることもあれば、新聞記事からスピーチ・プライバシーに大きく関わる事案と考えて我々の方からコンタクトをとることもある。

例えば、リーガルリサーチのデータベースで「United States v. Jones」と検索すると、この判例の射程を争点とする訴訟を新たに把握できる。その訴訟が控訴審まで進み興味深いと ACLU が考えれば、自らアミカスブリーフ[26]を申請する場合もある。裁判所から連絡があることも稀だがある。まだ刑事弁護人も選任されていないが、新たな技術による監視が問題となっており、判事が問題点を整理したいときなど、一方的な裁判所の命令により裁判所宛の主張書面を提出するよう依頼されることがある。

裁判所の依頼があった場合には費用はもらわない。我々が訴訟提起した場合には訴訟費用を受け取るときがあるが、提出書面の作成に関する費用はでない。資金は他から得られるものもいろいろあり、弁護士費用のみに頼る必要はない。なお ACLU のスタッフは給与制で働いており、政策提言の意見書や自らの訴訟も担当している。

仕事内容はプロジェクトによって異なる。直接クライアントを代弁する件もあるが、監視に関連した仕事が多い部署では政策提言的な書面作成が多い。スタンディング（当事者適格）のあるクライアントがなかなか見つからないというのもある。他に、ワシントンＤＣでの立法府のロビー活動として、議会での証言や、FOIA（情報公開）の請求も常にある。

他のプロジェクトの場合には、クライアントを直接代弁する案件が圧倒的に多い部門もある。女性の権利やジェンダーのプロジェクトなどがそうだ。どの事案に関わるかは、組織全体の優先順位や、プロジェクトレビューでの優先順位による。

その優先順位の中で、個々の弁護士がどの事案を取り上げるかを決めるが、複数の上司の承認が必要となる。とりわけ新たな問題が含まれる事案であれば上司の判断の比重が大きくなることもあるが、過去にすでに７，８回書面を裁判所に出していて、また別の裁判所で同じような書面を出せばよいということであれば、改めての決裁は必要ない。

キャリアパスは様々で、ロースクールを卒業後一貫して ACLU で働く者もいる。一年半前にリタイアした弁護士は 40 年間所属していた。素晴らしい実績を残した。管理職であるディレクターになることなく、ずっと現場でやりがいある仕事をしていた。

[26] 訴訟当事者以外の第三者が裁判所に意見書（アミカスブリーフ）を提出して助言を行う制度。米国ではアミカスブリーフに基づき歴史的な判決がなされることもある。

５年、10 年だけここにいて、別の州のリーガルディレクターになったり、民間の法律事務所と行き来する者もいる。ここを辞めて別の NGO で働くという人も多い。ACLU ではプライバシー問題に関わり、その後教育関係のスタートアップの技術系の会社に転職した弁護士もいる。ACLU でこのようなキャリアパスは少ないが、ワシントン DC の Center for Democracy in Technology という組織では、デジタルプライバシーの案件を多く扱っていることもあり、技術系の会社と行き来する弁護士が少なくない。

ACLU から政府に転職する人もいる。司法省や公民権の部門、教育の部門など。検察官は稀。共和党政権時より民主党政権時のほうが多い。より馴染むということだろう。

第 3 部

Brennan Center for Justice (BCJ)

BRENNAN CENTER FOR JUSTICE
TWENTY YEARS
at New York University School of Law

（BCJ ホームページより転載）

（BCJ 事務所にて）

１．BCJ について

BCJ は、民主主義と公平な正義というアメリカの二大理想の実現・向上を目指して、法律及び政策を研究する無党派団体である。活動範囲は、選挙権から財政再建に関する運動、大量投獄からテロリズムとの闘いにおける憲法的な保障まで多岐にわたる。シンクタンクパート、弁護士パート、通信ハブに関する最前線パートなどに分かれている。それぞれ精密な調査に基づき革新的な政策を生み出している。議会や州、裁判所における多数意見に対して戦いを続けている（ホームページ：http://www.brennancenter.org/）。

Ⅰ．ヒアリング先

・Michael German

BCJ 研究員兼所属弁護士。対テロ活動における市民の人権や基本的自由の確保が研究テーマ。自由と国家安全保障プログラム担当。ウェイクフォレスト大学哲学科卒、ノースウエスタン大学ロースクール修了。FBI の特別捜査官として 16 年間、対テロ捜査活動に従事した後、ナショナルディフェンス大学の准教授として法執行機関とテロリズムについて研究。アメリカ自由人権協会のワシントン事務所で国家安全保障とプライバシー部門担当弁護士などを歴任。

・Michael Price

BCJ 所属弁護士。自由と国家安全保障プログラム担当。コロンビア大学政治学科中東・アジア言語文化学科卒、ニューヨーク大学ロースクール修了。刑事弁護人協会(NACDL)にてグアンタナモ被収容者の弁護のための法的支援のとりまとめを担うとともに、プライバシー、電子的監視や政府の機密指定などに関して訴訟、および市民に対する啓発活動を行っていた。ニューヨーク大学人権クリニックで、アメリカが海外に置く秘密軍事施設ブラックサイトで CIA に拘束され拷問を受けたイエメン人の代理人を務めた経験などをもつ。

Ⅱ．BCJ の組織・運営等について

BCJ は、民主主義プログラム、司法プログラム、自由と国家安全保障プログラムなどのプログラムに分かれてそれぞれが独立して研究に従事している。ニューヨークとワシントンにオフィスがあり、スタッフは総勢１００人ほど。個人のクライアントの訴訟等を扱うことはあまりなく、公共政策に関する調査研究が主な仕事である。運営費用は個人からの寄付や補助金で賄っている。BCJ のオフィスは NYU 内の建物にあり、当初は NYU のロースクールの一部として資金提供を受けていたが、現在は完全に独立している。とはいえ NYU ロースクールと BCJ とは、電子メールアドレスの共有、図書館の利用、法学部生のインターン、リサーチアシスタントの受け入れなどの点で現在も協働している。

Ⅲ．自由と国家安全保障プログラムについて

自由と国家安全保障プログラムには、「政府と市民との間の適正な情報の流通を図

る」、「テロの脅威とテロ被疑者に対する効果的な方法論を確立する」、「監督と透明性の適正なメカニズムを守る」という三つの行動指針がある。

これらの行動指針に従って、市民や省庁に対する啓発活動、様々な裁判例でのアミカスブリーフの提出、議員やそのスタッフへの情報提供、リサーチを行った上での論文の発表、メディアへの働きかけ、必要に応じて訴訟などありとあらゆる手中にあるツールを使って活動している。

リサーチのテーマやトピックは、基本的に各々のスタッフが考えて、お互いに協力関係を築きながら取り扱っており、例外的に新聞に意見広告を出す場合などは組織全体の承認を得た上で行う。

現在は議会の監督機能、すなわち 1970 年代には議会の委員会で諜報活動の指針やその実践に対する評価を行うものがあったが、それが依然として機能しているかという点について研究している。ガイドライン自体が 40 年以上経ってしまっているし、アメリカ同時多発テロ事件以降、そのガイドライン自体が排除されるという現象が起きており、スノーデンによる NSA の大量情報収集の暴露などの問題が生じている。昨今、政府は Countering Violent Extremism というコンセプトに基づいて “プリテロリスト”という概念を立ち上げて対テロ対策を行っているが、その認定方法にはなんらの科学的根拠もなく、偏見に基づいてテロリストではない人間に怒りを与えてテロリスト化させてしまうという問題もある。

過激派によるテロの防止のための政府の活動について、情報公開法を利用して情報を入手して論文を書いたり、NYPD のムスリムに対する監視・弾圧問題に関するアミカスブリーフを提出したり、新たなテクノロジーを使用した監視活動の調査やこのような監視活動の透明性に関する研究などに従事している。

２．政府からの情報の開示について

情報公開法などを利用して政府からの情報の取得を試みることが多い。すぐに情報が公開されることもあれば、何度も繰り返してようやく政府から情報が公開されることもある。当然ながら政府にとって都合が悪い情報であれば、情報の入手には時間がかかる。その公開が十分ではないときには更なる段階、すなわち訴訟を検討せざるを得ない。訴訟を起こすぞと脅せば済む場合もあるし、実際に訴訟を提起せざるを得ないこともある。

現在、暴力過激主義への対抗策に関する情報の公開を求めているが、2014 年 12 月ころに情報公開請求をして、１年半かかってようやく一部が開示されるようになった。省庁によって情報公開請求に対する対応は異なる。州や地方自治体の警察署は割と簡単に情報を出してくれるが、国家レベル、特に NSA や CIA は、国家安全保障に関する機密であるとして情報をなかなか出してくれない。

連邦政府がよく使う理由づけは「グローマー拒否」である。冷戦時代にグローマーという核潜水艦が存在したが、これについて情報公開請求をした場合、政府としてはこれに関する情報があるかないか応答をすることだけでテクノロジーの存否がロシアに知られてしまうから、政府は応答自体を拒否することが許されるとする古い裁判例に基づく主張である。「グローマー拒否」をされてしまうと訴訟で争うことも困難で

ある。ただ、判事によっては、インカメラ手続を通じてその情報のチェックを求める場合もある。

訴訟手続では、政府は公開を拒否する様々な理由を繰り出して訴訟を遅延させていく。先ほども述べたように、情報を公開させるためには訴訟で争うことを示唆して脅すか、実際に訴訟で争わなければ望む結果が得られないが、BCJ や ACLU、その他のグループはそれでもしつこく情報の公開を求め続けている。

3．監視捜査について

BCJ は、監視捜査の問題にも取り組んでいる。警察など捜査当局による情報収集の方法、例えば NYPD のムスリムコミュニティーに対する監視、FBI による暴力過激主義への対抗策について調査を進めている。特定の事案について調査結果に基づいて論文を発表したり、市民に対する啓発活動を行っている。

公衆の道路や建物における監視活動についてはプライバシーが及ばないとされている（第三者法理）。このルールが決められたのは電子技術がそれほど発達していない時代であった。現在は、電子技術、つまり電子メールや携帯電話に収められたデータなどが急速に発達しており、新たなルール作りが必要とされている。政府や市民団体を含め、皆が模索しているところである。

GPS による追跡の問題も生じているし、携帯電話の追跡による監視という問題もカリフォルニアで起きている。第三者法理については、高裁レベルの裁判所で意見の相違があるため、ここ１、２年ぐらいで最高裁がなんらかの結論を出すと考えている。最高裁がこの法理を変更してくれるものと信じているが、どのように変更するのかは不明である。

4．捜査・諜報活動とプライバシー、現状の手法が抱える問題

国家安全保障に関する諜報活動についてのルールは 1970 年代に制定されたものであり、海外の情報の傍受は政府の思いどおりになっている。例えば、今、私がこの部屋から電子メールを送った場合、一旦カナダにあるサーバーを経由すると政府が自由に傍受できてしまうことになる。政府は米国市民のプライバシーは保護していると述べていたが、スノーデンの暴露によって、国家安全保障とは関係のない貿易の情報やその他の情報を NSA が収集していたことが明らかになった。

昨今、ISIS などのテロリストの問題が生じており、それがあまりにセンセーショナルなことに市民の目が奪われており、政府はそれを利用して捜査・諜報活動とプライバシーの問題の説明責任を免れている。非常に残念である。

国家安全保障とプライバシーの両立という問題はアメリカでもよく議論される課題である。私の FBI での経験では、国家安全保障のためにテロリストではない人たちの情報を集めるというのは、砂漠の中で針を一本見つけるような無駄な努力であり、テロリスト側からすればいくらでも抜け穴がある。テロリストグループと今日関わっていないからといって、明日も関わらないという保証はないという理由で、大量の情報を集めるというモデル自体が不備に満ちているといわざるを得ない。結局、大量の情報を集めすぎて実効性がなくなってしまっている。あるテロ事件を起こした被疑者は、

テロリストとして監視対象となっていたにもかかわらず、３回もアメリカ出入国を繰り返し、ロシアとも関わっていたのに見逃されてしまってテロ事件を起こされてしまった。

アメリカ同時多発テロ事件のハイジャック犯人についても、情報は十分にあったにもかかわらず、テロを防げなかった。つまり、情報の収集活動も必要だが、その情報をどうやって管理するか、そして無罪の人をどのように見極めるかというところに問題があることを認識しなければならない。

これはアメリカだけの問題ではない。ベルギーやフランスなどでもテロ事件が起きるたびに、捜査当局はその犯人の情報を知っていた、トルコでも同様の事件を起こしていたという問題が生じる。捜査・諜報活動とプライバシー、現在の手法が抱える問題というのは世界共通の問題である。

第 4 部

Professor Stephen Schulhofer
(シュルホーファー教授)

１．シュルホーファー教授のプロフィール

ニューヨーク大学法学部教授。専門は刑法。プリンストン大学卒業、ハーバード大学ロースクール修了。ハーバードローレビューの編集者となり、連邦最高裁判事ヒューゴ・ブラックの調査官を経験。刑事罰に関する研究者として研究者のキャリアを歩み始め、1980 年代には司法取引によることなく非陪審審理の適正を図る可能性についての分析を行い、その後、警察による取調べにおけるミランダ・ルール[27]に関する研究やガイドラインの提案などを行う。1990 年代半ばからミランダ・ルールによる自白への影響や、刑事司法行政における性的虐待の取り扱いなどの研究を行う。著作に”The Enemy Within：Intelligence Gathering, Law Enforcement and Civil Liberties in the Wake of September 11”など（ホームページ：https://its.law.nyu.edu/facultyprofiles/index.cfm?fuseaction=profile.overview&personid=20270）。

２．FISC・FISA を利用した活動の拡大と濫用

FISC（Foreign Intelligence Surveillance Court: 外国諜報活動監視裁判所）は、国家の安全を保障するため、外国諜報活動に対する物理的な捜索および電子機器を使用した監視による情報の収集の手続について定めたアメリカ合衆国の法律 FISA（Foreign Intelligence Surveillance Act・外国諜報活動監視法）に基づいて設置された裁判所である。

国家安全保障と関係のない一般的な犯罪（薬物事件や殺人事件等）については FISC・FISA を利用しての電子機器を使用した監視活動は出来ないとされていた。しかし、2001 年 9 月 11 日のアメリカ同時多発テロ事件以降、FISC はその機能や活動を拡大し、ある特定の個人をターゲットとしてこの個人に対する監視のための令状請求及びこの許否を判断するという基本的な活動にとどまらず、プログラム的な意思決定に基づく監視活動（一定の条件を定めて、その条件に該当する人々全員をターゲットにする監視活動）を行うようになるなど、合法的な基礎を欠く活動を行うようになってきた。

特に、アメリカ同時多発テロ事件以降の 15 年間のうち 14 年間は合法的な基礎を欠く活動が行われ、FISC の活動が性質上、秘密にされなければならないという点が濫用されてしまっていた。

３．FISC・FISA の活動が秘密にされることの是非

FISC の活動は、その性質上、秘密にされなければならない。例えば、テロリストがよく使うテクニックとして、全ての電話を 10 秒以内で切るという手法がある。ある個人が全ての電話を 10 秒以内で切っていれば、その個人にはテロリストの疑いが生じる。このような場合、FISC の判断を仰いで、捜査機関は当該個人の電話を盗聴して監視することになるが、捜査機関がその特定の個人の監視を行っているという事実は、当然ながら秘密にされなければならない。

---

[27] アメリカの刑事手続において連邦最高裁判例法上確立された捜査上のルール。捜査機関が被疑者に対し、黙秘権・弁護人依頼権などについて遺漏なく告知しなければ、被疑者の供述は公判で証拠として用いることができないとするもの。ミランダ警告、ミランダ準則ともいわれる。

このように、特定の個人をターゲットとする監視活動は秘密にされなければならない。同様に、プログラム的な意思決定に基づく監視活動が秘密にされなければならない場合もある。

しかし、性質上、秘密にされなければならないという点が濫用されてしまっているというのは重大な問題であり、私個人は、FISC の活動はもっと開示されなければならず、全体として透明性を高める必要があると考えている。

4．捜査機関による監視活動が正当か不当かを分けることができるのか

監視活動が正当か不当かを分けることができるのか。シンプルな答えはない。

エドワード・スノーデンは様々なことを暴露したが、そのうち、NSA（国家安全保障局）がメタデータを大量収集していたという事実に着目して考えてみたい。すなわち、NSA は、FISC の判断を仰いで、メタデータの大量収集を行っていたが、その根拠となった法律・条文は、愛国者法（Patriot ACT）215 条である。FISA に基づく監視活動には、監視の対象と国家安全保障との間に関連性が認められなければならない。当然ながら、ここまでは関連するがここからは関連しないという閾値が存在するはずだが、政府は、全てのメタデータが国家安全保障と関連すると強弁していた。私自身、この政府の主張は条文の解釈を誤ったものであると考えていたが、それ以降、何件かの訴訟がなされ、この政府の主張は条文の解釈を誤ったものであるとの裁判所による判断がなされた。

他方、監視活動が正当か不当かという点は、条文の解釈に基づき区別する違法・適法の点から判断されるべきではなく、その監視活動が公衆に開示されるべきであったか否かという点から判断されるべきである。そして、上記の NSA によるメタデータの大量収集は、（開示に伴う監視捜査の弊害がないため）公衆に開示されるべきであったことは明らかである。では、なぜ政府が公衆に開示しなかったかというと、それは、政府自身が、全てのメタデータが国家安全保障と関連するものであるとの主張の正当性を弁護できなかったからである。

政府が透明性を確保しなかったが故に、誤った意思決定が行われた、これが監視活動を秘密にすることが不当であるといえる一例である。

監視活動が特定の個人をターゲットとするか、プログラム的な意思決定に基づくかにより、透明性の程度が同じであっても正当か不当かの判断は異なる。特定の個人をターゲットとして監視活動を行っている場合、その監視活動については正当に秘密にすることができる。他方、プログラム的な意思決定に基づいて監視活動を秘密にすることは、一部を除いて不当である。プログラム的な意思決定の条件（例えば 10 秒以内に全ての電話を切っている場合には、当該個人を監視対象とする等）は、これが公になるとテロリストが抜け穴を作って乗り越えてしまうので、この条件を秘密にすることは正当である。他方、メタデータの大量収集あるいは通信内容の収集を行うとき、その収集の方法については秘密にすることは正当だが、その大量収集を行っているという事実自体を秘密にすることは不当である。その大量収集を行っているという事実を公衆に開示し、公衆から承認を受けた上で行うことはなんら問題ない。

５．監視活動を秘密にする手続

捜査機関による監視活動を秘密にする手続を検討するにあたり、第一に秘密にする対象の基準が問題となるが、一義的な答えはない。個別具体的に判断するしかない。

第二に、プログラム的な監視捜査について、ある特定の事項について秘密にすべきか否かについては、独立した機関が決定しなければならない。これは非常に重要な点である。例えば、大学の規則において、「教授は不当なことを一切してはならない。もし不当なことをした場合、それを報告するか否かはその教授自身が自ら決めなければならない」という規則があった場合、この規則は全く意味がなくなる。

アメリカには、「狐に鶏小屋を守らせてはならない」ということわざがあるが、自己の利益が最初に重視されてしまうので、機関と利害関係を有する関係者に意思決定をさせてはならない。したがって、特定の事項を秘密にすべきか否かは、NSA や CIA が決めてはならない。独立した評価機関が決めなければならない。アメリカの制度はこの点で失敗している。ある特定の事項を秘密にすべきか公衆に開示すべきかを、秘密にすることで利益を得る人たちが決めているからである。

独立した評価機関は国家寄りの判断をするかもしれないが、その評価機関があるというだけでも、権限を濫用しようとする人間が出てこなくなるという効果がある。

６．FISC の存在意義　～日本等の諸外国との比較～

（参加者からのコメント；日本においては、犯罪捜査のための通信傍受に関する法律が存在し、特別の判事ではなく、通常の判事が通信の傍受等の可否を審査するが、国家安全保障に関する通信の傍受等は審査の対象としていない。他方、国家安全保障に関する捜査は、アメリカのように独立した機関が存在するわけではなく、警察の一部門である公安警察が行っている。日本の公安警察が通信の傍受等を行っているのか、どのような捜査を行っているのか、どのようにテロリストの対策をしているのかという点は全くのブラックボックスである。他の国はどうか。）

フランスには盗聴を許可する法制度が存在するが、その手続はアメリカの法制度と比較してもやや緩やかである。それでも、フランスの国家安全保障を担っている対外治安総局（DGSE）は、手続を守らずに自由に活動を行っている。フランスの国民の反応は、「DGSE が盗聴等を行っているのはわかっているよ」というものである。

シークレットサービスは世界中で同様に、いずれかの監督に服すことなく自由に勝手なことを行っているが、自分たちは国家を守っているから正当化されると考えている。

FISC の監視は他の諸外国と比較して意味があるのかと問われると、なにも存在しないよりはましである。諸外国のシークレットサービスは盗聴に関する規制を全く無視して行っているというのが実情であり、アメリカの FISC は監視機関として存在しているという点で意味がある。

７．現行法制度の限界　～アメリカと日本の通信傍受に関する法律の規制の不十分性～

従前行われていたワイヤータッピング（電話盗聴）はコミュニケーション情報をリアルタイムで取得するものである。ただ、現在のコミュニケーション情報はほとんど

がサーバー上に保管されていて、リアルタイムでやり取りされているわけではない。捜査の目的はそのコミュニケーション情報を取得することだが、コミュニケーションの最中に取得する必要がないものが多い。現在のコミュニケーション情報はサーバーから取得できてしまうのである。

アメリカには盗聴法（Title Ⅲ・1968 年制定）が存在し、盗聴に対する強力な規制がなされている。盗聴法が制定された 1960 年代はコミュニケーション情報をリアルタイムで取得するという電話盗聴がプライバシーに対する大きな脅威だったからである。

しかし、今やほとんど電話による会話はなされていない。テキストメッセージや電子メールが主流であり、現在のプライバシーに対する大きな脅威は盗聴ではなく、保存されたコミュニケーション情報の取得である。先ほどは、NSA によるメタデータの収集の話をしたが、メタデータにはアドレス情報、発信先、受信先などが含まれている。これらの取得はプライバシーに対する脅威である。また、サーバーに保存されているコンテンツ（内容）の収集もプライバシーに対する脅威である。

私たちは、政府がメタデータやコンテンツに対してどの程度アクセスできるのかということを法的に規制しなければならないが、現行法の規制は十分ではない。日本の通信傍受法も 15 年前に制定された法制度なのであれば、現在のプライバシーに対する大きな脅威である保存されたコミュニケーション情報の取得への法的規制は十分ではないだろう。

8．アメリカの現行法制度の状況

アメリカには、ECPA（Electronic Communications Privacy Act: 電気通信プライバシー保護法）という、令状なしに電子メールの情報などの取得を禁止する法律が存在するが、同法によって十分なプライバシー保護がなされているとは言えない。そもそも ECPA が制定されたのは 1986 年であり、同法の保護対象は保存期間が 180 日に満たないもののみであった。今日、プライバシー情報は 180 日を超えて保存されることが通常であるから、この点において、ECPA は改正されなければならない。また、捜査機関等がどのような場合にこれらの保存されたデータの取得が可能かという点において、より具体的な制限を設ける必要もある。加えて、同法は、全ての保存されたデータ、例えばクラウドなどにも適用されるべきである。「A さんが B さんに送られたものでなければ、コミュニケーションとは言えないから、ECPA の適用を受けない」とするのは、捜査機関にコミュニケーション情報の取得の抜け穴を与えているようなものだからである。

9．現行法制度の改正に関するアメリカ議会の動き

コミュニケーションには三つの種類がある。一つ目は国内で完結するもの。二つ目は外国と外国の間で行われているもの。三つ目は部分的に外国が絡むものである。

例えば、私と妻がともに NY にいる場合、私と妻が電子メールのやりとりをするのは一つ目の国内と国内の間で行われているコミュニケーションである。私が NY にいて兄が外国にいる場合、私と兄が電子メールでコミュニケーションを行うのは、三つ

目の部分的に外国が絡むコミュニケーションである。このように、今日、グローバルなコミュニケーションが一般的になっている。ほとんどの法令は純粋に国内のみで完結するコミュニケーションのみを保護しようとしており、不十分となってきている。

2008 年に FISA が改正され、国内に限らず海外にいるアメリカ国民のコミュニケーション情報の取得についても FISC の令状審査を要件とするよう規制を強化したが、まだ抜け穴があり、市民的自由を求める団体からは不完全であるとの主張がなされていた。

アメリカ議会は基本的には情報の開示を積極的に求めている。まず、米国自由法（USA Freedom Act）により、議会は法的に重要な FISC の意見は公衆に開示しなければならないとした。例えば、愛国者法 215 条に関する FISC の意見は開示しなければならないとした。また、透明性に関連することとして、議会は FISC に対し、政府と対立する意見と突き合わせることを求めるようになった。従前、FISC の判事は政府の意見のみを聞いて判断を下していた。これを、CIA に籍を置いているような人間ではなく、市民的自由の実現に関する実務的な活動を行っているアメリカ自由人権協会の弁護士等の意見を突き合わせた上で議論しなければならないとした。

議員の中にはもっと情報の開示を進めるべきであると考えている人もいるが、そのように進めることが可能な状況には至っていない。なぜなら、政権側が公衆のプライバシー保護を強力にしすぎることに抵抗しており、従前の法改正等も妥協の産物でしかない。米国自由法も、政権側がここまでなら妥協するがこれ以上は妥協しないとして法制化されたものである。

10. 捜査機関及び諜報機関が取得した情報の管理・利用

日本では諜報活動と捜査活動のいずれも警察が担っているということだが、アメリカは諜報活動と捜査活動を担う機関は分かれている。それぞれの機関が得た情報については理論的には区別されることになっており、原則を言えば、情報の取得が国家安全保障のためのものか、あるいは刑事犯罪の解決のためかという点で区別をすることになる。

しかし、実際にはその境目は曖昧で、情報の区別は極めて難しい問題である。例えば、2004 年にスペインのマドリードで起きた 100 人以上が死亡した列車同時爆破テロ事件で、アメリカ人のメイフィールド氏という人物が事件に関与した可能性があるとして誤認逮捕されたことがあった。彼はそのまま起訴に向けて捜査を受けることとなったが、誰と共謀したのか、誰が爆弾を製造したのか、誰がその情報をもっていたのかといった事実の調査は、国家安全保障に関する諜報活動にも含まれうる事項であり、捜査活動と諜報活動とは重複する部分があることが分かるだろう。

他方で、捜査活動と諜報活動との間には、「壁」という問題もある。多くの人は、アメリカ同時多発テロ事件を防げなかった原因は、この「壁」、つまり、捜査活動と諜報活動という二つの領域間での情報交換ができなかったからだと考えている。

外国に対する諜報活動に関して言えば、諜報活動と捜査活動とをしっかりと区別することは必要である。具体的に言えば、外国に対する諜報活動として電話の盗聴をしていた際に、ある人物が浮気をしている妻を殺害しようとしているという情報を得た

としても、それは諜報活動とはなんら関係のない事実であるから、捜査活動に利用するということは許されるべきではない。他方で、対諜報活動や対テロ活動を行うときには、「壁」を超えた情報交換が必要にもなる。

このように、捜査活動と諜報活動とをどのように区別すべきか、これらの活動で得た情報をどのように管理・利用すべきかという点には常に問題がつきまとう。

11. データマイニングの問題　～連邦最高裁の展望～

今日ではデータマイニングが非常に話題に上がっているが、データマイニングはプライバシーに対する大きな脅威である。ヨーロッパではプライバシーの権利が厳格に尊重されているが、アメリカ合衆国憲法はプライバシー権について明文規定を持っておらず、プライバシーの権利に基づいてデータの保護を受けるという期待はできない状況にある。

例えば Google を例に挙げれば、私が検索した言葉、私が電子メールをした相手、その電子メールでなにを書いたかといったデータは全て、Google に渡ってしまっている。このようなデータを政府に取得されてしまうことは、プライバシーの権利を侵害する恐れがあり、合衆国憲法修正４条の問題となるが、連邦最高裁によって確定された第三者法理があり、プライバシーの権利侵害性が認められないかもしれない。

アメリカ合衆国憲法が制定されたのは 1787 年であり、その時代であれば、デスクの中に遺書、日記、信書などを入れておけばプライベートな生活を守ることができた。しかしながら、今日に至っては、ほとんどのコミュニケーションであってもインターネットサービスプロバイダー（ISP）を介さなければならない、それが現代の生活様式となっている。つまり、政府は、私たちの社会生活全てにアクセスすることができる状態になっている。合衆国憲法修正４条そのものを変えてしまうという方法もあるかもしれないが、憲法の条文を変更するには手続のハードルが非常に高いことに加え、少数者の権利を侵害する内容に変更されてしまうおそれもあることからすれば、合衆国憲法修正４条そのものを変えるというのは不可能だろう。最高裁はいずれ第三者法理を覆さなければならないであろう。

第 5 部

Adjunct Professor and Executive Director of the Center on Law and Security

Zachary K. Goldman

（ゴールドマン教授）

１．ゴールドマン教授のプロフィール

ロースクール卒業後、２年ほど財務省のファイナンシャルインテリジェンスのグループで仕事をした。ごく短期間だが日本に行ったこともある。その後、国防省の共同参謀長の最高幹部らの下で働いた。短期間、ＮＹの法律事務所で法律実務に従事した後、４年前に NYU に赴任した。

現在は、NYU ロースクールでナショナルセキュリティとサイバーセキュリティーについて教鞭をとっている。ナショナルセキュリティ、特にカウンターテロリズム・インテリジェンスに特化して研究している。インテリジェンスに関するヨーロッパと米国の比較研究に関する共著がある。

２．米国のインテリジェンスについて

アメリカの諜報制度はここ２年で変化を遂げた。一つは、ナショナルセキュリティとインテリジェンスの国内における課題。もう一つは、具体的なインテリジェンス活動の内容。全く二つの異なるカテゴリーで、緊張関係も異なる。国内におけるものとして、米国は以下のような課題に直面している。Ⅰ．インテリジェンス活動と伝統的な刑事事件の捜査活動の整合性、Ⅱ．データの収集とそのデータの使用の関係、すなわち収集に着目して規制するか、使用に着目して規制するか、Ⅲ．メタデータとコンテンツデータなど、異なるタイプのデータをどのように機密化するか、Ⅳ．政府と民間の関係の４つである。

Ⅰ．インテリジェンスと捜査（刑事法）

諜報活動としての情報収集と、刑事事件の捜査としての情報収集は基本となる概念が異なる。原則として、諜報活動は米国国外の外国人に対して行われる。米国憲法で各種権利が保障された米国人に対する活動ではない。他方で捜査活動は米国内におけるもので、とりわけ刑事裁判で用いる情報に関しては憲法上の権利が関連してくる。

近年、諜報活動で得た情報が捜査に役立つのであれば情報が共用されるべきだと考える人々が増えており、その具体化について議論されている。

しかし、法的規制があまりない中で収集された情報が捜査で使われることについては、アメリカ自由人権協会などが問題視している。

Ⅱ．情報の収集と利用

かつては、情報収集の局面で正当性を議論していた。一度適法に収集した情報はその後どのように利用してもよいと考えられてきた[28]。

しかし、現在はデータの意味合いが異なる。政府は様々なデータを常に収集できる状況にあり、広汎かつ膨大にデータを収集している。その後の利用の局面で規制をする必要が出てきており、いかに効果的に意味のある制約ができるかが課題にな

[28] 日本における同様の議論として、山本龍彦「監視捜査における情報取得行為の意味」法律時報 2015 年５月号 60 頁以下など

っている。具体的には、データ処理・保存（期間や態様）・分析（どのような種類の分析ができるか)、アクセス権者、共有など。データ量自体があまりにも増えているため、利用の局面においてより詳細な考慮が必要となっている。さらなる課題は、この意思決定を誰がすべきか、―裁判所か、議会か、行政か―、である。

諜報分野には三権が関与する。立法府が活動の最小化を試み、これを司法府が承認して、諜報部門が執行し、この活動を行政府と議会が監督する。完璧ではないが、権限分配として賢明な分配だと思う。

実際に最小化の手続内容がどうあるべきかについては、様々な意見があると思う。しかし、ルール自体の形と、そのルールに即して誰が当該組織の中で権限を持つべきかということは区別して考えられるべきである。

Ⅲ．データの種類ごとの規律、特にメタデータについて

1970 年代に連邦最高裁のいくつかの判例により第三者提供の法理が確立された。これは、銀行などの第三者に提供すると当該データに関するプライバシーの期待が失われるというもので、銀行の取引履歴や電話のメタデータなどで問題になった。

時間が経つにつれて、この法理は非常にセンシティブなデータにも適用されるようになった。例えば携帯電話のロケーションデータなども、通信会社という第三者が保有する以上憲法上の保護がないとされた。

今は、第三者提供の法理がどこまで妥当するかについて議論されている。この法理を捨ててセンシティブなデータに関する新たなルールが作られるべきだとも言われている。しかし、実際にプライバシーが放棄されたデータはあり、警察が捜査において適法に収集するこのようなデータと保護されるべきメタデータとをどのように区別するかが問題となる。

今、米国の立法府は、プライバシーの保護と捜査活動・インテリジェンス活動の調整に苦心している。個人情報を収集してよいかどうか、どれだけの期間保存してよいか、どんな時に使ってよいか、それ以外にどのような情報を収集してよいか、裁判所からいつ承認を得るべきかなど、明確なルールを構築しなければならない。

テクノロジーは常に変化しており、これは最も難しい問題の一つである。例えば、歩き方は一人一人異なり微妙な違いがあるため、テクノロジーの発展に伴い洗練されたプログラムで人間を非常に高い精度で特定できる[29]。顔認証技術もそうだ。フットボールゲームの最中にスタジアムにいる６万人を顔認証でスキャンして、逮捕状が出ている人物を探し出し、逮捕できる。

これらはすべて、令状なしで可能な状態になっており、どうするかを考えなければならない。率直に言って私はシンプルに適用できるルールは作れないと思う。コンテンツと非コンテンツを簡単に区別できるルールがないように。

29　歩容識別と呼ばれる。日本の「警察庁では既に歩容認証技術使った犯罪捜査が行われ、実際に逮捕まで至ったこともある」とされる。参考として http://monoist.atmarkit.co.jp/mn/articles/1507/17/news037.html

Ⅳ．政府と民間との関係性

二つのポイントがある。

① どのような状況下で、政府は民間から強制的に情報を取得できるか。

例えば、アップル対 FBI[30]はよく知られたケースである。

② 民間企業のデータ収集にどういった制約をかけるべきか。

米国には一般的なデータ保護法がない。金融、医療などの特定分野のデータについての保護法はあるが、一般消費者のデータなどについての保護法がない。今後、どれだけ広汎に民間企業を規制できるかが問題になる。

民間企業がデータを蓄積しなければ、政府がこれを差し出すよう命令することもできない。

こういった一連の課題に、米国内の警察の情報部門が取り組んでいる。

過去、多くの民間企業は任意に協力していたが、スノーデンリークの後、民間企業が政府の裏切りを知って政府と対峙するようになり、以前は任意で提出していたものについて、裁判所の許可を求めるようになっている。アップル対 FBI は好例である。以前であれば、アップルは警察の要求に応じたと思うが、今は戦おうとしている。このようなダイナミズムも広がっている。

なお、私見として、スノーデンリークについては評価していない。個々の諜報プログラムについて事実に基づく公共の議論がより行われるようになったことは唯一評価できる。それ以外は全て良くなかった。市民が広く情報を得ることは重要だが、非常に破壊的な状況がもたらされた。別の形で行われていればまた異なったかと思うが。

３．外国人の保護と外交的な懸念

米国は、他の国と同じように、米国内で受けられる保護と、米国外の外国人に対する保護が違う。一般的には、国外の外国人より国内の外国人に対する保護のほうが厚い。しかし、この線引きがどれだけ安定的かは疑問がある。

マイクロソフト、フェイスブック、アップル、グーグル等は海外の顧客を抱えている。これらの企業の支店からすると、米国内外を問わず、経済成長の元とある顧客であり、これらの人々を政府による監視・サイバー犯罪、海外諜報活動等の脅威から守る必要がある。

米国に対して、外国人についても国際人権法が適用され保護されるべきだと EU が強く主張し、ブラジルも主張している。国連などは、国際人権法は監視について権限を持つべきだと主張している。海外の諜報活動も制約を受けるべきだ、と。

---

30 14 人が死亡した銃乱射事件の犯人（事件後に逃走し、警察との銃撃戦の末に射殺された）が使用していた iPhone5c を解析するために、FBI がアクセスを試みたがパスコードがわからなかったことから、連邦地裁に対し、アップルに捜査協力を命じる内容の令状の発令を申し立て、2016 年 2 月 16 日、同裁判所がこの申立を認めた。同月 25 日、アップルがこの命令に異議を申し立て、異議審に係属したが、その判断前に FBI がアップルの助力なくしてセキュリティを破ることができたことを理由に申立を取り下げた。詳細は、末尾参考資料・JCLU Newsletter 399 号 井桁大介「テロとアメリカ 第１回 アップル対 FBI」参照。

米国は、上記二つの視点が具体的にどのように改革に影響するかを気にしている。

４．FAA702 条改正論議について

最も重要な監視法である FAA（FISA Amendment Act の略。外国諜報活動監視法改正法。FISA は、Foreign Intelligence Surveillance Act の略）702 条[31]が 2017 年 12 月に失効する予定だが、これを維持できるか、改正するかという問題がある。

着目すべきポイントは二つある。同条の米国民に対する適用の在り方と、海外の外国人に対する慣習を変えるか、である。

この監視プログラムは、インテリジェンスコミュニティにとって米国流の表現で「線路の上に寝そべる」と言われるほど、諜報活動の生命線と言われている。諜報部門はアグレッシブにロビー活動をするだろう。海外で今までと同様に諜報活動をしたいと。同条の適用のあり方は、国内では少し変わるかもしれないが、海外の活動は変えたくないということだ。国内はともかくとして、海外の権限を維持したいと。

愛国者法 215 条[32]に基づく電話のメタデータ収集（同条に基づき、「業務記録」として、通信会社に対し、通信会社が収集した電話のメタデータの提出命令が出せるとの解釈がなされた）は、私ももともと懐疑的であったが、米国自由法の下で廃止され、収集対象者を限定する方向に変更した。

他方、FAA702 条は多くの分野で有用であると考えられており、私もそう考えている。この点は、各人で見解が分かれるところであろう。

同条の改正は非常に難しい課題だと思う。私は米国内の市民に対するものは改革しつつ、海外における活動はそのまま維持すべきだと考えている。

米国にとっては戦略的に経済力と技術力（イノベーションの力）が最も重要であり、監視プログラムにより技術業界（テクノロジーコミュニティ）がダメージを受けることは望ましいことではない。他方、FAA702 条のプログラムは非常に重要である。私の知る限り、世界中のすべての国々が、自国民と海外の外国人とを線引きしている。海外で重要な諜報収集コミュニティを維持するのは非常に重要であり、それが FAA702 条の役割でもある。インテリジェンスコミュニティが顧客の信頼を回復しつつ、同時に 702 条プログラムの効力を維持することが重要と考えている。

通信には、①ほとんど米国市民間のもの、②ほとんど外国人だけのもの、③ほとんど外国人同士だが、一部米国人が関わっているか、国籍不明のものが考えられる。この三つを区別することは難しい。

イラク戦争で、イラクの電話回線から情報を集めることができたとして、ごく一部

---

31 インターネット上の通信監視プログラムの運用を認める規定。2017 年 12 月に期限を迎え、議会が再承認しなければ失効する。外国情報監視法は、広範かつ権利を侵害するような情報収集を認めるものだとして人権団体などから批判を浴びているが、トランプ政権は、プライバシー保護の観点からの改正をすることなく、従前の内容での議会の承認を得たいとの考えを明らかにしている。

32 国際テロや秘密諜報活動の対策として、FISC（Foreign Intelligence Surveillance Court）の承認を受け、捜査当局が各種の業務記録を入手できることを定めた条項。NSA は、この規定を根拠に、個人の通話やメール等の通信情報を「業務記録」として入手し、事実上無制限の情報収集を行っていたと批判されるに至った。末尾参考資料・JCLU Newsletter 401 号 井桁大介「テロとアメリカ 第３回 テロ法制の過去と現在 中編」参照。

に米国人の通信もあったが、ほとんどが外国人同士の通信であった。

例えば、私が何か犯罪に関わっていると警察に疑われたとして、私は米国市民で、米国内にいるから、上記と異なるルールが適用される。

難しいのは、①ある人が、米国外にいるが米国内の人と通信している場合、②一連の通信で、一見、外国人同士に見えるが、インターネットの経路に米国が関わる場合、③米国外の人間をモニターしている間にその者が米国内に移動する場合

という三つの場面だろう。線引きできる可能性はあるものの、100％常に明確になるわけではない。

５．データ使用のルールについて

おそらく明確なルールは存在しない。FIPPS（Fair Information Practice Principles、情報取扱いに関する公正慣行原則）は 1970 年代にプライバシー系の弁護士やソフトウェア技術者に広く受け入れられた。その一つとして、どのようなデータ収集が行われているかを人々に通知されるべきとするものがある。OECD でも同様の原則がある[33]。また、使用されるデータの種類や内容を個人は選択することができ、問題があれば削除する権利があることも含まれている[34]。これはヨーロッパの法律に広く取り入れられているが、米国の法律はあまりない。

世界はあまりにも複雑になっている。これらの原則は非常に抽象的、あいまいで、米国法、とりわけ諜報プログラムに正確な形で導入するのは非常に困難である。他の米国法と競合してしまう。米国法の中にはデータが合法的に収集された場合には、合法的な使用を許可するというものがある。これは収集目的の範囲内に利用が制限されるとする FIPPS が謳う内容と齟齬することとなる。

例えば、諜報活動の中で全く関係のない犯罪の証拠を入手した場合、この情報を犯罪捜査に用いることができるか。FIPPS などの原則に従うならば答えはノーとなる。しかし、ほとんどのアメリカ人は、犯罪捜査に用いるべきだというだろう。

現在、政府や民間企業は膨大な個人データを収集している。収集元は不明確で、使用先も不明確である。そのような状況で、どのように明確なルールを設定するかは大きな課題である。まだ直接法制化されていないうえ、どのように法制化するかは難しい問題である。

部分的には FIPPS などの原則を取り入れることもできるかもしれない。プライバシーシールド協定が米国とＥＵでなされた[35]が、その中にすべて盛り込まれているわけではなく、またあらゆる状況でそれができるわけではない。

---

[33] OECD８原則（1980 年）のうち、収集制限の原則（３項）、公開の原則（６項）など

[34] 同原則の利用制限の原則（２項）

[35] 米国と EU の間で個人情報を移転させる際の包括的な枠組みとしては、従前いわゆるセーフハーバー協定が設けられていたが、2015 年 10 月にスノーデンリークをきっかけとして EU 司法裁判所により同協定が無効と判断され、2016 年８月から新たな包括合意としてプライバシーシールド協定が取り交わされた。

６．テロ対策の諜報活動とプライバシー保護のバランス

テロ対策の諜報活動とプライバシー保護のバランスが、米国の議論の中心である。それ以外にも、様々な懸念事項がある。国家の利益がセキュリティとプライバシーの間で脅威にさらされるだけでなく、米国の経済力の問題もあるし、米国の技術力についての門戸の開き方もあるし、我々の友好国との外交の問題もあるし、米国の世界におけるリーダーシップの問題もある。

二つの価値観でのバランスではなくて、５つか６つの異なる価値観のバランスになると思う。今日お話ししたテーマには、多くの懸念が異なる形で絡んでくる、非常に複雑で難しい課題である。

参 考 資 料

プリズムの衝撃――監視国家と立憲主義　　大 林 啓 吾

（JCLU Newsletter 387 号～389 号所収）

テロとアメリカ 第１回　　アップル対 FBI
テロとアメリカ 第２回～第４回　テロ法制の過去と現在

井 桁 大 介

（JCLU Newsletter 399 号～402 号所収）

プリズムの衝撃

――監視国家と立憲主義（1）

千葉大学大学院専門法務研究科准教授・会員 大林 啓吾

序――プリズム計画

2013年6月6日、世界に衝撃が走った。アメリカの諜報機関NSAがインターネット等の通信を監視していることを、ガーディアン紙とワシントンポスト紙が暴露したからである[1)]。NSAは「プリズム」（Prism）と呼ばれる監視プログラムを実行しており、インターネット上のメールやスカイプ、チャット等のやり取りにアクセスしたり、その他の通信手段も監視していることが明らかになった。こうした監視は映画や小説等でしばしば題材に上がっていたこともあり、監視されているかもしれないという懸念はあったものの、どこか日常生活とはかけ離れた出来事として捉えられていた感があった[2)]。だが、それが現実のものとなった以上、この問題に向き合わなければならない。

とはいえ、日本のお茶の間では、それほど事態を深刻に受け止めなかったかもしれない。なぜなら、この事件は遠く太平洋を隔てたアメリカで起きた事件であり、日本とは関係がないように思えるからである。しかし、プリズムの対象はアメリカと外国との通信であり、日本にとって対岸の火事では済まされない。実際、その後の報道で、日本も対象になっていたことが明らかになっている[3)]。

あるいは、日本が監視対象になっていたとしてもテロ対策のためだから仕方ないと割り切ってしまうか、そもそも自分は何も悪いことはしていないから痛くも痒くもないと思う人もいるだろう。たしかに、アレクサンダーNSA局長の証言によると、阻止できたテロ計画は20以上の国で、50件以上あったという[4)]。しかしながら、監視が必要または無痛であるとしても、常時監視されている状態が健全な社会だといえるだろうか。この種の事件はアメリカに限らず各国で生じうる共通の問題であり、この事実が突き付ける課題は思った以上に深刻なものである。

では、何が問題なのか。それは紛れもなく、安全保障の名のもとにじわじわと浸透する監視国家の問題である。監視国家といえば、ベンサムのパノプティコンやオーウェルのテレスクリーンが想起されるが、今回のプリズムもそれらに負けるとも劣らない。私はこのニュースに接した時、映画「エネミー・オブ・アメリカ」（1998年）を思い出した。映画では監視強化のための法案の成否をめぐって殺人事件が発生し、偶然事件に関わってしまった者たちがひたすらNSAの追手から逃げるのだが、NSAの監視システムによりどこに逃げても見つかってしまう。NSAがハイテクを駆使して至るところで対象者の姿・行動を捕捉するシーンは圧巻で、当時も今もハイテクについていけない私には大変印象深いものとして記憶に残っている。

プリズムはそこまでハイテクを用いるわけではないのだが、そのインパクトを見誤ってはならない。というのも、インターネットが一般的な情報通信手段となっている今、それを監視されることは日常生活に監視が入り込んでいく様相を呈することとなる。しかも、9.11から10年以上経過してもなお、安全保障の名目で広範な監視が許されるとすれば、監視が常態化していることをもあらわしているといえよう。かかる状況は、もはや自由と安全という問題の枠組では収まりきらず、監視国家と立憲主義という深淵な問題に移行しつつある。

監視国家が立憲主義に変容をもたらすおそれがあ

1) Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 6, 2013, http://www.guardian.co.uk/world/2013/jun/06/ nsa-phone-records-verizon-court-order; Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://articles.washingtonpost.com/2013-06-06 /news/39784046_1_prism-nsa-u-s-servers.

2) 2013年6月18日毎日新聞東京朝刊[社説]。「驚くべき事件なのに、やっぱりそうかという印象がつきまとう。国家による情報収集が創造を超えるレベルに達していることを、私たちは薄々感じていたからだろう」と評されている。

3) Ewen MacAskill and Julian Border, *New NSA Leaks Show How US Is Bugging Its European Allies Exclusive: Edward Snowden Papers Reveal 38 Targets Including EU, France and Italy*, GUARDIAN, June 30, 2013, http://www.guardian.co.uk/ world/2013 /jun/30/ nsa-leaks-us-bugging-european-allies.

4) 2013年6月19日毎日新聞東京夕刊。

ることは、すでにバルキンの指摘するところである[5]。監視国家が進むと、監視の実行役である執行府が強大化し、事後処罰から事前予防にシフトすることで自由が縮減するおそれがある。また、政府が民間企業を利用して情報管理を行うことで、政府自身は憲法上の統制を受けずに監視を強めていく可能性もある。その結果、個人のプライバシーは、政府と企業の双方によって脅威にさらされることになるのである[6]。

ところが、監視行為や監視内容は一般市民にとって不可知であるがゆえに、具体的な権利侵害が表面化しにくいというやっかいな課題を抱える。この潜在的権利侵害を甘受すべきか否か、換言すれば司法救済可能なものへと転換させるか否か、という問題は、今後の立憲主義の行方を占うものである。また、今回のプリズム計画は、形式上は法律に基づいて行われている点も見逃せない。つまり、現在の法制度では合法的に監視することができる仕組みになっているのである。ゆえに監視から免れたいと思う者に残された武器はやはり憲法しかない。

以下では、今回の事件を契機に、監視の法的構造を紐解きながら、監視国家の憲法問題を考えてみたい。

1. NSAによる監視 ――G・W・ブッシュ政権の遺産?

まず、プリズム計画に至る流れを概観しておく。プリズム計画の実行役であるNSAは、トルーマン大統領の命令によって創設され、別名「存在しない機関」(No Such Agency) と呼ばれるほど、その実態がベールに包まれている機関である。その活動内容を把握することができないことから、市民生活を監視しているのではないかという噂が後を絶たなかった。

その杞憂が現実のものとなったのが、今から8年前に暴露されたNSA盗聴事件である[7]。G・W・ブッシュ大統領(以下、「ブッシュ大統領」という)は、TSP (Terrorist Surveillance Program) と銘打って、令状なしで外国と国内の間の通信をNSAに盗聴させてきた。アメリカには外国諜報活動監視法(FISA)という法律があり、本法により外国と国内の間の通信を傍受する場合には原則として外国諜報活動監視裁判所(FISC)の許可が必要とされていた[8]。しかし、NSAが行ってきた盗聴はFISAの規定を無視しており、FISCの許可を得ていなかった。つまり、それは違法行為であることが明白だったのである。しかし、ブッシュ大統領は、連邦議会が武力行使容認決議(AUMF)[9]によってテロ対策に必要な行為を大統領に認めていたはずであると反論した。そして、かりにそれによって認められていなくても、テロ対策のために盗聴を行うことは執行府の責務として憲法上認められた行為であり、法律に従う必要がないと主張したのである。これに対しては、連邦議会が強く反発し、メディアや学界からも多くの批判を浴びた。

この行為の違法性を法的に糾弾しようとして動いたのがACLUであり、自分たちの会話が盗聴されていた可能性が高いとして訴訟を提起した。だが、裁判には大きな壁が立ちふさがっていた。当事者適格という壁である。盗聴が行われていたことが明るみにでたものの、盗聴対象が明らかになっていなかったことから、ACLUの権利侵害を認めさせるためには、当事者適格という関門を突破しなければならなかったのである。一審は、盗聴対象に含まれている可能性を重視して当事者適格を認めたが[10]、控訴審は具体的な証明等がなければならないとして当事者適格を認めず[11]、連邦最高裁もそれを支持して裁量上訴を認めなかった。

しかし、立法府の反発が強いことに加え、一審判決は本案で盗聴行為の違法性および違憲性を認めていたことから、ブッシュ大統領は法整備を進め、2008年にFISAの修正がなされた(修正後の法律をFAAという)。FAAの702条(合衆国法典1881a条)により、外国の諜報関連の情報だと合理的に信じられる場合で

5) Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

6) Orin S. Kerr, *A Response to Balkin*, 93 MINN. L. REV. 2179 (2009). そのため、監視国家に対応するためには、政府による監視に憲法上の統制をかけつつ、民間企業に対する法的規制が必要である。

7) James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

8) 50 U.S.C. 1803(a)(1). なお、FISCの判事は連邦最高裁長官が任命する11名の連邦地裁判事からなる。

9) Authorization for Use of Military Force, Pub. L. No.107-40, 115 Stat. 224 (2001).これにより、大統領は軍隊をテロ対策に用いることができる権限を授権された。

10) ACLU v. NSA, 438 F. Supp. 2d 754 (2006). 連邦地裁は、盗聴により、①原告は萎縮効果という損害を被り、②盗聴対象には原告らの会話が含まれる可能性があり、③盗聴行為の違憲判断により萎縮効果が除去されて原告は救済されるとして、原告適格を認めた。

11) ACLU v. NSA, 493 F.3d 644 (6th. Cir. 2007), *cert. denied*, 128 S. Ct. 1334 (2008). 連邦高裁は、①盗聴されたという証拠はなく、②委縮効果との関係性はなく、③損害がない以上判決による救済可能性も存在しないとした。

あれば、FISCの許可を得た上で、1年間通信傍受できることになった[12]。従来、外国のエージェントの活動に関する情報といったように、通信対象には相応の容疑が必要とされていた。だが、本改正により、事実上、ほとんど対象を絞る必要がなくなったといえる。つまり、外国の諜報情報に関すると予想されれば、その通信を傍受することができるようになったのである。このように、法律上、実質的な対象の特定が不要となっていることから、FISCはほとんどの傍受申請を許可しており、許可の実態は通常の裁判所の令状よりもかなり緩和された形となっている[13]。

2. 監視計画の概要――G･W･オバマ?

ブッシュ大統領が政権末期に残したFAAという遺産は、ブッシュ政権の盗聴行為を批判していたオバマ大統領にとっても使い道のあるものであった。実際、この法制度を実行していたのが、今回のプリズムだったのである。新聞報道によると、NSAの監視プログラムは、電話番号や通話時間等のメタデータを収集するメインウェイ（Mainway）、電話の通話内容を収集するニュークレオン（Nucleon）、インターネット上のメールアドレス等のメタデータを収集するマリーナ（Marina）、そして外国との通信内容を収集するプリズム、があるとされる[14]。このうち、プリズムは2007年からブッシュ政権がスタートさせたもので[15]、オバマ政権はそれを引き継ぐ形となっている。

オバマ政権は、マイクロソフト、ヤフー、グーグル、フェイスブック、ユーチューブ、スカイプ、アップル等の9社に対し、メール等のデータにアクセスさせるように求めていた。FAAの規定により、司法長官と国家情報局長は電子メディアに対し、先のような外国情報を入手するためにあらゆる情報の提供を命じることができるとしているからである[16]。しかもFAAにより、電子メディアは情報提供による法的責任を負わないと規定されており、情報提供しやすい環境が整えられている[17]。そのため、オバマ政権では2008年以降対象を拡大し、数百万人を対象にしてきたとされる。また、メインウェイの一環と考えられる情報収集も行われており、ベライゾン社に電話の通話記録（メタデータ）を提供させてきたと報じられている。

こうした情報収集は、暴露されるまで明るみにでなかったので、インターネット上ではブッシュ大統領と変わらないとして、「G・W・オバマ」などの揶揄が飛び交った。前ブッシュ政権の盗聴行為を批判し、透明性を前面に打ち出していたオバマ大統領であったからこそ、余計にリベラル派の市民を大きく落胆させたのである。また、グーグルやフェイスブックはプリズムのような大きな傍受計画に加担した事実はないとしており[18]、事実に関する政府発表との食い違いも、政権の信頼性を揺るがす一因となっている。

これに対してオバマ大統領はまるでブッシュと一緒にされてはたまらないといわんばかりに、ただちにその正当化をはかった[19]。ブッシュ大統領の場合と異なり、プリズムはFISAに基づく合法的な行為であることを強調したのである。また、それはテロを防ぐために必要な行為であり、しかも外国にいる者の通信が対象となっているのであって、市民のプライバシーには最大限の配慮を払っているとした。オバマ大統領の反論後、国家情報局も弁明書を出している[20]。弁明書は、プリズムがFAA702条に基づく行為であることを確認し、それが手続に則っていることを強調した。とりわけ、プリズムによる情報収集はFISCの許可と電子メディアの協力があって行えるものであるとして、NSAが独断で行っているわけではないと主張した。

たしかに、FAAの規定がある以上、法律上は合法

12）50 U.S.C. 1881a(a).

13）Mitra Ebadolahi, *Warrantless Wiretapping Under the FISA Amendment Act*, 39 HUMAN RIGHTS 11 (2013).

14）Barton Gellman, *U.S. surveillance architecture includes collection of revealing Internet, phone metadata*, WASH. POST, June 16, 2013, http://www.washingtonpost.com /investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_print.html.

15）Protect America Act of 2007, §105B. なお、2007年にアメリカ保護法(PAA)が制定され、一定の要件の下に令状なしで外国との通信傍受が可能になっていたが、サンセット法であったため、新たに2008年にFAAが制定されることとなった。

16）50 U.S.C. 1881a (h)(1)(A).

17）50 U.S.C. 1881a (h)(3).

18）Craig Timberg and Cecilia Kang, *High-Tech Giants Urge Openness on Probes*, WASH. POST, June 8, 2013, at A7.

19）Peter Finn and Ellen Nakashima, *Obama Defends NSA Collection of Citizens' Data*, WASH. POST, June 8, 2013, at A1.

20）*Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, DIRECTOR OF NATIONAL INTELLIGENCE WASH. DC 20511 (June 8, 2013).

的に通信を傍受することができる[21]。だが、それはあくまで法律上は合法だということに注意しなければならない。たとえ法律に則っていたとしても、それが憲法上正当化される行為であるか否かは別問題だからである。

3. FAAの合憲性

実は、プリズムが発覚する前からFAAの合憲性が司法の場で問われていた。ACLUやアムネスティらが、FAAが表現の自由を侵害し違憲であるとして訴えを起こしたClapper v. Amnesty連邦最高裁判決[22]である。ところが、連邦最高裁は5対4の僅差で当事者適格に欠けるとして、訴えを却下した。法廷意見によれば、当事者適格をみたすためには、具体的で、特定された、実際の、差し迫った損害があり、問題となっている行為が原因で、請求を認容する判決が出ることによって救済されなければならないという。これを本件に当てはめると、原告の通信が対象となっているという主張は憶測にすぎない。仮に対象になっているとしても1881a条に基づいて傍受しているとは限らず、1881a条による傍受が行われているとしてもFISCが許可しているともいえない。また、FISCの許可があったとしてもまだ傍受を続けているかわからず、たとえ傍受の中に原告の通信が入っていたとしてもそれは当初から対象とされていたのではなく偶然含まれていたのかもしれない。ゆえに、本件では当事者適格がみたされていないとして、訴えを却下したのである。

一方、ブライヤー判事の反対意見は、原告の損害が仮定的ではなく、具体的で特定された損害であるとする[23]。損害の有無は、通信傍受が実際または切迫しているかどうかで判断される。原告は、1881a条の対象となりうるコミュニケーションをとってきたという事実があること、原告はテロが関係しそうな通信に関心があるだけでなく政府もそれに関心があったこと、政府は過去にもそうした情報を収集していたこと、政府はそうした通信を傍受する能力を有していることなどからして、政府は原告の通信を傍受していた可能性が高い。さらに、法廷意見は、脅威となる損害が確実に切迫（certainly impending）していなければならないとしているが、そもそも将来に起きる事象は不確実であり、先例はこれまで一定のケースにおいて将来の損害の可能性を認めてきた。したがって、本件では切迫した損害があり、当事者適格を認めるべきであると反論した。

法廷意見と反対意見は当事者適格の有無をめぐり真っ向から対立しているのであるが、法廷意見の想定する当事者適格はかなり射程が狭いものである。法廷意見の枠組で考えると、この種の事案では、具体的な監視行為が明らかになり、そこで監視対象とされた個人が特定され、どのようなプロセスで何を目的として監視していたのかがはっきりしなければ、当事者適格が認められないかのように思える。

そうなると、今回発覚したプリズムに対して、司法がどのような対応をするのだろうか。実際、プリズムに対しては早速ACLUが訴えを提起している。ACLUによれば、ベライゾンの顧客にはACLUも含まれていることから、当事者適格のハードルを乗り越えることができるという[24]。ただし、提出記録の中にACLUが入っているかどうかは不明であるため、ただちに当事者適格が認められるとは限らない点に留意しておかなければならない。

このように、FAAの合憲性の問題以前に、当事者適格の問題が主戦場になっているのが現状である。しかしながら、もしFAAが違憲であるにもかかわらず、当事者適格の問題を突破できないがゆえに違憲判断を獲得することができないとすれば、この問題は画餅の権利ともいうべきものとなる。なぜなら、具体的な侵害行為が行われているにもかかわらず、対象が明らかにならないがゆえに、当該行為の違法性を糾弾できないという事態が生じるからである。では、事態の打開をはかるためには何が必要であろうか。

次号（2）に続く

＊ 2013年7月8日脱稿。プリズム事件の内容については脱稿時までに知り得た情報を基にしているので、その後の報道により事実関係が変わる可能性があることをお断りしておく。

21）今回のプリズムについては、司法長官および国家情報局長が外国にいると合理的に信じられる者の通信につき、FISCの許可に基づいて傍受することを認める1881a条を基に、電子メディアに情報提供を要求できる1881a 条(h)(1)(A)に依拠しながら、NSAに情報収集させたと考えられる。

22）Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

23）*Id.* at 1155-1165 (Breyer, J., dissenting).

24）Ellen Nakashima and Scott Wilson, *ACLU Challenges NSA Program*, WASH. POST, June 12, 2013, at A5.

プリズムの衝撃

――監視国家と立憲主義（2）

千葉大学大学院専門法務研究科准教授・会員 大林 啓吾

―前号のあらすじ―

2013年6月6日、アメリカの諜報機関であるNSAがプリズムと呼ばれる監視プログラムを実行して、インターネット上の通信を監視していたことが暴露された。近年、監視の網は広がるいっぽうであるが、プリズムはそれ自体の問題にとどまらず、監視国家の是非を考える契機となりそうである。

プリズムは、FAAという法律に基づいて実行されているため、合法的に行われたものである。しかし、そうした行為が憲法上正当化されるかどうかは別問題である。実際、プリズムが発覚する前から、ACLUやアムネスティらがFAAは表現の自由等を侵害し違憲であるとの裁判を起こしていた。ところが、連邦最高裁は、具体的な監視行為や監視対象とされた個人が特定されなければ当事者適格が認められないとして、訴えを却下した。

そうなると、監視が憲法違反であるとしても、裁判所でそれを問うことは困難になってしまう。この現状を打開するためにはどうすればいいだろうか。

4 何の権利が侵害されているのか?

ここで闇雲に当事者適格のハードルを越えるための技術論をひねり出そうとしても、実体的判断の場面で侵害が正当化されてしまえば同じことである。ゆえに、FAAに基づく監視行為がいかなる権利を侵害しているのかをきちんと分析しておかなければならない。

監視行為によって侵害される権利といえば、一般的な感覚からすれば、プライバシーの権利が思い浮かぶだろう。むしろ、それ以外に何があるのか、とすら感じるかもしれない。ただし、アメリカの法文化は独自の発展を遂げていることに注意しなければならない。

まず、アメリカの判例法理はいまだ古典的プライバシー観に縛られている感がある。そのため、いわゆる自己情報コントロール権としての情報プライバシー権が判例上十分に展開しているとはいえない[25]。しかも、政府による監視の問題は令状との関係が問題視されることから、修正14条に基づく一般的プライバシー権の文脈ではなく、修正4条に基づく刑事手続に関するプライバシー権の問題として認識されることになる。つまり、主として令状主義の問題に収斂されてしまう可能性が高い。FAAの文脈でいうと、FISCの許可だけで一年間監視できるシステムは修正4条の令状主義の要請との関係で問題となり、プライバシー権を侵害するのではないかという問題になるわけである。

さらに、アメリカは表現の自由を重視する国であることを忘れてはならない。表現の自由の観点からすると、政府の監視行為に対しては自由な情報の流通を阻害しかねないプライバシー権よりも表現の自由の問題として構成した方が自由な表現空間を狭めなくてすむ。実際、アメリカでは情報に関する事件がプライバシー権よりも表現の自由の問題として把握されることがある[26]。加えて、監視行為は表現活動を委縮させるものであることから、表現の自由の問題を主張した方がプライバシー権よりも当事者適格の壁を突破しやすくなるというメリットもある。したがって、プリズム問題もプライバシー権の問題だけでなく、表現の自由の問題も並行して考えていく必要がある。ただし、時として両者は緊張関係に陥る可能性があるため、その接合が可能かどうかも吟味しなければならない。

まずは、プライバシー権の法理を確認しておこう。アメリカの刑事手続に関するプライバシー権もまた独自の発展を遂げている。かつて連邦最高裁は、修正4条の令状主義は物理的捜査（捜索）に対してのみ要請されるとしてきた[27]。そのため、通信傍受については令状が不要とされてきたのである。しかし、1967年のKatz v. United States連邦最高裁判

25）判例法理については、大林啓吾「アメリカにおける情報プライバシー権の法理」千葉大学法学論集27巻4号157頁（2013年）参照。

26）*See,.e.g.*, Anita L. Allen, *First Amendment Privacy and the Battle for Progressively Liberal Social Change*, 14 U. PA. J. CONST. L. 885 (2012).

27）Olmstead v. United States, 277 U.S. 438 (1928).

決[28] が盗聴にも令状が必要であるとしたことにより、1968年法（TitleⅢ）が制定され、通信傍受にも令状が要件となった。その後、コンピューター上の通信に対応するため、1986年に法改正が行われて電子コミュニケーションプライバシー法（ECPA）が制定された。その結果、パソコン等の電子通信を傍受するためには令状が必要とされることになった。このように、国内における電子通信については、裁判所の令状がなければ修正4条違反となる。

これに例外を設けたのが、1978年に制定されたFISAであった。外国との通信に関する傍受は特殊な領域の問題であることから、それについては裁判所の令状ではなく、FISCという特別裁判所の許可にかからしめることになったのである。

実は、今回のケースも、FISAの手続に基づき、FISCの許可を得ているので、修正4条の要請をみたしているようにみえる。しかしながら、FAAに基づく通信傍受は、FISCの許可条件が緩やかであることに加え、漠然とした対象のまま一年もの間通信を傍受することができる。しかも、FISAレポートをみると、ほとんどすべての通信傍受申請に許可が与えられている。たとえば、2012年のレポートをみても、電子通信の傍受申請が1789件あり、このうち１件については政府側が撤回したものの、残るすべての申請が許可された[29]。FISCは40件の申請に修正を施しているが、ほぼ政府の申請を認めているのが現状である。したがって、たとえ法律で傍受権限を執行府に付与していても、その内容が適正でなければ修正4条との関連で問題になる。

5　第三者任意提供の法理の問題

しかしながら、プライバシー権の侵害を主張する場合には、やっかいな障壁が立ちはだかる。それが、「第三者任意提供の法理」（third party doctrine）である。この法理は、自発的に個人情報を第三者に提供した場合、修正4条のプライバシー保護が及ばないというものである。たとえば、インターネットを利用してメール通信を行った場合、自らすすんで個人情報をインターネットプロバイダー（第三者）に提供したことになり、政府がそれを収集・利用しても修正4条に基づくプライバシーの侵害にはならないということである。

この法理は、1976年のUnited States v. Miller連邦最高裁判決[30] によって示された法理で、銀行記録は本人が自発的に銀行という第三者に個人情報を提供したものであるから、修正4条のプライバシー保護が及ばないとし、政府が当該記録を銀行から入手してもプライバシーの問題は生じないとした。しかし、これに対しては批判が強く、1978年に連邦議会は金融記録に関する保護法（The Right to Financial Privacy Act of 1978）を制定している。一方、連邦最高裁はこの法理を維持する姿勢を崩さず、1979年のSmith v. Maryland連邦最高裁判決[31] では自宅からかけた電話番号の記録にも第三者任意提供の法理を適用し、プライバシーの保護が及ばないとされた。ただし、この判決に対しても連邦議会が反発し、電話番号記録を保護する法律（Pen Register Act）を制定している。

その後、連邦最高裁は第三者任意提供の法理に限定をかける傾向があるものの、この法理自体を放棄してはいない。すると、この第三者任意提供の法理がネット上の情報にも適用される可能性がある。その是非は、Katz判決の合理的期待の法理をどのように理解するかにもよるが、そもそも第三者任意提供の法理自体の妥当性には疑問がある[32]。この法理は自発的に公にさらすことでプライバシー性を放棄することになるというロジックに基づくが、しかし、個人情報を事業者に提供することが公にさらすことと同義であるわけではない。特定のサービスを利用するために自らの情報を提供しても、それはあくまで当該サービスを利用するために提供するのであって、他者に公開されることとは別問題のはずである。むしろ、合理的期待論を文字通り受け止めれば、プライバシーとして保護されると考えることが客観的に見て合理的であることが重要なのであるから、提供した個人情報は当該事業者との契約等の関係でのみ使用されることが通常期待されるといえるのではないだろうか[33]。

28）Katz v. United States, 389 U.S. 347 (1967).

29）FISA Annual Reports to Congress of 2012, (Apr. 30, 2013), http://www.fas.org/irp/ agency/doj/fisa/2012rept.pdf

30）United States v. Miller, 425 U.S. 435 (1976).

31）Smith v. Maryland, 442 U.S. 735 (1979).

32）United States v. Jones, 132 S.Ct. 945, 957 (2012)(Sotomayor, J., concurring). ソトマイヨール判事は、「第三者に任意で公開した情報にはプライバシーの合理的期待がないという前提については再考する必要がある」と述べている。

33）この点につき、日本では講演会名簿提出事件（最2小判平成15年9月12日民集57巻8号973頁）において、情報を取得した側が本人に無断で個人情報を警察に開示する行為は,任意に提供した個人情報の適切な管理についての合理的な期待を裏切るものであり,プライバシーを侵害すると判断されている。ただし、この事件における被告は国ではなく、情報を提供した法人である。

それは、あくまで個人と事業者との関係において使用される個人情報であり、そこに介入してくる政府に対する関係とは異なるのである[34]。

ましてや、ネットを通じたコミュニケーションが日常生活に不可欠になっている現状を踏まえると、ネットについてはなおさら第三者任意提供の法理を適用することには問題がある[35]。なぜなら、ネットにアクセスしなければ通信できないという環境にある以上、アクセスした時点で自己情報を任意提供したとみなされてしまえば、アクセスすることができなくなり、結果的に通信を行うことができなくなるからである。とすれば、ネットにアクセスすることがただちに第三者たるプロバイダーに対して個人情報を自由に提供または使用してもよいことを意味するわけではなく、実際に通信する段階においてどの方法を選ぶかという時点で初めて個人情報を提供するかどうかの選択を行うことになるといえよう。

したがって、第三者任意提供の法理を理由に、政府の情報収集を正当化することには無理があるといえる。そうした論理の飛躍があるにもかかわらず、連邦最高裁がこの法理を放棄しないことにはいかなる理由があるのだろうか。それは、合理的期待の法理の射程が曖昧であることが大きいが[36]、そこには連邦最高裁が重視してきた表現の自由との調整をどうはかるかという問題が潜在しているように思われる。なぜなら、プライバシー権の保護を高めると情報を自由に利用できなくなり、自由な表現空間に支障をもたらすおそれがあるからである。しかし、監視行為に対するプライバシー権の主張を考える場合、プライバシー権と表現の自由は相互補完的に機能する可能性があり、その調整論を検討する必要がある。

6 プライバシーの量と質

そこで、プライバシー権と表現の自由を調整しながら、知的プライバシー（intellectual privacy）として再構成するのがリチャーズである。リチャーズは、ブランダイス判事のプライバシー観に依拠しながら、プライバシー権と表現の自由につき、公共討論の観点から調整をはかる。プライバシー権は、公共討論と関係のない言論による私的介入を阻止するものであり、ブランダイスのプライバシー論文[37]もそうした趣旨のものであった。他面において、ブランダイス判事はOlmstead連邦最高裁判決における反対意見[38]で、修正４条の憲法起草者が個人の知性（intellect）の重要性を認識していたことに触れながら、プライバシー権を持ち出し、盗聴がプライバシー権の侵害になるとした[39]。つまり、プライバシー権は私的領域を保護しつつ公共討論の重要性を提示するという両側面を併せ持つ、知的プライバシー権だと考えるのである。

こうしたプライバシー観のもと、リチャーズは、政府の監視行為は２つの側面において被害をもたらすという[40]。１つは、知的プライバシー権の侵害である。監視されるおそれがあると、市民は政治や社会問題についてコミュニケーションをとらなくなり、公共討論が実現されなくなる。もう１つは、監視による差別や強制的効果が生じるおそれがあることである。監視目的とは関係なく、政府批判等が取り締まられるおそれがあるのである。

これに対して、シトロン＝グレイは、リチャーズのように情報の質に着目するのではなく、情報の全体量を問題にすべきだとする[41]。かれらによれば、技術の発展により大量の情報集積が可能になったことこそが監視社会を生み出しており、市民は収集されるプライバシーの質よりも、量が合理的に保護されるように期待することができるという。政府は民間と協同して無制約に情報を集積しており、もはや情報の性質はプライバシーの本質ではなくなっている。しかも、政府の収集した情報が知的活動に関連するものなのかどうかを特定することが難しいことから、情報の性質に着目して訴えを提起することも実際上は困難である。そのため、プライバシーの量に関する合理的な保護を求めて、司法のみならず、立法や行政に対しても

34) Brett Snider, *NSA, FBI Surveillance: Legally Justified?*, FIND LAW, June 7, 2013, http://blogs.findlaw.com/blotter/2013/06/nsa-fbi-surveillance-legally-justified.html

35) Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Forth Amendment*, 13 FL. COASTAL. L. REV. 33, 63-78 (2011).

36) Brandon T. Crowther, *(Un)Reasonable Expectation of Digital Privacy*, 2012 B.Y.U. L. REV. 343 (2012).

37) Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

38) *Olmstead*, 277 U.S. at 471-485 (Brandeis, J., dissenting).

39) Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010).

40) Neil M. Richards, *Privacy and Technology: The Dangerous of Surveillance*, 126 HARV. L. REV. 1934 (2013).

41) Danielle Keats Citron and David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262 (2013).

それを要求していくべきだと考えるのである。

一方、ポズナーは、莫大な量の個人情報の収集がプライバシー権に影響することを認めながらも、コンピューターによる自動収集化により、プライバシーの問題が回避されるという[42]。コンピューターは意思を持っていないことから、個人情報を機械的に扱うだけである。つまり、意思を持たない機械が情報を集めてもプライバシーが覗かれたことにはならないので、プライバシー権の問題が生じないというのである。

また、スタンツのように、プライバシー権が問題になるのは公開の場面であって、収集の段階では問題にならないという見解もある[43]。そのため、NSAが情報を収集していてもプライバシー権が侵害されたことにはならず、プライバシー情報が公になって初めて侵害が生じるというのである。

だが、プライバシー権といっても、状況に応じて様々な保障のレベルがあり、そのレベルごとに考えていくべきだとする見解がある[44]。ソロブによれば、プライバシー権の問題は、収集と公開のいずれかの段階においてのみ生じるわけではない。それは、収集、管理、公開の各段階においてそれぞれ問題が起きる。これらのうち、データマイニングでは、収集された情報がどのように保管され、分析され、使用されるのかという点が最も重要な問題となる。

情報の保管、分析、使用については、令状主義、表現の自由、平等の問題が生じうる。もっとも、令状主義は主として情報収集の段階に対応するものであることから、収集後の情報管理の場面で機能させるためには工夫が必要である。一方、表現事項や宗教事項等に着目しながら情報の内容をプロファイルし、その結果に基づいてブラックリストに載せる行為は表現の自由の問題を惹起する。また、人種や民族に基づきプロファイルし、それに応じた差別的取扱いを行うことは平等の問題を生じさせることになる。

次号(3)に続く

42）Richard A. Posner, *Our Domestic Intelligence Crisis*,WASH. POST A31 (Dec. 21, 2005).

43）William J. Stuntz, *Secret Service: Against Privacy and Transparency*, NEW REPUBLIC 12 (Apr. 17, 2006).

44）Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008).

プリズムの衝撃

――監視国家と立憲主義(3)

千葉大学大学院専門法務研究科准教授・会員 大林 啓吾

―前号までのあらすじ―

2013年6月、NSAがプリズムやメインウェイと呼ばれる監視プログラムを実行して、インターネット上の通信や電話記録などを監視していたことが暴露された。これらの計画は、FAAという法律に基づいて合法的に行われたが、憲法上正当化されるかは別問題である。

FAAに基づく通信傍受はFISCという特別裁判所の許可によって実施されるが、FISCはほぼすべてに許可を与えており、政府は傍受の対象を漠然としたまま、1年もの長期にわたって通信傍受ができるという現状がある。このことは、令状主義を定めた修正4条との関連で問題になりうる。本号では、この問題がプライバシー権を侵害しているのではないかという点につき、理論的分析を続けると同時に、最近の下級審の動向を踏まえながら、今後の展望について考えてみることにする。

7 文脈アプローチによるパラドックスの回避

このように、国家による情報の取扱いは様々な憲法問題を惹起することから、ソロブは情報収集や管理方法についての透明性が重要であると説く[46]。テロ対策のために情報を集めて分析する場合、その内容を明らかにしてしまうと意味がなくなってしまうおそれがあることから、透明性が確保されないことが多い。しかし、政府が何をしているのかが明らかにならなければ、情報がどのように集められ、使用されているのかがわからず、権利侵害がなされているかもわからない。その結果、権利侵害の救済を行うことが不可能になってしまう。

かかる状況に対応するためには、プライバシー権について、場面や状況ごとに考えていくアプローチが重要である。というのも、今回のプリズム事件について、プライバシー権からアプローチすると、あるパラドックスを抱えるからである。情報漏洩や情報流出などの偶発的事象によって初めて事が露見するという特性は、そうした事件が市民のプライバシー保護にとって僥倖となる反面、プライバシー保護を強化するために情報システムをますます密閉するというパラドックスに陥る。つまり、プライバシーを守るためには情報管理が厳重になされなければならないものの、情報管理のために外部からのアクセスを遮断すればするほど、勝手に情報が収集・管理・利用されていることが明らかにされにくくなってしまうおそれが生じるのである。これは、プライバシー権のうち、公開されない側面のみにとらわれてしまうことで生じるパラドックスである。

この問題に対しては場面ごとに分けながら制度的改善をはかることにより、ある程度対応することができる。なぜなら、収集の段階で要件を絞ったり、管理や利用にも一定の制限を設けたりすることは、両方ともプライバシー権の保護につながるからである。では、プリズムのような監視行為によってプライバシー権が侵害された場合、どのようにして当事者適格の問題をクリアすればいいだろうか。ここで登場するのが統治論である。

8 統治論――マクロとミクロの憲法問題

クーは、監視行為の問題にはマクロレベルとミクロレベルの問題があるという[47]。マクロレベルの問題とは形式的な意味での法的統制のことである。TSP問題の際、執行府が立法統制を受けないまま盗聴をしていたことが最も問題視された。しかも、裁判においても当事者適格ではねられていることから、司法統制にもかかっていない。そこで、立法統制および司法統制に服せしめるべく、制定されたのがFAAであった。FAAは、法律による手続を規定し、FISCの許可にかからしめる枠組を設けたのである。このように、法的統制をかけるという意味でFAAは肯定的に評価できる。が、しかし、視点を変えると、令状なしの通信傍受に法的な意味でお墨付きを与えたという見方もできる。なぜなら、FAAは、司法長官と国家情報局長が外国諜

46) *Id.* at 359-361.

47) Raymond Shih Ray Ku, *Unlimited Power: Why the President's (Warrantless) Surveillance Program Is Unconstitutional,* 42 CASE W. RES. J. INT' L L. 647 (2010).

報に関する情報を得るために合衆国外にいると合理的に信じられる者の通信を、FISCの許可を得れば一年間傍受できるとしているからである。そのため、この法的手続に反しない限り、執行府は合法的に長期間通信傍受をすることができるようになったのである。

すると、もはやマクロレベルの形式的な法的問題は解決済みということになり、問題は実質的内容に移る。クーはこれをミクロレベルの問題とし、当該手続が修正4条の令状主義を没却していないかを検討しなければならないという。このとき、重要なのは、修正4条を権利論としてではなく、統治の観点から活用することである。クーによれば、かつてジャクソン判事が法の支配におけるルールを強調したように、修正4条はプライバシー権の保護にとどまらず、全般的な私的自由の保障を規定したものであり、政府が私的領域に介入する際のルールを定めたものであるという。そのため、FAAの手続が修正4条の令状主義を埋没させていないかどうかを分析しなければならない。すると、FAAは、傍受対象となる場所等を提示することを要求せず、政府による私的領域への介入を大幅に緩和したものとなっており、修正4条が要請するルールをみたしているとはいえないと、クーは結論づけている。

クーが指摘するように、通信傍受が法律に基づいて行われる以上、そこに形式的問題があるとは言い難い。だが、その内容に問題があるとすれば、その違憲性を司法の場で問うことが必要である。ただし、当事者適格の壁が予想以上に高い場合、個人の主観的権利を前面に押し出すだけでなく、客観的ルール違反を問うことにより、実際の損害の要件を突破する糸口を見出すわけである。

このように、クーの議論は客観的法制度の合憲性を問う理論として提示されており、監視プログラムの合憲性など、自己の権利が侵害されていることを具体的に立証しにくい場合にも、司法統制を試みる議論として興味深い。

もっとも、下級審では、クーの理論を用いるまでもなく、今回の事案において当事者適格を認める判断が登場している。

9　下級審の動向

プリズム計画が暴露された後、ACLUらの市民団体はただちに訴訟を提起していた[48]。裁判では、NSAの４つの監視プログラムのうち、とくに電話のメタデータを収集していたことが争われた。そして、この裁判に関する２つの判決が2013年12月に下されたのである。しかも、Klayman v. Obama連邦地裁判決[49]が違憲判断を下したのに対し、ACLU v. Clapper連邦地裁判決[50]は合憲判断を下しており、２つの連邦地裁で判断が異なる結果となっている。

判決結果は異なるものの、両判決ともに当事者適格を認めていることがまずは注目される。両判決は、NSAが電話に関するメタデータを収集していることは新聞の暴露やFISCの許可命令により明らかになっており、ベライゾンの顧客である原告はその対象となっている可能性が高いと判断したのである。ブッシュ政権の盗聴が裁判となったACLU v. NSA連邦地裁判決[51]でも当事者適格が認められていたことからすれば、一審レベルでは当事者適格が認められやすく、上級審に進むにつれて否定的になる可能性もあるが、今回のケースでは新聞の暴露だけでなく、FISCの許可命令という具体的国家行為によって、政府が監視していたことが明らかになっている。そして、ベライゾンの顧客である原告はこの監視プログラムの対象になっていたという推定が働く。そのため、本件原告は前回のケースよりも監視対象となっていた可能性が高く、当事者適格が認められやすくなっているといえるかもしれない。

さて、気になる権利侵害の問題については、両判決で判断が分かれた。その際、争点となったのは、前号で指摘したように、やはり第三者任意提供の法理の適用であった。Klayman v. Obama判決は、第三者任意提供の法理の先例としてしばしば引用されるSmith v. Maryland判決[52]が本件では参照に値しないとし、代わりに車にGPSを取り付けて約１ヶ月にわたり追跡したことがプライバシー権を侵害するとした2012年のUnited States v. Jones判決[53]を先例として参照すべきだとする。というの

48）大林啓吾「プリズムの衝撃――監視国家と立憲主義（1）」JCLU Newsletter 387号11頁（2013年）を参照。

49）Klayman v. Obama, 2013 U.S. Dist. LEXIS 177169 (D.D.C., Dec. 16, 2013).

50）ACLU v. Clapper, 2013 U.S. Dist. LEXIS 180863 (S.D.N.Y., Dec. 27, 2013).

51）*ACLU v. NSA*, 438 F. Supp. 2d 754.

52）*Smith v. Maryland*, 442 U.S. 735.

53）*United States v. Jones*, 132 S.Ct. 945.

も、特定事件の捜査のために短期間特定個人の電話記録を収集したSmith v. Maryland判決と異なり、今回のケースでは、①約5年間という長期にわたり情報が収集されたこと、②通常、あらゆる電話会社が政府の情報収集に協力しているとは想定されないこと、③今回のケースでは何百万ものデータが収集されていること、④現在の政府は以前と比べてはるかに多くの情報を収集し解析できること、などの特徴があるからである。そのため、本件はハイテクを使って長期にわたり位置情報を収集したことが問題となったUnited States v. Jones判決に近い事案である。本件では、政府が違法行為の疑いがない者に対して個別の令状をとらずに5年間にわたり電話のメタデータを収集したことから、それはプライバシーの期待を侵害している。ゆえに、電話記録であっても第三者任意提供の法理は適用されず、プライバシー権侵害が認められるとした。

その上で判決は、本件捜査が修正4条に照らして正当であったか否かの判断に移り、政府利益と個人の権利との比較衡量を行う。政府の利益は当該情報収集によって将来のテロを防ぐことであるが、この情報収集によって差し迫った危険を実際に防ぐことができたという例を示していないため、その利益は疑わしい。一方で、原告らには長期間電話記録が収集されていないという、重要なプライバシーの期待があり、それが侵害されている。したがって、原告のプライバシーの利益は政府の情報収集の利益に勝り、本件情報収集は修正4条に反して違憲である。その結果、判決は、政府に対して電話のメタデータに関する情報収集を中止し、これまでに収集したデータを破棄しなければならないという命令を出した。

一方、ACLU v. Clapper判決は、本件においても第三者任意提供の法理を適用し、プライバシー権の侵害が認められないとした。なぜなら、第三者任意提供の法理により、原告は電話記録についてプライバシーを放棄していることになるからである。連邦最高裁はUnited States v. Jones判決においてGPSの取り付けが修正4条に違反するとしたが、Smith v. Maryland判決を覆さなかったので、第三者任意提供の法理はなお有効である。Smith v. Maryland判決が先例として生きている以上、第三者任意提供の法理が適用され、NSAの電話のメタデータの収集はプライバシー権を侵害しているとはいえないとした。

このように、一審レベルの下級審は当事者適格を認めた上で、実体的権利侵害の有無につき、第三者任意提供の法理を適用するか否かで判断を行っている。もし、当事者適格の問題を乗り越えることができるとすれば実体的権利の問題をどのように考えるべきかが主戦場となるが、判例法理にそって考えてみると、これがなかなかやっかいである。なぜなら、本件は刑事手続と行政手続の狭間にある問題であり、刑事手続上のプライバシー権の問題として判断するのか、情報プライバシー権の問題として判断するのかが定かではない。前者であれば下級審が判断したように合理的期待の有無と第三者任意提供の法理の問題が中心になり、後者であれば情報プライバシーに該当するかどうかの問題が争点となるように思われる。

前者が問題となった場合、たとえ第三者任意提供の法理が適用されるとしても、日々の電話記録が常に収集されるという事態は異常であり、通常、人々はそのような事態を想定していないことから、メインウェイ等はプライバシーの期待を侵害しているといえるのではないだろうか[54]。後者については、当該情報の性質や政府利益の重要性を考慮しながら、政府が当該情報の管理を適切に行っているかどうかを問うのがこれまでの判例法理のスタイルである[55]。電話記録という情報の性質とテロ対策に必要だとする政府の利益を考慮した場合、電話記録は単純個人情報にすぎないのに対し、テロ対策に必要だとする政府の利益はそれなりの重要性を有するので、情報収集自体は認められそうである。しかし、当該情報収集のテロ対策への有効性も抽象的すぎるきらいがあり、情報プライバシー権に当然に優先するとはいえないことから、続けて情報管理の適切性が問われることになろう。この点、今回の事件では情報が漏れているので、適切な管理が行われているとはいえないように思われる[56]。

そうなると、いずれにせよ、今回の事件はプライバシー権を侵害するという結論に至るのが自然なのではないだろうか。

---

54) ただし、修正4条に照らして捜査が合理的であったかどうかは別途判断される可能性がある。

55) *See, e.g.*, Whalen v. Roe, 429 U.S. 589 (1977); NASA v. Nelson, 131 S.Ct. 746 (2011).

56) 本来であれば、情報収集自体が問題であると思われるが、判例はなおプライバシー権の本質を私事の公開とみなしているので、判例法理にそって考える場合、管理の場面が争点になると考えられる。

後序――プライバシー計画

監視国家はただちに立憲主義を崩壊させるわけではないが、徐々に監視の目を広げながらそれを常態化していくところに、その怖さがある。そうした既成事実の積み重ねに対し、いつどのような疑問符を打てるかが、喫緊の課題である。状況が行き着くところまでいってしまうと、もはや取り返しがつかない可能性が高い。なぜなら、いったん創られた社会状況をそれ以前に戻すことは容易ではないからである。そうなる前に疑問を呈し、そこに潜む憲法問題を直視する必要がある。その時こそ、立憲主義が動揺していることにも気づくことができるのではないだろうか。眼前に広がるのは、膨脹を続ける執行府の姿と縮減し続ける自由空間であり、立憲主義が岐路に立たされていることを否応にも自覚せざるをえないからである。

ところが、それに抗うための術がすぐに見つかるわけでもない。プリズム計画はまさにその難しさを表す問題であった。これに対しては、何が問題なのかを吟味し、プライバシー権保護の計画を検討することがさしあたりの処方箋であると思われる。

監視国家がプライバシー権を侵害しているとすれば、立法府および司法府はそれに対応する責務がある[57]。実際、アメリカでは社会状況に応じて立法府と司法府のいずれかがプライバシー権保護を発展させてきたという経緯があるが、プリズム問題にみられるように、最近では双方ともにプライバシー権保護に追いついていない感がある。このとき、世論または政治に訴えて法律修正を促すか、裁判を通してプライバシー権の保護を勝ち取るか、という２つの方法がありうる。どちらの戦略を選ぶかは、その時々の事情を考えなければならない。政府の侵害行為に対して、司法救済の見込みはないが、立法的改善に期待が持てる場合、それは選挙を通して政治に改善を迫ることになる。一方、立法府に改善を期待できない場合、司法救済に頼るしかない。かつてブランダイス判事が主張したように、修正4条に基づくプライバシー権の保護は自由権的側面が強いことから本来司法が担うべき責務であるとすれば[58]、司法を動かす法理論を模索することになろうか。

あるいは、第3のアプローチとして、国家機関以外に目を向ける方法もありうる。その典型例が、カナダで提唱されたプライバシーバイデザイン（privacy by design）のように、民間企業に対応を迫るという方法である。これは、民間企業があらかじめプライバシー保護を埋め込んだ技術や組織の設計をすることの重要性を説くものであり、近年注目が集まっている。プリズム計画にみられるように、監視国家は民間企業を巻き込む形で進展しているが、それは逆に民間企業によるプライバシーの事前保護が有効であることを示唆しているといえる。企業は何らかの経済的インセンティブがなければこうした対応を行わないかもしれないが、企業が無断で政府に個人情報を提供した場合に裁判でプライバシー侵害が認められるようになれば、企業もプライバシー設計に重点を置くようになるかもしれない。これを懸念したからこそ、政府はFAAによって企業のプライバシー侵害の免責を認めることで、企業を抱きかかえようとしたわけである。よって、この点からも、司法がプライバシー権侵害を認めることの意義が潜在しているといえる。

すると、プリズム計画に対抗するプライバシー計画は、やはり司法を舞台にプライバシー権を確立していくことが目下の課題であるように思われる。このとき、当事者適格の壁を乗り越えるためにも、筋のいい事件を選んで訴訟を提起する弁護士の役割とそのための法理論を提供する学者の役割が求められることになろう。

かかるアメリカの状況は、決して他人事ではなく、日本でもすでに技術面および法令面において監視国家の基盤が整いつつある。そのため、アメリカの例を等閑視せず、あらためて監視国家がもたらす立憲主義への影響に刮目しなければならない。その際、他の精神的自由権と比べてプライバシー権については相応の保護を行ってきた日本の司法が今後いかなる展開を見せるのかが注目されるところである。

57）Marc Rothenberg and David Brody, *Protecting Privacy: The Role of the Courts and Congress*, 39 HUMAN RIGHTS 7, 10 (2013).

58）*Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

テロとアメリカ 第①回

アップル対FBI

会員・弁護士　井桁大介

2016年2月16日、アメリカ連邦地方裁判所がアップルにFBIへの捜査協力を命じました。その翌日、アップルCEOのティム・クックは長文のレターを自社のウェブサイトに載せ、この命令に異議を申し立てることを宣言しました[1]。それ以降この問題は法廷の内外で大変な議論を呼びました。本連載では今後数回にわたりアメリカのテロ対策の最前線をご報告する予定ですが、今回はその初回として、このアップル対FBIに関する議論をご紹介します。

事案の概要

2015年12月2日、カリフォルニア州サン・ベルナルディーノで14人が死亡する銃乱射事件が起きました。犯人はSyed Rizwan Farook とTashfeen Marikの夫妻で、事件後に車で逃走したものの警察との銃撃戦の末にいずれも射殺されました。FBIはイスラム過激派思想に感化されたホームグローンテロリストによるテロと断定し、彼らの背後関係を捜査しています。

FBIは彼らの事件前後の動向、特に立ち寄った場所と接触した人物に関する情報を収集するために、FarookのiPhone（5cモデル・iOS9）に残された情報にアクセスしようと試みました[2]。しかし、彼のデバイスにはパスコードがかけられていました。iPhone同モデルのセキュリティレベルは高く、ロックを解除するには対象端末にパスコードを打ち込む以外の方法はないとされていました[3]。アップルは顧客のパスコードを保存しない運用をとっており、死亡したFarook以外にパスコードを知るものはいません。捜査機関が解除するにはランダムにパスコードを打ち込んでいくしかありませんが、同モデルにはパスコードを4回打ち間違えると相当時間が経過しない限り再度の入力ができなくなる機能（時間延長機能）や、10回打ち間違えると自動的に端末内の全情報を削除するプログラム（自動消去機能）が組み込まれています（なお、自動消去機能は持ち主がオン／オフを設定できます。）。パスコードは4桁なので1万回試せば[4]いずれかの組み合わせがヒットするのですが、時間延長機能があるため4回目以降は大幅に時間がかかることとなり、また、自動消去機能がオンに設定されている可能性がある以上FBIとしてそのリスクを冒すことができません。

そこでFBIはAll Writs Act[5]に基づき、カリフォルニア州中央地区アメリカ連邦地方裁判所に対し、アップルに捜査協力を命令する令状を発令するよう申し立てました。同裁判所のSheri Pim令状裁判官は2016年2月16日にこの申し立てを認め、アップルに以下の捜査協力を命じました[6]。

1) 捜査官がFarookのiPhoneのデータにアクセスするため、合理的な技術援助を提供すること。
2) 前項における援助には、以下の3つの機能が含まれていなければならない。
   i. 自動消去機能の回避又は無効化
   ii. （手作業ではなく）電子的にパスコードを打ち込めるようにすること。
   iii.時間延長機能の無効化
3) 技術援助は、本体のOSやデータを改変せずに独自に作動するソフトウェアイメージファイルの提供が想定されるが、それに限らない。
4) 政府が同意する他の実現可能な手段を用いることもできる。
5) 費用負担については政府と協議すること。
6) データ管理の責任はアップルではなく捜査官にある。
7) 本命令により不合理な負担を課せられると考える場合は、本命令受領後5営業日以内に異議を述べること。

同月25日、アップルはこの命令に異議を申し立てました[7]。アップルの主張の骨子は、冒頭に紹介したティム・クックのメッセージに端的に整理されています。概要は以下のとおりです。

①スマートフォンには私的な会話、写真、金融情報、健康情報などが詰まっており、プライバシー保護の必要性が極めて高い[8]。
②今回のテロは許されるものではない。アップルはFBIに

---

1) http://www.apple.com/customer-letter/
2) 本来、スマートフォンの中身を見るには令状が必要となる。ライリー事件最高裁判決参照。 Riley v. California, 134 S. Ct. 2473（2014） http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf　本件ではFarookが死亡していた上、対象のスマートフォンが雇用主名義だったためその同意に基づき令状なく捜査された。雇用主の同意のみで従業員のスマートフォンの中身を捜索できるかは議論があるが本稿では取り扱わない。
3) 山下哲也『iPhoneロック解除をめぐる対立の意味』 2016.3.22 付けWEBRONZA, http://webronza.asahi.com/science/articles/2016031500004.html　なお本文で後述するとおり、FBIは後にそのセキュリティを破ることに成功する。
4) ブルートフォース（総当り攻撃）と呼ばれる。
5) 裁判所・裁判官は法を実現するために必要かつ相当な令状を発令できるというもの。全文は以下のとおり。
   (a)　The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.
   (b)　An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.
6) https://regmedia.co.uk/2016/02/17/apple_order.pdf
7) カリフォルニア州令状裁判官の決定に対し、カリフォルニア州地区連邦裁判所に異議を申し立てたもの。http://ja.scribd.com/doc/300626962/Patently-Apple-Apple-Motion-to-Vacate-Order-Compelling-Them-to-Assist-the-FBI-in-Searching-a-Seized-iPhone
8) スマートフォン（を初めとする携帯電話）に含まれるプライバシー情報の特殊性については、前掲注2ライリー事件参照。詳細は本文内で後述する。

対し情報や技術を可能な限り提供してきた。
③しかし今回の命令には応じられない。これはiPhoneのOSにバックドア（裏口）を設けるよう命じるものである。
④FBIは提供された技術をFarookのiPhoneにしか用いないと主張しているがそのような保証はない。バックドアの技術が知れわたれば、以後、別のiPhoneにも使われかねず、歯止めは利かない。iPhone利用者のプライバシーは致命的な危機にさらされる。

事件は異議審に係属し、アップルから詳細な主張書面が相次いで提出されたほか[9]、法学者、ACLUなどのNGO、コンピュータセキュリティの専門家、主要なテクノロジーカンパニー（マイクロソフト・グーグル・アマゾン・ヤフーなど）などによる多数のアミカスブリーフ（法廷助言書）が提出されました[10]。法廷の内外でプライバシー、テクノロジー、ナショナルセキュリティをめぐる最先端の議論が繰り広げられ、裁判所の判断が期待される中、口頭弁論は3月22日に予定されていましたが、直前になってFBIが審理の延期を申請。裁判所はこれを認め期日を4月4日に再設定しました。延期の理由としてFBIがアップルの助力なくセキュリティを破ることに成功したと報道されていましたが[11]、3月28日、報道されていたとおり、アップルの助力なく情報にアクセスできたことを理由に、FBIはAll Writs Actに基づく申し立てを取り下げ、審理は終結となりました[12]。

寸評

この事件はデジタルプライバシーの将来を占うものでした。取り下げという決着となったため司法判断は先送りとなりましたが、法律上の争点は今回の事件によっておおむね整理されたといえます。今回はその中から日本の法体系でも参考となる3つの論点を紹介します。

1 携帯電話のプライバシー

携帯電話、特にスマートフォンはプライバシーの概念を根底から変えた、というのがここ数年のアメリカの議論です。そのランドマークとなったのがライリー事件最高裁判決[13]です。この事件の争点は、逮捕時に押収した被疑者の携帯電話内部の情報を捜査機関が令状なしに見ることができるかというものでした。この判決では、以下のとおり現代における携帯電話の重要性が整理されています（結論として無令状捜索を否定）。

①現代の携帯電話、特にスマートフォンはミニコンピュータというべきであり、電話としてだけでなく、カメラ、ビデオプレーヤー、住所録、カレンダー、テープレコーダー、図書館、日記、アルバム、テレビ、地図、新聞などとして使われている。
②多くの人にとって生活必需品で、しかも常に携帯しているという特殊性がある。
③住所、私的なメモ、健康情報、銀行情報などの異なるタイプの詳細な情報が含まれていることがあるが、これらを組み合わせることで個々の情報単体では得られない情報が得られる。
④検索履歴も、例えば病気に関する検索など個人の私的な関心を明らかにする点で他の物件とは質的に異なる。
⑤保存される量も圧倒的に多い。家中に保存されている情報に勝るとも劣らない。
⑥さらにクラウド情報にアクセスできることを考えると、どこまでが携帯電話という物件に保存されている情報かの線引きも難しく、捜索の対象が無限定に広がりかねない。

特に以下の判示は、携帯電話がプライバシーの性質を一変させたことを端的に表したものとして話題になりました。

「政府は携帯電話のデジタルデータの捜索は他の有体物の中身を捜索することと実質的に区別できないと主張するが、これは馬に乗る旅行と月への旅行を区別できないと主張するようなものだ。いずれもA地点からB地点に行くという点では同じだが、それ以外にひとくくりに扱う理由はない。現代の携帯電話に対する捜索は、煙草入れや財布やカバンに対する捜索をはるかに超えたプライバシーへの懸念を伴うのだ」

ライリー判決以降、携帯電話のプライバシーの重要性を強調するいくつかの判決が下されています[14]。今回の技術協力命令は、このような時代の流れに真っ向から反するものとして議論を呼んだといえます。

2 セキュリティ対セキュリティ

今回の事件に関連し下院司法委員会[15]で行われた公聴会で証言したSusan Landau教授は、今回の事件を「セキュリティ対セキュリティ」の問題だと指摘しました[16]。すなわち、個別犯罪の捜査とサイバーテロの予防という2つのセキュリティの対立です[17]。教授によれば、今回の命令は個別事件の捜査というミクロのセキュリティを優先して、サイバー

9) 例えば、以下を参照。https://www.justsecurity.org/wp-content/uploads/2016/02/apple.motiontovacate.pdf
プライバシーの重要性を強調した上で、All Writs Act を今回の命令の根拠とすることの違法性や、今回の命令が修正1条や修正5条（デュープロセス条項）に反することなどが主張されている。
10) 一覧は以下を参照のこと。 http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html
11) 報道によるとFBIはかねてより世界中のハッカー、技術者から技術協力の申し出を受けていたようである。最終的にイスラエルのセキュリティ会社がFBIにアップルのセキュリティを無効化する技術を提供したとされている。
12) カリフォルニア州で令状が発令された数日後、ニューヨーク州ブルックリン地区連邦裁判所がAll Writs Actに基づく同じような捜査協力の申し立てを却下し、話題になった（http://www.nytimes.com/interactive/2016/02/29/technology/document-Orenstein-Order.html参照）。政府が却下決定に異議を申し立てたため、バックドアの是非に関する先例となる可能性を秘めていたが、最終的にこちらの事件でもFBIが独力でセキュリティ解除に成功し、事件は取り下げられた。なお、いずれの事件についても、スマートフォンを捜索した結果、何らかの有益な情報が入手されたとの報道には接していない。
13) 前掲注2
14) 例えば State of Maryland v. Kerron（2016）https://www.documentcloud.org/documents/2781646-1496s15.html
15) 公聴会の概要は以下を参照 https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/
16) 教授の証言録は以下を参照 https://judiciary.house.gov/wp-content/uploads/2016/02/Landau-Written-Testimony.pdf

セキュリティというマクロの問題を軽視した結果、2つの点で致命的な危険をもたらすとされています。1つは、本件のような捜査協力が常態化すれば、多数の無効化ソフトが作られることとなり、その一部が流出してサイバーネットワーク上に致命的な欠陥が生まれることとなる危険です。もう1つは、アメリカの裁判でアップルに命令できるという先例を作れば、必ず他国（特に専制国家）でも同様の命令が発令され、人権侵害や弾圧に使われるという点です。

サイバーセキュリティは、国家の安全保障にかかわる分野であっても、その大部分を民間企業に依存しています。アップルが最先端のセキュリティを開発したことは、サイバーテロの予防に大いに寄与する点で国家安全保障の見地からも称揚されるべきことであり、捜査協力の拒絶を捜査妨害と非難するなど時代錯誤だと批判されているのです[18]。

3　227年前の法律を適用することの是非が投げかける極めて現代的な問題

本件では、捜査機関が携帯電話の情報にアクセスできるという実体法の問題には争いがなく（前掲注2参照）、議論されているのはその手法としてアップルに捜査協力を命令するという手続が許されるかという問題です。そこで出てきたのがAll Writs Actの適用の是非という法律問題です。

All Writs Actは1789年に成立したもので、初代大統領のワシントンが署名した最古の法律の一つです。一部の論考では227年前に成立した古めかしい法律が不当に使われたと指摘されていましたが、埃をかぶって死文化していた法律が突然持ち出されたわけでは決してありません。実際、ACLUが公刊情報から整理しただけでも、2008年以降現在までにアップルとグーグルに対し合計で63件の捜査協力命令がAll Writs Actに基づき認められています[19]。

All Writs Actは、司法府が非定型的な命令を発付できるとする法律です。法律で定められていない捜査手法を創設できるため、これまでも最先端のテクノロジーを用いる捜査の根拠として使われてきました。

しかし、All Writs Actに基づく捜査手法の創設を無制約に認めると、大きな問題が生じるとACLUなどは批判しています。例えば、ある最先端の捜査手法を認めるとプライバシーの侵害やサイバーセキュリティの弱体化が予想されるため、議会は充実した議論の結果法律の制定を控えると決定していたにもかかわらず、1人の裁判官が捜査機関の要請を受けて数日のうちに全く新しい捜査手法を認めることができてよいのかという問題です。

このようにAll Writs Actの適用の是非は、単なる手続法の問題にとどまりません。新しい捜査手法の導入の是非という、ときには国の行く末を左右しかねない問題を、個別事件における司法の判断のみにゆだねて良いのか。それこそが今回の究極の問題です。このように考えると、この問題が決して227年前の古めかしい法律の解釈に関するマニアックな議論ではないことがお分かりになるかと思います[20]。国際化が進み、テクノロジーが進化し、数年で社会構造ががらりと変わる現代において、その国のあり方を決めるのは誰かという、重大な議論が潜んでいるのです。

結び

ライリー事件の補足意見でAlito判事は、携帯電話のプライバシーの問題は議会で決着させるのが望ましいと述べました。上述のとおり2016年3月1日には下院の司法委員会で本件に関する公聴会が開かれ、FBI長官、アップルの代理人、著名な学者、そして地元警察の代表者がそれぞれの立場からこの問題について証言するなど、議論はその舞台を立法府に移しつつあります。

例え別の新たな事件において、All Writs Actによるiphoneのセキュリティ無効化が裁判所により認められたとしても、そこで議論が終わるわけではありません。その判断を先例として政府・捜査機関がさらなる協力をアップルやグーグルなどに求めてくることは必至です[21]。司法がいかなる判断を下そうとも、社会の変化に即応した立法の重要性はいささかも揺らがないのです。

9.11以降、アメリカ政府はテロ対策を強化し、近年のテクノロジーの進歩にあわせてその捜査手法も進化しています。捜査機関のテクノロジーの利用を議会はどこまで制御すべきか。議会が果たすべき役割は高まるばかりです。次回は、9.11以降アメリカ議会が果たしてきた役割、すなわちテロ対策関連の立法過程を整理し、現在繰り広げられている最新の議論を紹介したいと思います。

17）現代において、サイバーセキュリティは国家安全保障の見地から極めて重要である。実際、ここ数年の間に、中国、ロシア、イランの各政府に支援された組織が、米国の政府機関や企業、法律事務所などに対し、知的財産を狙った大規模なサイバーテロを仕掛けていたことが明らかとなった。中国によるサイバー攻撃の実情は、例えば以下を参照　https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
また、ロシア政府によるウクライナの発電所に対するサイバー攻撃を生々しくレポートするものとして、https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

18）サイバーネットワークは免疫システムに例えられる。一部の細胞がやられても、免疫細胞が機能していれば、全体の健康は保たれる。アップルなどのテクノロジー企業は定期的にバグを修正し、顧客にソフトウェアアップデートを促して、全体のセキュリティを維持している。LawFareの以下の記事は、バックドアが横行すれば、顧客がアップルから送られてくるアップデートを信用せず、結果としてシステム全体が脆弱になる危険があると指摘している。https://www.lawfareblog.com/be-careful-what-you-wish-device-hacking-and-law

19）https://www.aclu.org/blog/speak-freely/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone

20）この問題について先例的価値を有するのがNew York State v. New York Telephone Company（1977）判決である。賭博事件の捜査に関し、電話の発信先番号を自動的に記録するペンレジスターという装置の設置許可を裁判所に求め、裁判所がAll Writs Actに基づき電話会社に当該装置の設置等に関する協力を命じた。最高裁判所はこの判断を是認した。この判決はAll Writs Actの適用の可否に関し4つの要件を定立したとされている。本件との関係で重要な要件は、「議会の（明示または暗黙の）容認」という要件であり、議会が行政の当該捜査を実質的に容認しているという状況が必要だと考えられている。
本件で捜査機関側はこの要件に関し、FarookのiPhoneの内部情報の捜索自体は実体法で許容されているから、その内部の情報を見るための技術協力をアップルに命じることを議会は容認していると考えるべきだとしてこの判例の射程が及ぶと主張している。これに対しアップルやACLUは要件を満たさないと主張している。例えばACLUはそのアミカスブリーフにおいて、以前行政府にモバイルデバイスの製造元に対するデバイスのセキュリティを解除するよう命令する権限を与えるか否かが議論された際、議会はその権限の付与を注意深く避けてきたことを指摘している。すなわち、ここ数年、政府がアップル等のテクノロジーカンパニーにバックドアの設置を命じるための法律を制定するよう求めてきたが、議会はこれを退けてきた経緯があるわけである。さらにACLUは、1994年に制定されたCommunications Assistance for Law Enforcement Actという法律において、通信会社には捜査協力を命じることができる旨の条項が盛り込まれたものの、アップル等の情報サービス会社はその対象から除外された立法経緯があることや、近年FBIなどがアップル等の情報サービス会社もこの法律の対象とするよう働きかけてきたが、議会がこれを拒絶してきたことなどを紹介している。このように、アップル等に捜査協力を命じる法律を制定する十分な機会と時間がありながら議会がそれを拒絶してきたにもかかわらず、司法が令状を発付することは、All Writs Actの精神に反し許されないと強調している。

21）対象デバイスのすべての操作を覗き見るソフトの埋め込みや、位置情報を自動的に送信する機能の設置などが予想される。

テロとアメリカ 第②回

テロ法制の過去と現在 前編

会員・弁護士 井桁 大介

前回は、アップル対米連邦捜査局（FBI）を題材にアメリカのテロ対策の現状をご紹介しました。今回は次号と2回に分けて（予定）、テロ対策法制の概略をご紹介します。

アメリカのテロ法制の歴史は、第二次大戦後すぐの黎明期を除くと、（1）1970年代後半から80年代の勃興期、（2）2001年の「9.11」以降のパニック的拡大期、（3）2013年6月のスノーデンリーク以降の見直し期の3つの時期に分けることができます。今号では、テロ対策法制の基礎的な枠組みが確立された勃興期に焦点を絞ってご紹介しつつ、拡大期と見直し期の議論状況の概略を整理し、次号において拡大期と見直し期における法令の具体的な改定内容をご紹介します。

（会員・弁護士 井桁 大介）

勃興期―1970年代から80年代にかけて

この勃興期にテロ対策法制の中核を占める重要な3つの法律、すなわち盗聴法（Title Ⅲ of the Omnibus Crime Control and Safe Street Act）、FISA（Foreign Intelligence Surveillance Act）、ECPA（Electronic Communication Privacy Act）が制定されました。また、大統領令（Executive Order）12333号という重要な命令が発令されたのもこの時期です。以下、順を追ってそれぞれの特徴などをご紹介します。各法令の守備範囲が、特定の事件に関する事後的な捜査（犯罪捜査）なのか、それとも犯罪予防的な諜報活動（インテリジェンス活動）なのかを念頭に置きながら読み進めていただくと理解しやすいかと思います。

盗聴法制定のきっかけとその特徴

1965年2月にFBIが、違法なギャンブル行為のやりとりを盗聴するために、被疑者のKatz氏が利用する公衆電話に特殊な装置を付けて胴元との通話を傍受し、その内容を証拠として起訴した事件がありました。連邦最高裁は1967年に、無令状で行われる盗聴は合衆国憲法修正4条[1]に違反するとして原審を破棄して差し戻しました（Katz判決）。この判決をきっかけとして、盗聴捜査の要件等を法定する必要が高まり、1968年に盗聴法が制定されました。

この法律は、国内における犯罪捜査において、合理的な理由があるときに令状に基づく盗聴を認めるものです。政府の転覆をはかる明白かつ現在の危険がある場合など無令状盗聴が許される場合をいくつか定めていましたが、インテリジェンス活動、とりわけ国家の安全保障（ナショナル・セキュリティ）のために必要と考えられる盗聴捜査に関しても令状が必要か否かについては、言及していませんでした。この点がFISA制定のきっかけとなります。

留学の風景：第二次世界大戦期のアメリカにおける、日系人の強制収容の不当性を訴えたミノル・ヤスイ氏の胸像横で息子とともに（デンバーにて筆者）

FISA制定のきっかけとその特徴

1969年の晩秋、前年に起きたCIA施設の爆破事件に関して3名が逮捕、起訴されました。被告人のうちの1人は、政府が被告人らの電子的な情報を無令状で監視していたと主張して該当する証拠の開示を求めたところ、政府は国家の安全保障（ナショナル・セキュリティ）の見地から本件では無令状でも監視が許されると主張して開示を拒絶しました。これにより、ナショナル・セキュリティのための監視であれば無令状での盗聴（電子的情報を含む）が許されるのか否かが争われました。

1） “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” （不合理な捜索及び逮捕・押収から、その身体・家屋・書類及び所有物の安全を保障される人民の権利は、これを侵してはならない。宣誓または確約によって証拠づけられた相当の理由に基づくものであって、捜索すべき場所及び逮捕すべき人または押収すべき物件を特定して記載するものでなければ、いかなる令状も発してはならない。）

1972年、連邦最高裁は、国家内部のナショナル・セキュリティに関する捜査[2]については、通常の犯罪捜査と同じく無令状の盗聴は許されないと判示しました。他方で、国外から脅かされるナショナル・セキュリティの監視捜査に関しては当該判決の射程外であり[3]、裁判所が適用するべきルールが議会において作られるべきだと判示しました（Keith判決）。

この裁判所の示唆を受けて制定されたのがFISAという名称の、対外的なインテリジェンス活動における電子的な監視捜査[4]を規律した基礎法です。特徴は3つあり、目的、対象、そして手続のそれぞれについて独特の規律が定められています。

第1に、捜査の主要な目的が対外の諜報活動である場合に限られます。つまり犯罪捜査目的の場合には適用されません。また国内の諜報活動も同様です。この帰結として、FISAに基づいて集められた電子情報は、一定な要件を満たさなければ犯罪捜査に転用できません（いわゆるMinimization規制）。

第2に、捜査の対象は、外国の機関またはそのエージェント（平たく言えばスパイ）の電子的な通信情報に限られます。

第3に、捜査の要件は、実体要件・手続要件ともに、通常の犯罪捜査と異なります。まず実体要件として、通常の犯罪捜査の場合にはいわゆる罪を犯したことを疑うに足りる相当な理由（Probable Cause）が必要ですが、FISAに基づく令状の場合は、対象が外国のスパイであることの相当の理由で足ります。

また、令状を発令するのは通常の裁判所ではありません。FISAに基づいて特別に設置されたFISC（Foreign Intelligence Surveillance Court）[5]です。申請内容に明らかな誤りがない場合を除き令状が発令されるうえ[6]、事前・事後を問わず令状の内容は対象者を含む第三者に公開されません。議会の特別委員会に対する年次の報告やその監督があるとはいえ、事後の検証は困難な構造となっています。

ECPA制定のきっかけとその特徴

ECPAは、盗聴法とFISAが対象としていない領域、すなわち、犯罪捜査目的で電子通信を傍受する捜査領域を規律した法律です。1986年に盗聴法の条文を加筆・修正する形で制定されました。

ECPAの最大の特徴は、通信そのものを傍受する捜査と保存された通信内容にアクセスする捜査を区別した点です。つまり電子メールを送受信の段階で傍受することには厳格な規制を求めた一方、一度送受信され、プロバイダのサーバに保存されたメールについては、緩やかな要件で取得できることとされました。

この区分には1979年のSmith判決が大きく影響しています。連邦最高裁は、電話内容の盗聴には令状が必要（Katz判決・盗聴法参照）だが、電話をいつ、どこで、だれがだれに対して架電したかという情報（いわゆるメタデータ）については、第三者である電話会社が当然にアクセスできる情報である以上、厳格な保護の対象とはならないと判示しました。これはいわゆるサードパーティードクトリンと呼ばれるもので、第三者のアクセスを前提とする情報についてはプライバシーの保護が原則として及ばないとする判例法理となっていきます。この判決は電話に関するものでしたが、これを電子情報にも拡大したのがECPAです。ECPAにより、捜査機関が保存された電子情報を取得するには、通常の犯罪捜査令状よりも要件が緩やかなECPA令状を取得すればよいこととなりました。例えば電子メールについては、プロバイダのサーバに保存されてから180日以上経過したものは原則として警察が自由にアクセスできる立て付けとなっています。これは制定当時には電子メールをプロバイダにおいて長期間保存することが想定されていなかったためといわれています。

大統領令12333号の特徴

盗聴法やFISAの理念に基づき、国内における通信は、外国人同士の通信であれ令状主義が適用されます。国外のアメリカ人の通信も同様です。大統領令12333号は、盗聴法やFISAの対象外である、在外の外国人の通信についてのルールを定めたものです。

2) 判決では“the domestic aspects of national security”と表現されています。
3) 判決では、“express no opinion as to [the surveillance of the] activities of foreign powers or their agents”と表現されています。
4) 当時は電子メールが念頭に置かれていましたが、後にその対象が広がっていきます。
5) 構成員は全国の連邦地裁から特別に選任された裁判官です。
6) そのため却下は極めて困難です。1979年から2006年に申請された22990件中、却下されたのはわずかに5件と報告されています（https://epic.org/privacy/surveillance/fisa/stats/default.html）。

第1に目的は、相手国の電子監視に対抗するものに限定されます。第2に対象となる情報の種類に限定はありません。メタデータであれ通信内容であれ、電話内容であれ電子情報であれ、包括的に取得が可能です。第3に要件ですが、裁判所のチェックは必要ありません。担当の行政局が事前に設定した手続に即していて、かつ政府のAttorney Generalの認証があれば、監視が認められます。議会に対する事後の報告も必要とされておらず、基本的に政府内部で完結する仕組みとなっています。

小括

駆け足でご紹介してきましたが、この3つの法律と1つの大統領令がテロ対策に用いられる情報収集活動の基本的な枠組みとなります。

改めて概要を整理すると以下のとおりです。

	盗聴法	FISA	ECPA	EO12333
目的	犯罪捜査	ナショナル・セキュリティ	犯罪捜査	外国からの電子監視への対抗
対象	通話内容	電子情報	メタデータ	すべて
手続	令状	FISC	裁判所命令	AG認証
関連情報	Katz判決	Keith判決	Smith判決 第三者法理	

次号に向けて―9.11以後の展開とスノーデンリークによる見直しの概略

これらの法令は、9.11以後、イスラム過激派とのテロ対策活動に活用するべく、様々な改定や解釈の拡大がなされていきました。そしてスノーデンリークによってその全貌が明らかとなり、様々な批判が巻き起こりました。詳細は次号においてご紹介しますが、以下の4点がとりわけ重要です。

第1に、FISAに基づく大量監視です。FISCや議会の監督が十分に機能せず、ほぼすべての申請が認証され、事後の是正も乏しかったため、諜報機関の電子監視が拡大の一途をたどりました。テロと無関係な数兆のメール、電子情報、電話のメタデータなどが取得されており、アメリカ人のプライバシーの意識を根底から揺さぶることとなりました。

第2に、ECPAが依拠する第三者法理です。メールやアプリなどの利用において、守秘義務を負う取扱業者がサービスの保守・運営に必要な範囲で情報にアクセスできることと、捜査機関がその情報を自由に利用できるとすることは、プライバシーの制約の程度が全く異なるはずです。特に電子情報の利用が不可欠な現代においては見直しが急務とされています。

第3に、大統領令12333の拡大解釈の問題です。海外の要人の携帯電話の盗聴や、海外のサーバに保存されたあらゆる電子情報を監視していたことが大規模な批判を巻き起こしたことは記憶に新しいと思います。イスラム過激派との戦いにおいては、あらゆる監視が相手勢力の電子監視に対抗する、という名目が成り立つため、在外の外国人に関する情報でありさえすればあらゆる情報を監視することが正当化されてしまいます。さらにイギリスの諜報機関と協力し、アメリカはアメリカ国外の情報を、イギリスはイギリス国外の情報を収集し、相互に共有することで、ほとんどの国内法規制を脱法できてしまいます。このように、国外の外国人であれば一切の保障を及ぼさないという制度設計自体に深刻な問題がはらんでいることが明らかとなりました。

第4に、Incidentallyという言葉の独り歩きです。FISAに基づいて収集される情報は、原則として外国のAgentの通話内容ですが、通話の相手方がアメリカ人である場合も当然に予想されます。FISAは当初からアメリカ人を対象とした監視は許容していませんが、外国人を対象とした通信の相手方が意図せずにアメリカ人である場合には[7]、取得した情報を保存・利用してよいという立て付けをとっています。これは大統領令12333でも基本的に同様です。すなわち意図せず入手した場合には、仮にその通信の相手方がアメリカ人であっても、破棄する必要はなく、諜報活動に用いることができます。当初のFISAの制度設計の場合には大きな問題とはならなかったのですが、後にFISAが改正され、情報収集の対象が、Agentのみならず何らかの協力者であればよくなったために、一気に範囲が拡大され、事実上対象者の規制が外れてしまいました。いわば、IncidentallyとFISAおよび大統領令12333の合わせ技により、膨大なアメリカ人に関する電子情報の収集・保存が実現したわけです。

次号まで少し時間が空きますが、これら4つの問題意識をご記憶いただければ幸いです。

7)　相手がアメリカ人であることを事前に知りつつ意図的に監視した場合はこの限りではありません。

テロとアメリカ 第3回

テロ法制の過去と現在 中編

会員・弁護士 井桁 大介

前号よりお送りするアメリカ・テロ法制の過去と現在。前回は、テロ対策法制の基礎法ともいうべき盗聴法、FISA及びECPAの概略を紹介しました。

本号では、USA Patriot Act（いわゆる愛国者法）とFISA2008年改正という、9.11以降に制定された2つの重要な法律を紹介します。 （会員・弁護士 井桁大介）

USA Patriot Act

この法律は9.11のわずか8日後に議会に法案が提出され、10月26日にブッシュ大統領の署名を経て成立しました。正式名称はUniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2011ですが、一般に頭文字をとってUSA Patriot Actと呼ばれます。350ページに及ぶ膨大な法律であり、161の章に分かれて16の異なるテーマを取り扱っています。

テロ捜査権限を拡大した法律という印象の強い法律ですが、実際にはそれ以外の内容も数多く含まれています。例えば移民の被害者を対象とする特別の在留許可制度や遺族を対象とする支援基金の創設といった9.11テロの被害者支援を目的とする規定、テロ容疑者を拘束する場合の期間制限の短縮（従前の6週間から7日）といった捜査機関の権限を制限する方向の規定も盛り込まれました[1]。さらに、捜査機関の予算の拡充やデータベースのアップグレード、CIAとFBIの協力体制の構築といった、テロ対策にとって有益でありながら、市民の権利を制限することのない対策も取られています。

とはいえ、この法律を有名にしたのはやはり、市民の権利と引き換えに捜査権限が拡充された条項です。ここではそのうち4つの重要な条文を紹介します[2]。

213条ー秘密捜索

建物の捜索をする際には、原則としてドアをノックし事前に令状を見せる必要があります。従来から判例法により、麻薬事犯などで令状の効果を損ねてしまう特殊なケースに限って、例外的にドアのノックや令状の提示を不要とする秘密捜索が許されていましたが、その要件は秘密捜索が「不可欠な場合（essential）」、「必要な場合（necessary）」、またはそうすべき「合理的な理由（good reason）」がある場合に限られていました。

213条は、この要件を「令状の効果を損ねるかもしれない（may have an adverse result）」場合と大幅に緩和し、さらに事後的に捜査の事実を通知するまでの期間をそれまでの原則7日から「合理的な期間（reasonable period）」でよいとしました[3]。秘密捜索の要件を大幅に緩めたわけです。

この規定の最大の問題点は、テロ対策として盛り込まれたにもかかわらず、対象がテロ捜査に限定されていない点です。捜査目的や対象犯罪などに何らの制限も課せられていないため、例え軽犯罪であっても適用が可能となっているのです。

そもそも9.11の以前から、国際テロ対策のためであればFISAによって秘密捜索がかなり広範に認められていたため、この法改正によるテロ対策の効果はほとんどないとされていました。

実際、2006年から2009年までに、213条に基づき1755件の秘密捜索が実施されましたが、そのうちテロ捜査の件数はわずか15件、割合にして0．8％にとどまり、残る大半は麻薬捜査や詐欺事件に利用されています。

このように213条は、テロ対策として導入されたにもかかわらず、テロ対策としてはほとんど効果がないことが実証された、いわば焼け太りの典型として強い批判にさらされています。

214条と216条ー電子メールのペンレジスター

ペンレジスターとは、電話の発着信の番号を記録する装置のことで[4]、いわゆるメタデータ[5]の収集を目的とする監視捜査の一つです。

改正以前から、捜査機関は、対象とする回線がテロ活動に用いられている恐れがあるなど限られた場合に、FISAで定められた手続の下、FISC（Foreign Intelligence Surveillance Court）の令状を受けた上で、当該回線のメタデータを収集することができました（同法402条）[6]。

---

1) ただし、後に例外規定が原則化することで期間制限は有名無実化しました。
2) そのほか、テロ団体を支援する幅広い活動を刑法犯としたいわゆるマテリアルサポート条項（805条）のように、表現の自由や弁護活動と緊張関係にある法改正もなされています。
3) 7日以内という原則は維持されていますが、以前よりもかなり頻繁に延長されるようになっています。また従前は延長は7日が限度とされていましたが、改正後は事後通知が90日後になったケースや、起訴に至るまで知らされなかったケースなどが出ています。
4) 正確には、対象とする電話番号を基準として、かけた先の番号を記録するものをペンレジスター、かかってきた番号を記録する装置をトラップ／トレースと呼びますが、本稿では両者を合わせてペンレジスターと呼びます。
5) いつ、どこで、だれがだれに対して、どれくらいの時間電話を掛けたかに関する情報。電話内容（コンテンツ）の対概念。
6) 対象の回線が国際テロ活動に関するものや、外国勢力のエージェントが関与するものであると信じるに足りる理由があることが要件とされていました。なお、前号で紹介したとおり、1979年のスミス判決によって、そもそも電話会社が保有する顧客のメタデータは修正4条の保障を受けないとされており、通常の犯罪捜査においても電話内容の盗聴に比して緩やかに取得が許されています。具体的には、当該取得されうる情報が進行中の犯罪捜査と関連していれば足りる（the information likely to be obtained…is relevant to an ongoing criminal investigation）とされています。

214条はこの要件を大幅に緩和し、対象の回線が誰のものかに関係なく、捜査目的が国際テロや秘密の諜報活動を予防することでさえあればデータ収集を許可しました。また、216条は、メタデータを取得できる範囲を、電話回線からEメールや検索履歴などのインターネット上の通信履歴についても広げました。

この検索履歴に関する情報の収集については、電話の相手方に関する情報と比して、プライバシーの程度は相当にセンシティブであり、図書館の貸出記録の収集に比肩するような思想調査が可能となるとして批判されています。

他方で、この改正により、政府は収集した情報の詳細を記録し、一定期間経過後に裁判所に提出することが義務付けられています。またFISCの令状は引き続き要件とされています。スミス判決が打ち出した第三者原則（third party doctrine）をそのまま適用すれば、かなり緩やかに収集することが許されていた情報に関して、法律によって一定の手続を要件としたことをとらえ、この条項はインターネット上のプライバシー権の保護を高めたと肯定的に捉える研究者もおり、評価は分かれています。

215条ーあらゆる有体物の取得

FBIは、Patriot Act以前から、FISCの許可の下、ホテル、レンタカー会社、倉庫会社といった限られた業種の企業から「業務文書（business record）」を入手することが許されていました（FISA501条）[7]。

この従前の規定の対象とする業種の限定を取り除き、かつ取得の対象を「業務文書」から「あらゆる有体物（any tangible things）」に広げたのが215条です[8]。

同規定により手続的要件も緩和されました。従前は、捜査の対象が「国外の勢力あるいはそのエージェント（foreign power or the agent of a foreign power）」であることを「信じるに足りる特定かつ具体的な事実（specific articulable facts giving reason to believe）」が必要でしたが、改正により、捜査目的が諜報活動であるか、または国際テロもしくは秘密の諜報活動を予防することでさえあれば、原則としてあらゆる情報を取得できることとなりました[9]。つまり、テロと全く関係のない市民であっても、情報収集の対象となるわけです。

このように広範な資料を緩やかな要件で収集できることを許すため、この条文は、思想調査に用いられる可能性を揶揄して、しばしば図書館条項（Library records provision）と呼ばれます。

さらに、215条による情報収集には、原則としていわゆる猿轡命令（gag order）が付されており、情報収集の対象者は提出命令の存在を公表することができません[10]。また異議申立手続は原則として非公開で行われます[11]。そのため、FBIがいつ、どの会社に対し、どのような種類の資料の提出を求めたかが公にされることがほとんどありません[12]。

このような特徴から、215条はスノーデンリークの以前から、市民の権利を不当に制限する条項として厳しい批判の対象となっていました。

505条ーNational Security Letterの拡充

National Security Letterとは、裁判所の判断を経ることなく政府・捜査機関の判断のみで発することのできるサピーナ（Subpoena）により、特定の業者[13]に対し、保管する個人情報の提出を求める制度です[14]。利用はテロ捜査に限られており、通常の犯罪捜査に用いることはできません。

505条の特徴は、取得できる情報の範囲を大幅に広げた点にあります。従前はスパイの疑いがある個人の情報に限られていましたが、505条により対象の限定が外され、進行中のテロ捜査と「関連する（relevant）」ものであれば、いかなる個人の情報であっても収集できるようになりました。テロ活動やスパイ活動はおろか、犯罪と全く関係のないアメリカ市民に関するものであっても、個人情報が取得されます。

また、猿轡命令を付すことができ、実際にほとんどのケースに付されています。そのため、特別な情報公開訴訟などを除き、命令の存在が公になることはほとんどありません。また、情報公開訴訟を経ても、内容は黒塗りで提出され全く明らかにされないのが実情です。

報道などによると、これまでに毎年3万通以上が発せられているとも[15]、2003年から2006年の合計で20万件以上が発せられているともいわれています[16]。かなり緩やかに犯罪と無縁の市民の通信情報が取得されているうえ、監督制度がほとんど設けられていないことから、Patriot Actで最も問題のある条項と批判されることもあります[17]。

---

7) なお、明文上、215条に基づく捜査が許されるのはFBIのみです。次号で紹介するとおり、スノーデンリークによって、NSAが独自に215条に基づく監視捜査を実施していることが明かとなり、これは違法の疑いが強いと批判されています。
8) 法改正以前より、裁判所の命令状に基づき、特定の事件の捜査のためであれば、あらゆる物品（any books, papers, documents, data, or other objects）の提出を命じることができました。元々命令状の取得要件はかなり緩かなものであったので、215条の利用が具体的な諜報活動の防止などに限定されていれば、新たに広げられる対象は合理的な範囲にとどめられたかもしれません。しかし、215条が事件との結びつきや特定性の要件を取り払い、対象の選定を事実上政府に一任した結果、後述のとおり、その対象は極限まで広げられていきました。
9) 条文上の例外は、表現の自由や信教の自由を保障する修正1条によって保障される活動に依拠して、対象を選定してはならないということのみです。
10) Section 215, (d)
11) 同(f), (5)
12) 猿轡条項が合理的とされる領域に盗聴法制があります。命令を受けた電話会社などが令状の存在を明らかにしてしまうと、盗聴捜査の効果が致命的に損なわれてしまうためです。しかし、215条に関しては、対象の有体物が収集された後であれば捜査の効果は損なわれる恐れがなく、対象者に猿轡をはめる必要性は乏しいとされています。実際、通常の捜査活動では、捜査を受けた当事者や第三者は、修正1条の表現の自由の保障の下、原則として自由に捜査内容について語ることができます（もちろん重要な捜査情報を被疑者に伝えて逃亡を容易にした場合などは、共犯規定などで処罰されます。）。そのため、一律に猿轡をはめる215条は厳しく批判されています。
13) 金融機関、電話会社やインターネットサービスプロバイダ、信用情報保有会社に限られています。
14) 日本の捜査関係事項照会（刑事訴訟法197条2項）との比較でいうと、捜査機関自身が裁判所などの第三者の判断を経ることなく報告を求めることができるという点で共通しますが、National Security LetterはNational Securityに関する事項に限られている点、提出を拒絶した場合に罰則が設けられている点、対象の業者が限られている点など、相違点は数多くあります。
15) blog.librarylaw.com/librarylaw/files/McDermott505Chart.doc
16) http://www.washingtonpost.com/wp-dyn/content/article/2008/03/13/AR2008031302277.html
17) 違憲性をめぐるいくつかの訴訟が提訴され、2011年、サンフランシスコ連邦地裁において、この規定を違憲とする判決が出されました。政府が控訴し連邦高裁で争われていましたが、2015年6月にUSA FREEDOM Act（次号で詳述）が制定され505条についても改正がなされたため、連邦高裁は改正後の505条について改めて憲法判断をするよう事件を連邦地裁に差し戻しました。2016年3月、連邦地裁は改正によって違憲性は払しょくされたとして合憲判断を下しました（In re: National Security Letter 2011（11-2173）。 https://www.eff.org/cases/re-matter-2011-national-security-letter参照）。

FISA2008年改正法（FAA）

9.11以後の法改正のうち、支持派と批判派の間で最も激しい議論がかわされているのがこの法律です。なかでも702条は、それまでのFISAの枠組みを根底から変容させるものとして、象徴的な意味を与えられています。

正式名称を50 U.S. Code §1881 a - Procedures for targeting certain persons outside the United States other than United States Personsとするこの法律は、FAA（FISA Amendment Act）と呼ばれることもあります。その名のとおりFISAを改正し、701条から707条を新設する法律です。

その最大の特徴は、電話であれインターネット上の通信であれ、通信内容（コンテンツ）そのものを、裁判所の個別の判断なく収集することを認めたことにあります[18]。これは、裁判所の令状がなければ通信内容が収集されることはないという伝統的な考え方[19]を覆すものでした。

条文の構造は複雑ですが、一言で言えば、事前規制型から事後監督型とし、より機動的な監視捜査をできるようにしたものといえます。

第1に、従前は、通信の当事者の一方が外国の勢力またはそのエージェントである「相当の理由（Probable Cause）」が必要とされていましたが、FAAでは、一方当事者が国外に住む外国人でありさえすれば、通信内容を取得できることとなりました。通信の一方当事者がアメリカ人であったり、アメリカ国内にいることを事前に知っていた場合には、監視は許されません。外国の諜報（foreign intelligence）目的という縛りは残されたものの、従前よりも格段に対象が広げられることとなりました。

第2に、従前は、監視捜査の前にFISCの特別な令状を取得する必要がありましたが、FAAでは裁判所の事前の許可は必要ありません。政府内部の監督機関[20]の認証のみで、監視捜査を実施することができます。

第3に、事後監督制度が拡充されました。政府内部の監督機関は、通信の当事者がアメリカ人であることが事後的に明らかになった場合には、傍受の中止を命令したり、諜報活動とは無関係な傍受内容を廃棄しなければならないことが明文で定められました。そのほか、いくつかの政府内部の監督機関が、半年に一度、あるいは一年に一度、議会やFISCに報告書などを提出することが義務付けられています[21]。

この法律は制定以前から研究者の間でも評価が分かれていました。支持派は、現代のテロ対策のためには機動的な通信傍受が不可欠だと主張します[22]。また、冷戦時に制定されたFISAの想定敵国は共産主義国であり、盗聴の対象がスパイであることの「相当の理由」を明らかにすることは比較的容易でしたが、9.11以後の仮想敵は、国家とはいいがたい団体となり、例えばアルカイダの構成員であることや、ISの信奉者であることなどについて事前に「相当の理由」を明らかにすることは容易ではなく、構成員である「相当の理由」が明らかとなったときにはすでにテロの危険が目前に迫っており、令状を取っている暇がないと主張しています。従来の仕組みが機能しなくなっていたわけです。さらに、国外にいる外国人については、原則としてアメリカ合衆国憲法の保障が及ばないとされていることも、支持派の後押しとなりました。このような議論を経て、最終的に支持派が勝利を収めてFAAは議会を通過しました。

しかし、次号において詳述するように、2013年のスノーデンリークによって、NSAをはじめとする政府の捜査機関が、法律の当初の想定を超えて膨大な通信情報を収集していることが明らかとなりました。以降、批判派の巻き返しが強くなり、再び活発な議論が繰り広げられています。

本号のまとめと次号の予告

これまで述べてきた9.11以降の法改正を整理すると以下のようになります。

	213条	214条・216条	215条	505条	702条
目的	犯罪捜査	F.I.	F.I.	F.I.	F.I.
概要	秘密捜索	メールやネット履歴のメタデータ	あらゆる有体物の収集	特定の業者が保有する個人情報の収集	通信内容の傍受
手続	令状	FISC令状	FISC令状	サピーナ（Subpoena）	政府内部の監督機関の認証
特徴	テロ対策に役立っていない	Smith判決よりも保護を高めたとして肯定的な評価も	図書館条項。きわめて広範な監視権限	通信業者などが保有するメタデータを独自に収集	裁判所の事前審査なく、通信内容の収集を認めた初めての法律

F.I.: foreign intelligence

これらの法改正によって実際に政府がどのような監視捜査を実施しているかは、猿轡条項などの適用と相まって、厚いベールに包まれていました。そのベールを劇的に暴いたのが、スノーデンリークです。

次号では、スノーデンリークによって明らかとなったアメリカ政府の監視捜査の概要を紹介するとともに、リーク以後に繰り広げられている現在進行形の議論を紹介します。

（続く）

18）このプログラムは9.11の直後から、法律の規定なく、Terrorist Surveillance Program（TSP）と名付けられ秘密裏に実施されていました。FISAの手続を経ず、大統領令のみに基づいて通信内容を収集するプログラムです。実施直後から徹底した秘密主義が取られていましたが、2005年12月にニューヨークタイムズのスクープにより暴露され違法性の議論が巻き起こると、ブッシュ政権は一転、このプログラムをそのまま法律として制定することとしました。

19）実際、前注のとおり秘密裏にこのプログラムを運営していたブッシュ大統領自身、2004年に以下のように述べて、コンテンツの収集の際には必ず裁判所の事前審査を経ると明言していました。“Any time you hear the United States government talking about wiretaps, it requires…court order. Nothing has changed. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so.”（President's Remarks in a Discussion on the Patriot Act in Buffalo, New York, 40 Weekly Comp. Pres. Doc. 641（Apr. 20, 2004））

20）U.S. Attorney GeneralとDirector of National Intelligenceが共同で認証します。

21）前注の監督機関のほか、Inspector Generalや法務省（Department of Justice）もそれぞれの見地から独自に報告書を作成しなければなりません。

22）例えば、確かな情報により、100戸あるマンションのどこかにテロリストが潜入していることが明らかとなった場合、どの住民がテロリストかを相当な理由をもって明らかにしない限り盗聴できないとないするのは不合理で、すべての通話内容を盗聴したうえで、99の盗聴を廃棄し、1つの潜入先を見つけ出すことは合理的だと主張します。別の想定として、ある街にテロリストが潜入し、電話で核爆弾の起爆の合図を受けるために待機している確かな情報があるとします。この場合に、その街のすべての電話を盗聴することは、必要かつ合理的だとするのです。

テロとアメリカ 第4回

テロ法制の過去と現在 後編

JCLU会員・弁護士 井桁 大介

はじめに

2号にわたりアメリカにおけるテロ対策法制の歴史を紹介してきました。本号では、スノーデンリークによって明らかになったアメリカのテロ対策の全貌と、その後の改革の動きを紹介します。

スノーデンリークとは

NSA（National Security Agency: 国家安全保障局）の下請会社の職員であったエドワード・スノーデン氏によってリークされたアメリカ政府の膨大な内部資料の総称です。リークされた資料を基に、2013年6月からイギリスのガーディアン紙やアメリカのワシントンポスト紙などで始まった一連の調査報道により、秘密のベールに閉ざされていたアメリカ政府のテロ対策の全貌が明らかになりました。内容は多岐にわたりますが、以下の3点が重要です。

1つ目は、NSAがアメリカ大手の電話会社に命じ、毎日、顧客のすべてのメタデータを提出させていたというものです。これはアメリカ人にとって衝撃でした。それまで様々な監視捜査が噂されていましたが、対象は外国人に限られると思われていたためです。このプログラムは愛国者法215条（business record条項）に基づき実施されていたため、215条プログラムと呼ばれます。対象はメタデータのみで、通信内容は含まれません。

昨年６月のJCLU70周年プレシンポにてインタビューに応えるスノーデン氏

2つ目はPRISMと呼ばれるプログラムで、NSAが9つの世界的なインターネットサービス会社に命じ、特定の通信内容を提供させていたというものです。Facebookの投稿やチャット、Microsoftのスカイドライブのデータ、GoogleやYahooのメール内容などが本人に無断で取得されていました。

3つ目はUpstreamと呼ばれます。海底の光ファイバーケーブルなど、インターネット通信が流れるポイントに捜査員が直接アクセスし、目当ての通信を入手するというものです。

PRISMとUpstreamはともにFAA（FISA2008年改正法）702条により実施されていたため、合わせて702条プログラムとも呼ばれます。このプログラムはそれまでのテロ対策と一線を画するものであり、やはり衝撃を与えました。従来から通信内容の監視は認められていましたが、それはテロと関連する内容に限られていました。しかし702条プログラムでは通信内容の縛りは外され、代わりに通信主体がforeign powerまたはforeign agentであればどのような内容の通信でも対象とすることができます。その主体範囲はあいまいで幅広く、ドイツのメルケル首相の盗聴も許されるに至っていました。また目的もテロ対策という縛りが緩やかになり、貿易交渉や外交で優位に立つために盗聴が行われるようにもなっていました。しかも、ターゲットをネズミ算式に増やすことが許されていました。例えば、ターゲットとされたAさんがメールを送信したすべての人は、foreign powerやforeign agentでなくとも、第二次ターゲットとされます。さらに第二次ターゲットの1人であるBさんがメールを送信したすべての人も、第三次ターゲットとされます。こうして外国のスパイと無関係の膨大な市民が監視のターゲットとされ、メールや電話の内容を傍受されていたのです。702条プログラムだけで年間2500万件近くの通信情報が取得されていたと報告されています。

改革の動き

スノーデンリーク以後、アメリカでは多くの改革の動きが進められています。オバマ大統領（当時）と議会は共同で、独立委員会であるPCLOB（Privacy Civil Liberties Oversight Board）に対し、215条プログラムと702条プログラムの検証を命じました。PCLOBは詳細な検証報告書を発表し、いずれのプログラムにも法律上・政策上問題があること、特に215条プログラムは膨大な個人情報を入手しながら一つのテロ関連情報すら取得できておらず無意味であることが報告されました。

議会はこれを受け、2015年に米国自由法（USA Freedom Act）を制定し、215条プログラムを廃止しました。これは、1978年にFISAが制定されて以来初めて、政府の監視権限を制限する法律となりました。

改革の動きはアメリカ国内にとどまりません。EU司法裁判所は、2015年10月、スノーデンリークによってアメリカの企業が個人情報を顧客に無断で政府に提供することが明らかになったとして、セーフハーバー協定の無効を宣言しました。元来EU政府は、基本権憲章の厳しい制限の下、個人情報を取り扱う企業等に対して、EUと同等の制限を課していない限り、域外に個人情報を持ち出すことを禁止していました。しかし、この原則を厳格に適用すると日常生活に支障をきたすとして、アメリカ政府とEU政府の間で特別の取り決めを設け、一定の手続を踏んだアメリカ企業に限り、EUが求める厳格な個人情報管理をするものとみなす協定が取り交わされました。これがセーフハーバー協定です。スノーデンリークによって、この推定が崩れたとして、協定が無効とされたのです。

国連でも、スノーデンリークを受け、テロ対策を理由とする監視とプライバシーの関係が重要課題として取り上げられ、2013年12月、「デジタル時代のプライバシー（“The right to privacy in the digital age”）」とする総会決議が採択されました。2015年7月には国連人権理事会により、プライバシーに関する特別報告者（ジョセフ・ケナタッチ教授）が選定されました。

スノーデンリークによって明らかになった事実は、決してアメリカだけの問題ではありません。テロ対策としての監視をどのように制御するかという、テロの時代において議論されなければならない最重要のテーマを突きつけているのです。

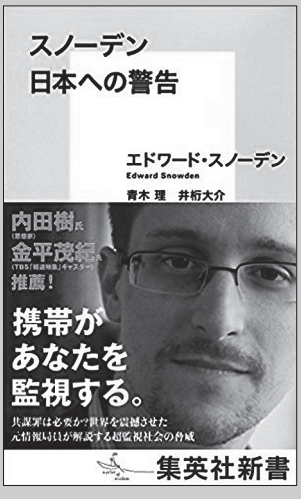
終わりに

政府が主張するテロ対策は本当に予防効果があるのか、一定の予防効果があるとして犠牲になる個人の利益はつりあったものか。スノーデンリーク以前、政府はテロ対策の機密性を理由にこれらの説明責任と向き合うことを避けていました。スノーデンリーク以後、テロ対策は錦の御旗ではなくなりました。政府は説明責任を果たさなければなりません。スノーデンリークは、テロ対策を提唱するすべての政府が学ぶべき教訓です。

しかし、日本政府は、2017年4月、その教訓を完全に無視するかのような共謀罪法案を国会に提出しました。今回の法案が本当にテロ対策に資するのか、どの程度役立つのかなど、政府が果たすべき説明はほとんど聞こえてきません。

私たちはいま、人類史上最も安全な時代を生きています。平成27年の刑法犯は前年比マイナス9.4％、平成8年と比べると40％近い減少です。殺人の件数は年間1000件以下と世界屈指の少なさです。組織的なテロに類する犯罪も95年の地下鉄サリン事件以来皆無です。この平和な時代になぜ、これまで必要とされていなかった犯罪類型が必要なのでしょうか。政府は合理的な説明を果たすべきです。

これまで紹介してきたアメリカのテロ法制の歴史が、今まさに起きている、日本におけるテロ対策の議論を理解する一助となれば幸いです。



昨年東大で行われた70周年プレシンポが本になりました。詳細な注釈と付録インタビュー付き。

テロ対策の是非を考える際に必要な論点が網羅されています。重版に伴いkindleも対応。是非お買い求めください。