エドワード・スノーデン『独白』訳者解説ボツ原稿

山形浩生

目次

本書は Edward Snowden *Permanent Record* （2019） 全訳となる。エドワード・スノーデンの自伝だ。スノーデンはもちろん、NSA およびその他各国諜報機関が行っている、ほぼ全国民に対する大量完全監視を 2013 年に内部告発した人物として知られる。

本書は、その人物の出自、子供時代を経て、暴露に到るまでの経歴、さらにはその決意までのプロセス、そしてロシアへの亡命に到る行動を、スノーデン自身が詳しく語ったものとなる。

1. 本書の概要：スノーデンの思想形成史

まず明確にしておくと、本書にはこれまでのスノーデン関連の各種文献や報道に登場しなかったような、新しい諜報活動の実態は出ていない。本書に説明されている通り、スノーデンは持ち出した資料をすべてジャーナリストたちに渡してしまい、自分の手持ちコピーは破棄したからだ。だから本書はむしろ、スノーデンという人物と、彼の言わば思想とその形成過程の話となる。

1.1. スノーデンの暴露

おそらく本書を手に取ろうとする人は、スノーデンの活動のハイライト、つまり 2013 年に香港で行われた各種内部文書の矢継ぎ早のリークと、同時に行われたスノーデン本人の告白はすでにご存じだろう。アメリカの NSA が、電話やネット上のほとんどあらゆる活動を完全に記録している、という曝露はこの訳者を含め、多くの人々にとって衝撃だった。

もちろん諜報機関や法執行機関が、厳しく法を遵守しているとは、だれも思っていなかっただろう。でも、あらゆる人のすべての通信やそれに伴うメタデータまで収集する、などということがそもそも可能とさえ多くの人は思っていなかったはずだ。1990 年代半ばに、アメリカ政府は、あらゆる通信機器の暗号に裏口の設置を義務づけようとして、大反対にあってそれを断念している。そこから十年ほどで、それをはるかに超えるすさまじい傍受体制が構築されているとは、だれも考えなかった。

またそれがアメリカのみならず、世界各国の諜報機関の協力により行われている、という通称ファイブアイズ体制の暴露も驚きだった。アメリカが自国内で怪しい動きをするのは、日本のぼくたちにとっては対岸の火事のようなものだが、日本を含む世界の主要国も様々な形で協力しているとなると、事情はいきなりきな臭くなる。そうした世界を覆う監視社会が、ほとんどだれも知らないうちに恐ろしいほど徹底した形で完成していたのを、スノーデンの告発は疑問の余地のない形で明らかにした。

それはもちろん、各国諜報組織だけの「手柄」ではない。20 世紀末に一般向けに解放されたインターネット、スノーデンにとっても原点であるインターネットが急速に普及し、さらにスマートフォンが生まれ、カメラとマイクと GPS による位置記録能力を備えた超強力なモニタリング／監視装置を、この十年ほどで世界中のあらゆる人が持ち歩くようになった。人々は自らすすんで監視に身を委ねたとすら言える。同時に、収集した莫大なデータを保管する記録装置のすさまじい進歩に、それを解析する手法や計算能力の大幅な向上も貢

献している。こうした技術環境の変化で、完全監視体制が実現する可能性については、多くの人が認識していた。

でも、技術的な可能性と、実際にできるのと、さらにはそれを本格的に実装し、運用するのとでは、話のレベルがまったくちがう。スノーデンの告発の意義は、「すべて記録監視されてるぞ！」という「証言」にとどまらなかった点にある。その具体的な実装と、その背後にある組織体制までを示す、文書記録を十分に提供できた。そしてその組織体制は、一部政府機関の暗躍などというレベルではなかった。電話会社やアップル、グーグルなどの巨大IT企業は、すべて諜報機関に自分たち（の顧客＝ぼくたち）のデータをリアルタイムでアクセスさせていた！

人々の世界観は、これで一変した。産官（そして一部は軍）が野合する一大監視社会というディストピアが、にわかに現実のものとなった。そして、この曝露でエドワード・スノーデンがアメリカ政府からすさまじい攻撃を受けたことも、その信憑性を大いに高めた。当初はスノーデンの行動を、何やら外国に金を積まれたのだろうとする見方もあったけれど、これはどう見ても変だ。彼は明らかにこの暴露で大きな個人的犠牲を払っている。どんなにお金を積まれても耐えがたい不自由を強いられている。

では、彼はなぜそんな行動に出たのだろうか？

1.2.　スノーデンの思想形成

本書のおもしろさは、まずそれを行ったエドワード・スノーデン自身の話だ。一九八三年に生まれ、テレビゲームから入り、日本のアニメに触れつつインターネットに深入りする様子は、実にありきたりながらも微笑ましく、楽しい。ちなみに、著者の世界観形成に大きく貢献したという『スーパーマリオ』だが、いまは少しは後退できるのでスノーデンが得たような悟りには貢献しないかもしれない。さらにマイクロソフトの認定資格って、バカにしていたけれど、効くんですね。驚きました。

だがもう一つおもしろいのは、NSA を筆頭にアメリカ――そして世界――の諜報業界が、大規模監視体制に突入したプロセスの部分だ。それはもちろん、2001 年の 9・11 アメリカ同時多発テロが大きな契機だった。そしてその瞬間に、スノーデンはたまたま（!!）ワシントンの NSA 本部の隣にいた！

9・11 を防げなかったトラウマ、そして事後対応もできずにパニックを起こして職場放棄してしまった後悔が、その後の NSA や CIA の異様な監視体制構築のきっかけとなり、それがアメリカの自由を見事に圧殺することで、皮肉にもビン＝ラディンたちの狙いを成功さ

せてしまった。

スノーデンはその現場にいて、そして自らもその同じ考え方にとらわれてキャリア形成を行う。アメリカを守る、とは本来はどういうことなのか？　アメリカを守るためにアメリカ憲法すら踏みにじる――それは本当に正当化されるのか？　その場合、そこで「守られ」ているアメリカとは？　建国の理念を失ったアメリカは、本当に「アメリカ」なのか？

本書最大の醍醐味は、スノーデン自身がキャリアの中で、こうした点に苦悩し、様々な価値観の板挟みとなりつつ、2013 年の暴露に到る決断を下すプロセスにある。そしてそれは、本書の読者の多くも、考えてみる必要がある話だ。ぼくはスノーデンのやったことは十分に理解できるし、完全に正当なことだったと思っている。でも多くの人は――特に奴隷根性のしみついた日本人の大半は――悪いルールでも絶対に遵守すべきなのだからスノーデンのやったことはいけない、とかいうことを平気で言う。でも本当にそうなのか？　人は何を守らねばならないのか？　国に、組織に忠実であるというのはどういうことなのか？

2. 本書の関連資料

すでに述べたように、本書には新しい暴露情報はない。またスノーデンが 2013 年に行った曝露の内容についても、ずいぶん簡単な記述しかない。具体的な文書の実例などはまったく載っていない。スノーデンの行動の意義を十分に理解するには、その暴露の中身をもっと具体的に知る必要がある。それには何よりもグレン・グリーンウォルド『暴露：スノーデンが私に託したファイル』（新潮社、2014）を読んでほしい。グリーンウォルドはもちろん、香港でスノーデンから実際の機密ファイル提供を受けたジャーナリストの一人だ。実際にどんなファイルが提供されたかについては、これが最もきちんとしている（というか、まとまった本はこれしかない）。

さらに、本書の内容の特に第三部以降は、すでにかなり詳しい記録とも言うべきものがある。オリバー・ストーン監督の映画『スノーデン』（2017）だ。

いま見直すと、この映画が史実にかなり忠実に作られていることがわかる。さすがにニコラス・ケイジ演じる人物はフィクションながら、いろいろな鍵となる台詞などはきちんと押さえられており、入念な取材に基づいた作品なのは明らかだ。主役のジョセフ・ゴードン＝レヴィットは、著者のかすかな南部訛りまで見事に真似た迫真の演技、グリーンウォルドやローラ・ポイトラス役も非常に実物に似せた造形となっており、再現ドラマとしてきわめて優秀だ。

またそこにも登場したジャーナリストのポイトラス監督『シチズンフォー：スノーデンの暴露』(2014) は、本書の香港以降の話を記録した名ドキュメンタリーだ。こちらでは本書に描かれた場面が、まさにリアルタイムで映っている。そしてオリバー・ストーンの映画と比較すると、現実というものが持つ変に呑気な感覚が非常に印象的ではある。ヘタをすればいまにも特殊部隊に突入されて全員拘束されかねない状況でも、みんな「あのドアがいつぶち破られるかもしれないねえ、ハハハハ」、と軽口を叩く。一方、突然何やら火災警報が鳴り、これは何かの陰謀か、と一同が顔を見合わせる。緊迫しているような、していないような、不思議な場面だ。

このドキュメンタリーを見ると、細かいところで本書の記述とくいちがう。本書だとスノーデンはハワイを出てから、ずっとガールフレンドには連絡を取っていないことになっている。ところが『シチズンフォー』では、当初から彼女に電話して、捜査に協力するよう指示を出している。ここらへん、何か配慮があるのか、それとも単なる記憶ちがいなのかはわからない。（ついでに彼女がいつの時点でどうやってスノーデンと連絡を取り、モスクワまでやってきたのかもわからない。当然ながらスノーデンは、自分の居場所についてはかなり神経質になっているので、彼女にホイホイ住所を送って訪問させたはずもない。）

さらに後日譚としても、『シチズンフォー』はきわめて優れている。スノーデンが持ち出し、『ガーディアン』紙に託した分の暴露文書は、その後イギリス諜報当局の圧力により完全に破棄されたことが描かれている。ジャーナリズムは、本当にスノーデンの信頼に応えられる存在だったのか——これは本書の扱う範囲をはるかに超える話ではある。でも、スノーデン事件の全貌をぼくたちが見ようとするときには、どうしても考えざるを得ない点だ。

3. 個人的な疑問

スノーデンの活動や暴露は重要ながら、あらゆる主張を鵜呑みにする必要もない。たとえば本書によれば、スノーデンは NSA の大量監視システムの核となる分散バックアップ方式を考案し、実装したという。クラウド方式の原型を考案したのも、スノーデンだとか。いずれも確認しようがない話ではある。

さらにそうした自慢話にとどまらず、もっと積極的に首を傾げるような話もある。スノーデンによれば、NSA は単に人々のトラフィックを監視するだけでなく、目をつけた人物のマシンに勝手にマルウェアを仕込んで操作するという。

だがこれは、釣りメールにウィルスを仕込んだファイルを添付するというような話とは

わけがちがう。普通のトラフィックにペイロードを乗せて侵入し、どんなシステムでも乗っ取れるというのは……にわかには信じがたい。

その具体的なマルウェア検出の報告を少なくともぼくは見たことがない。それほど強力なマルウェアが、これまで世のあらゆるセキュリティ専門家に気づかれないなどということが本当にあるのか？

また本書では、スノーデンは自分の手持ちデータを全部消去した、とされている。でもいまだに「スノーデンが新たに暴露した文書によると」といった報道がときどき見られる。2019 年 6 月にも、NSA がイスラエルに情報を流していた、という新しいスノーデン文書の報道があった。これは一体どういうことなのか？　実は完全に手元の文書を削除していなかったのか、それともいまも新しい諜報チャンネルがあり（たとえば NSA 部内者がリークのルートとしてスノーデンを使っているとか）、それ経由で情報が出てきているということなのか？　これもはっきりしない。

さらにどうやって NSA システムからファイルを SD カードに移したのか、といった技術おたくとして興味のある部分は秘密のままだ。これはいささか残念ではある。

4. 監視への対抗手段

もちろん、スノーデンの話で完全に確認できない部分があるからといって、彼の主張すべてを疑う必要などはない。一般に思われているよりずっと徹底した監視が行われていた、という彼の暴露はまちがいないものだ。そして重要なのは、それに対して具体的に対抗することだ。でも、具体的にとは？

スノーデンのおかげで、事態は少し改善した。NSA は、少なくともアメリカ国民に対する完全監視はやめたらしい。そうした監視を支持する各種規定も廃止されたようだ。

また本書では、グーグルもアップルもフェイスブックも、政府と結託してみんなのデータを売り飛ばす、悪の帝国にして政府のポチだ。でもスノーデンの暴露に伴う批判に応え、アップルはそこそこ頑張って iPhone などのセキュリティを改善してきた。またグーグルはウェブサイト用の http プロトコルの暗号化（https）を急速に進め、各種通信が傍受されにくくしてくれた。

でも、当然ながらそれで十分とはとても言えない。

監視に対抗するのはなかなか面倒だ。「そういうことをしちゃいけませんよ」という法律を作ってもらうのもいいだろう。でもそれですむなら警察はいらないし、家に鍵をかける必

要もない。そもそもスノーデンの暴露は、諜報機関がそういう法律を無視していた、ということなのだから。

しかも面倒なのは、いまや国が見てるぞ、というレベルの話ではない、ということだ。いまや各種大規模ネット企業が様々な形で人々のデータを集めている。そしてプライバシーを懸念し、各種の監視に抗議する人々でも、一方では平気で Gmail を使い、フェイスブックやツイッターで私生活を公開しまくっている。なんでもアマゾンで買い、クレジットカードで支払いをしている。SNS で自分の居場所を宣伝し、あらゆるファイルを自ら進んでクラウドに上げてしまう。そして、そうしたクラウド企業やネット企業は、そのデータを束ねて政府にホイホイと渡し、他の企業にそれを売り飛ばす。

では、それに対してどうすればいいのか？　具体的な対応とは何だろうか。

それは、自分がプライバシーを重視していることを行動で示すことだ。

それは、ツイッターで「監視社会ゆるさないぞ！　××やめろ！　リツイート希望」とか書き散らして悦に入ることではない。何かを実際に変えることだ。いまの監視やプライバシーの戦場は、相当部分がネット上に移行している。では、対抗手段の現場も当然ながらネット上になる。自分のネットへのインターフェースについて設定やソフトを見直すことこそが、プライバシー重視の第一の行動となる。

4.1.　プライバシー設定：初級編

そうした行動は、そんな大げさなものである必要はない。まず一つは、自分の SNS やスマホのプライバシー設定を見直して、余計なデータを勝手に集めたり流したりさせないようにすることだ。そうした設定については、ネット上にも多くの情報がある。「フェイスブック　プライバシー」で検索すれば、すぐにやり方はわかる。自分の居場所情報を勝手に集めるな、広告の選択に個人情報を使うな――そうした設定を変える人が増えるだけでも、多少はちがってくる。

同じくらい基本的なこととして、ウィンドウズや MacOS のソフトアップデートは、面倒臭がらずにきちんとあてよう。各種の脆弱性利用は、悪玉クラッカーも政府監視も同じだ。穴はふさぐにこしたことはない。

またいつも使うブラウザや検索エンジンを、プライバシー重視のものに切り替える手もある。あらゆるデータを収集したがるグーグル検索はやめて、情報利用を制限する

DuckDuckGo や Qwant を使う、ブラウザをプライバシー重視の Brave や Firefox などに変えるといったことだ。

SNS やメッセージソフトは、相手がいるのでなかなか自分だけでは変えられないけれど、メッセージソフトだけでもスノーデンおすすめの Signal やプーチンの圧力にも屈しなかったとされる Telegram などを使うようにする手もある。

そして重要なのは、パスワードだ。一般ユーザのセキュリティは、基本的にはパスワードで担保されている。パスワードの使い回しを避け、類推されないものにすることで、セキュリティは高まり、多少は監視されにくくなる。パスワードマネージャを使おう。そして可能な場所では、二段階認証を使おう。

一般人でも、ここまでやればかなりセキュリティは上がり、プライバシーも保たれ、情報を勝手に抜かれることも減る。もちろん、セキュリティが完璧になるということではない。ブラクラを踏んだり、変な釣りメールにつられたり、といった愚行は防ぎようがないし、多くの人はグーグルや SNS にはむしろ喜んで情報を提供する。まして NSA が本気を出せば、突破されるだろう。でも多少は手間のかかる存在にはなれる。そしてそういう人間がある程度増えるだけでも、プライバシーが価値観として重視されていることを示すことになる。

4.2. プライバシー設定：中級編

もう少しマニアックな領域に進めば、ブラウザで Tor を使うことはできる。これは本書の中にも登場するもので、ブラウザの接続を言わば攪乱し、だれがどこから何に接続しているのかわからなくしてしまう。各種 VPN サービスを使うのも一つの手ではある。別のサーバ経由で様々なサイトにアクセスすることになり、しかもデータは暗号化されるので、どこにアクセスして何を見ているかを外から知るのは困難となる。

メールを PGP で暗号化する、といった手間をかける人もいる。これにより、メールの内容は傍受されなくなる。ただしこれは、相手も PGP を使える／使っているというのが前提となる。さらにスノーデンによると、暗号化メールはかえって怪しまれて監視対象になりやすいとか（彼は、電子メールそのものがダメだとさえ言う）。でも、署名をするだけでもかなりちがう。相手が PGP を使っていなくても、メールは読んでもらえるし、その気になればこちらの身元を確認できるし、改ざんされていないこともわかる。

ただしハードルは上がる。本書でもグリーンウォルドはこれが導入できなかったがためにスノーデンとの接触が遅れ、結果的に彼を危険に曝すことになる。グリーンウォルドが苦労するなら、そこらの一般人に使ってもらうのはかなりつらい。

4.3. プライバシー設定：上級編

パラノイアぶりを発揮して、自分の使うコンピュータをいじる手もある。セキュリティマニアの一つのしるしは、コンピュータのカメラにテープを貼って、政府などによる監視を避けるというものだ。スノーデンの話を真に受けるなら、NSA はどんなマシンのマイクやカメラでも自由にアクセスできるはずだからだ。が、外で見られたときにバカかと思われる危険性があるのも事実だ。

そしてマシンの OS までいじる度胸があるなら、スノーデンが現在使っている Qubes OS（謝辞にも登場する）は非常におもしろいオペレーティングシステムだ。この OS は、コンピュータ上で行う各種の活動を厳しく分けることでセキュリティを高めようとするのだ。

一般に人々は、パソコンでウィンドウズや MacOS を使っている。さてこれらでセキュリティが突破され、個人情報が抜かれる大きな原因は、各種の活動が混在していることだ。ぼくたちは同じブラウザで、SNS に書き込みをして、怪しげな動画サイトを眺め、メールに添付されてきたファイルを平気で開いて、それからオンライン銀行や会社のサーバーにつないで、機密資料を見たりしている。どこかでウィルスやスパイウェアを仕込まれたら、あらゆる活動がバレる。

Qubes OS では、それを個別の仮想マシンで、完全に仕切る。趣味の買い物や動画サイトは、「遊び」マシンで行い、仕事関係は「仕事」マシンで行う。閲覧履歴もファイルもメールも、利用者が明示的に指示しない限り共有されることはない。NSA がウィルスを仕込んでマシンを乗っ取っても、その仮想マシンから外には出られない（はず。NSA に何ができるかは不詳なので）。

この OS については日本語の情報があまりないので、訳者が簡単なインストールガイドを作った。後出のサポートページにリンクを載せておく。ただし、パソコンの BIOS の設定を変えたりしないとインストールもできない。Linux の経験がそこそこないとなかなか面倒だし、コンピュータの扱いに慣れていないと、もとの状態（たぶんウィンドウズ）を回復できなくなってしまう。

4.4. プライバシーと権利：そのコスト

さて、これらは面倒だ。そんな面倒なことをみんながやるわけがない、と言う人も多いだろう。おっしゃる通り。万人が Tor を使い、メールを PGP で暗号化する——そんな状況が

期待できるわけもない。そして、それで完璧というわけでもない。

でも……そもそもセキュリティやプライバシーというのは、ある程度は面倒なものなのだ。家に鍵をかけるのはめんどくさい。暗証番号だのパスワードだのをきちんと設定するのは面倒だし、それでも完璧ではない。

でも、みんなそれだけの手間はかける。鍵のかかっていない家に侵入しても、不法侵入にはなる。お金をあなたが道端にむき出しで放置しておいても、それを取った人は泥棒だ。それでも、人は家に鍵をかけ、お金は財布にしまう。ある意味で、そういう規範や法律があるのは、多くの人が家に鍵をかけ、財布にお金をしまうという行動を通じ、財産保護を人々は望んでいるのだ、という意思表示をしているからだ。だからそれを社会として普遍化しようという動きが支持されたのだ。

これはプライバシーやセキュリティの話でも同じだ。「全員が」やるかどうかではない。面倒でも「ある程度の人が」それを敢えてやり、わざわざ対策を講じる、ということだ。

そもそも人権という考え方はずいぶん変なものだ。どこからともなく「人権」なるものが与えられていて、何もしなくても社会がコストを負担してそれを守ってくれる——本人がそれをまったく守ろうとせず、それを維持するために何ら負担をしなくてもかまわない——人権はそういうものだということになってるけれど、本当にそうなの？　プライバシーを自ら守ろうとしない人、そのためのコストを払う気もない人——極端な話をすれば、ぼくはそういう人々のプライバシーは守る必要がないとすら思う。これは他の権利も同様だ。各種権利にあぐらをかき、それを守るためのコストを負担しようとしない人々——そういう人々の権利は、原理的に言えば守るに値しないとすら思う。ちなみに、これは懐かしき「自己責任」論の一部だ。

これはさすがに極論ではある。でも、そこまでいかなくても、ある程度のコストを自ら負担してプライバシーを守ろうとする人が一定数いない限り、プライバシーは重要であって社会的にそれを確保し、守る方策が必要だという議論は説得力を持ち得ないと思う。これはプライバシーだけでなく、あらゆる「権利」「自由」についても同様だ。

だってそうなんだもの。人権は最初から「あった」ものではない。だれかがそういう権利を必要だと考え、そのために戦い、犠牲を払った。またも極論だが、その社会である権利のために死んだ人がいない限り、その権利はその社会には存在しないのだ、と主張する人さえいる。そこまで言うつもりはない。いちいち殉教者を出さなくても世の中は進歩できるべきだ。でも、みんなが費用をある程度は負担し、ある程度の犠牲の覚悟を示すことで、権利は生まれ、根付くのだ。その費用というのはプライバシーの場合、まずはなるべく多くの人が、右に書いたような設定変更やソフト導入を行うことだ。プライバシーを確保するために、多

少の手間をかけ、面倒を引き受けることだ。

スノーデンは、プライバシーと自由をきわめて重要なものと考え、それを損なう監視の実態を明らかにすべく、大きなコストを払った。そしてそれは状況をある程度は変えた。

だったら――「監視社会けしからん、NSA とファイブアイズゆるせん！」と考えるのであれば、隗より始めよ。あなたも、スマホの設定を変える程度の行動はしてはいかが？　むずかしいから、面倒だから――そんな逃げ口上で何もしない、個人情報ダダ漏れの人のプライバシー論に何の説得力がありましょうか。

むろんそうした技術的なやり方でなくても、何かできることはあるのかもしれない。この訳者には思いつかないような、非技術的なプライバシー保護の行動とは何だろうか？　コストもいろいろだ。本書を読むというコストを負担する人が増えるだけでも、その中から新しい手法を思いつき、実践し、社会の変化を促す人々が登場するのかもしれない。

5. おまけ：諜報活動について

本書の見所は他にもある。特におもしろかったのは、ジュネーブにおける人間諜報（HUMINT）と、スノーデンがやっていた信号諜報（SIGINT）との関わりを述べた部分だ。

日本では、インテリジェンスとか諜報とかいうと、だれのせいかは知らないが人間諜報ばかりが取り沙汰される。派手な政治かけひきの舞台裏についてのネタを小出しにしてみせ、そこに国家とは～とか神とは～とかいう愚にもつかないヨタを、深遠ぶった顔でからめてみせるのが諜報だと思われているようだ。

でも、もはやそういう人間諜報は限界がある。いまや人間諜報部分はますます縮小し、SIGINT 部分こそが主流になりつつある。もう、どっかの要人を捕まえてゲロらせればすむというものではない。

実は以前、まさにそうした諜報／スパイ業界の変化について CIA の人間が書いた本を訳したことがある。ロバート・スティール『オープンソース世界のスパイと秘密』だ[1]。全訳したところで版元が倒産してしまったので、宙に浮いているが、その主張はなかなか示唆的なものだった。

人間諜報中心の諜報活動が持つ欠陥を指摘した本だ。そうした活動は、常に秘密を重視する。要人やその周辺人物に接触するのは、秘密を知りたいからだ。でも、やがてそれは、秘密を秘密であるがために重視するという倒錯に陥る。そして、自分が手に入れた「秘密」の

[1] 全訳は https://cruel.org/books/intelligence/intelligencej.pdf

価値を維持するためにそれを隠匿し、他に秘密を持っていそうな人間ばかりに接触して、同じ「秘密」がそうした人々の間をいつまでも堂々めぐりするだけになる。そして秘密でないことを軽視するために、だれでも知っている現地の常識を平気で見すごす。

現地語で新聞読もうぜ。ちゃんと統計見ようぜ。スパイの世界であっても、大事なことはいまやほとんど公開情報にあるんだよ、というのがその本の趣旨だった。公開情報を系統だって継続的に集め続け、分析する仕組みを作るほうがずっと重要なのだ、と。同時に、もう諜報の対象も変わっている、とその本は指摘した。いまや国のスパイと産業スパイとは区別がつかない。国の競争力が技術にあるとき、政治家が何を考えようが、企業の状況次第で国の力関係も変わる。その意味でも、諜報は変化を余儀なくされるんだ、と。

本書に描かれた状況というのは、このスパイ業界の力点推移をさらに先に進めたものでもある。同時に、諜報の対象は外国にとどまらず、国内の自国民にもなっている。この変化をもとに、国家とは〜とか、あるいは神とは〜といった話をあれこれ展開することも可能ではあるはずだ。特にこの諜報の対象の変化は、かなり大きな意味合いを持っているようにも思うがいかがだろうか。

6. 最後に

本書の翻訳は、当初何やらずいぶん秘密めかしたメールで河出書房新社の吉住唯氏より相談がきて、中身もよくわからないまま承知させられ、原稿の束が何といまどき紙で送られてくるところから始まった。ちなみに、そのとき使われていた著者の偽名はアーサー・キング、つまりアーサー王だ。これが持つ意味合いは、本書をお読みになった方ならわかるだろう。その後も連絡はセキュリティ重視の Signal だけ、メール等の言及禁止といった細かい指示がきて当初は閉口したし、もったいつけすぎだろうと鼻白む思いもさせられた。

ところが原著刊行の翌日、アメリカ政府は版元を訴えた。内容を事前検閲させなかったから、とのこと。本書の存在／内容が事前にもれていたら、出版前に何らかの強硬手段がとられていた可能性も十分ある。著者の警戒は決して杞憂などではなく、己の不明を恥じる次第だ。

内容的には特にむずかしい部分もなく、白を黒とまちがえたような部分はないはずだが、変換ミスや思わぬかんちがいはあるかもしれない。もしお気づきの点があれば、訳者までご一報いただければ幸いだ。メールか、あるいはセキュリティを気にする方なら、鍵サーバから訳者のメールアドレスの PGP 公開鍵をダウンロードして暗号化したメールか、Signal で

Hiroo Yamagata まで連絡いただきたい。直すべきものは、サポートページ https://cruel.org/books/arthurking/ の正誤表に随時掲載する。

ちなみにスノーデンの記述を信じるのであれば、本書を読んでいるというだけで、みなさんはすでに NSA に目をつけられ、一挙一動、一言一句がすべて見張られていることになる。どうです、おっかないでしょう。ましてそれを訳したこのぼくは、なにやら壮絶な要注意人物になりそうだ。こんな本を訳しているばかりか、イランなんかにでかけ、さらにこれを書いているのはキューバ。アメリカの敵性国に足しげく通う怪しい人間というわけだ。おまけに中国にもしょっちゅうでかけ、使っているマシンはファーウェイ製。まあ、実際にはこの程度の人間は数万人規模でいるはずなので、別にそれで何か実害が生じるわけでもないだろうが、監視リストには入っている……のかなあ。

だから、サポートページには自衛の意味もこめて、右の Qubes OS インストールガイドも含め、いくつか各種セキュリティ関連の情報へのリンクも入れるようにする。それがみなさまにも多少なりともご参考になれば幸いだ。

2019 年 9 月　ハバナにて

山形浩生（hiyori13@alum.mit.edu）