隠すものが
なければ、
恐れることは
何もない？

2014 年 10 月

Cyber Security Research Institute（CSRI）によって実施された調査の結果、英国が監視国家に急速に変貌しつつあることが明らかになりました。企業と政府自身の活動を規制する措置を直ちにとらない限り、この変化による深刻な影響を元に戻すことは不可能です。

エドワード・スノーデンが、米国の諜報機関である NSA と英国版 NSA の GCHQ による広範な技術悪用を内部告発と、英国タブロイド紙の電話ハッキング・スキャンダルの結果、テクノロジーに対する意識が向上し、個人の行動が確実に変わってきています。

政府高官、プライバシー・コミュニティ、政府の情報システムの開発に携わる企業、政府の情報システムに携わったことのある金融サービス業界関係者、元諜報員、そしてマルコム・リフキンド情報安全保障委員長のような大物政治家を対象とした一連のインタビューに基づいて作成された冊子 CSRI 報告書は、到来した監視社会に関する政治的支配力および理解の欠如について警鐘を鳴らしています。

いわゆるスノーデン・エフェクトの前後に実施された意識調査は、監視文化がどれだけ深刻化しているかを示しています。

2004 年にガーディアン紙向けに ICM が実施した世論調査によると、回答者の 72%が安全のためならプライバシーを犠牲にすると答え、65%が諜報機関は問答無用で電子メールおよび通話にアクセスできるべきだと考え、63%が警察がこれらと同じ権力を持っていた方がよいと答えています。

スノーデンの告発から 1 年後の 2013 年に実施された YouGov/ケンブリッジ大学による調査の結果、回答者のうち、政府とセキュリティ・サービスが英国国民の通信を傍受する権利を持つべきだと答えたのはわずか 43%に過ぎず、外国人のメッセージのハッキングは許されるべきだと答えたのは 49%に止まりました。

また、本報告書の著者が 2014 年 10 月に委託した新しい調査の結果を見ると、一般大衆の大量監視に対する不安が急速に広がっていることが明らかになっています。

・回答者の 86.5%が、英国政府が大量監視を実施することに賛成しないと答えている

・回答者の 82.2%が、大量監視に対して懸念を抱いている

・回答者の 3 分の 1 未満（32.3%）が、自分のデジタルデータを政府が追跡していることを認識している

・回答者の 3 分の 2（77.85%）が、自分のデータが追跡されていることに懸念を抱いている

・回答者の 14%だけが、政府は公共の安全の目的で、すべての人々の個人情報にアクセスできる権利を持つべきだと考えている

・10 人のうち 1 人（10.45%）だけが、大量監視は良いことだと考えている

・こうした結果とは裏腹に、政府によって追跡されないように対策を講じているのはわずか 3%に過ぎない

（調査は成人 2000 人を対象に、Vital Research & Statistics によって 2014 年 10 月 10～13 日に実施された）

盗聴文化の増加に対する懸念の増加

情報監視に不安を感じたことで、数百人もの人々が個人情報を保護する方法を身につけられる講習を求めるようになっています。キャンペーングループ「Don't Spy on Us」によって 2014 年 6 月にロンドンのショーディッチ・タウンホールで開催された、「暗号パーティー」には参加希望者が殺到し、ブロックをぐるりと囲むほど長い列ができました。また、他の同様のイベントにも非常に多くの人々が集まっています。

「情報監視文化」に対するこの意識の高まりは、アメリカのクラウド・コンピューティング企業にも影響を与えています。インディペンデント紙が行った調査では、**米国のクラウドサーバが諜報機関にアクセスを提供するのではないかという警戒心が広がり、Cisco と Microsoft というテクノロジー企業 2 社は、10 億 7000 万ドル相当のビジネスを失ったことが明らかになりました。**

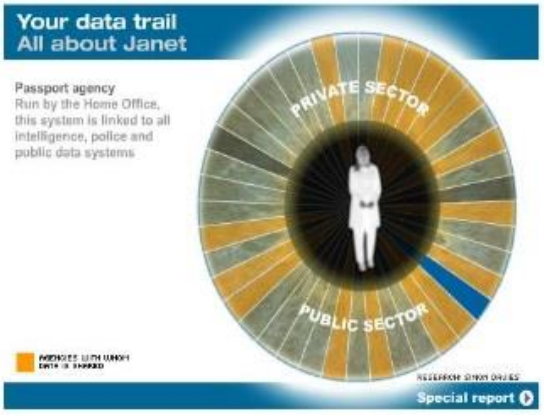
エドワード・スノーデンは、最近の声明で、合衆国憲法制定者たちは特定の権利を憲法に盛り込んだが、成文憲法を持たない英国人はそれを主張できないため、英国政府は米国政府よりも悪質であると警告しました。

ロンドン中心部で開催された Observer Ideas フェスティバルに Skype を介して参加したスノーデン氏は、GCHQ の監視能力には「本当に制限がない」と述べました。

彼は次のように述べています。「英国は、規制のためなら何をしてもいいシステムになっています。政府は興味を引くものすべてを収集していて、それが必要な理由を自由に正当化しているのです。そうする必要がない理由を正当化する権利は国民にはありません。これは危険なことです。自分に不利な証拠が収集されているのに、それに対して裁判所で異議を唱える機会を与えられていないのです。これは、司法制度全体を損なうものです。」

さまざまなテクノロジーおよびアプリケーションの中でも、メール、通話、ウェブ検索、ソーシャルメディア、地理情報を得るために西洋諸国の諜報機関が使用しているのは、Prism、Tempora、Echelon、Frenchelon、Fairview、MYSTIC、Carnivore、Optic Nerve、Quantum theory、World of Warcraft、Nosey Smurf、Dreamy Smurf、Tracker Smurf、Edgehill、Dishfire、Stoneghost、Squeaky Dolphin、および Royal Concierge です。

膨大なデータ収集



政府と民間企業も膨大な数の個人情報データベースを保有しています。2004 年、プライバシー・インターナショナルの創設者であるサイモン・デイビスは、ロンドンで夫と子どもと暮らす一般女性、Janet Sykes に関する情報を保持するすべてのデータベース（70）の合成画像を作成しました。データベースには、民間企業や、地元およびネットワークサービスのものも含まれていました。たとえば、インフォグラフィックの民間部分には、数々のポイントカードがありました。スーパーマーケット Tesco のロイヤルティ・プロジェクトを作成した開発者は、クラブカードを使った購買行動と食嗜好、郵便番号、年齢や性別などの人口統計データから、支持政党や投票行動を予測することが可能であると CSRI に語りました。

これは 7 年前のことです。2014 年 10 月に本報告書のためにインタビューを受けたデイビスは、かつて 70 だったデータベースの数は現在 700 を超えているだろうと予想します。国民一人ひとりについて保存されている情報の量と種類は、英国の国民保健サービスがケア・データ・プログラムを立ち上げる 2014 年冬に大幅に増加することが見込まれます。NHS 番号によって識別される各患者の詳細かつ機密の生涯医療情報が収集され、新設される Health and Social Care Information Centre（HSCIC）によって保存されることになるのです。NHS ウェブサイトによると、HSCIC の目的はよりよい医療を提供することであり、診療記録情報を集積し、そこから有用な情報を掘り出して予防医学と患者の治療成果の向上に役立つ統計情報を提供できるとしています。この新しいデータベースは、保険会社、銀行、住宅ローン企業にとって価値があり、資金難に苦しむ NHS 部門マネージャーが患者の情報を潜在的な収入源と考える可能性があると、評論家は警告します。

プライバシー・インターナショナルおよび「プライバシー・サージョン」ブログの著者であるサイモン・デイビスは、1983 年のデータ保護法起草時の概念である「全情報認知（TIA）」が目的であると言います。「ホワイトホールにおける TIA は、名前を敢えて口にしない宗教のようなものだ」と。しかし政府機関は、許可なくお互いのデータベースを共有または結合することはできません。「データベースを結合すると、コンテキストが変わり、情報も完全に変化してしまいます。しかし、官僚はこれを理解していません。すべてのデータは集合的であれ、単独であれ、公共の利益のためにあり、その利用は公共の利益になると信じているからです。**彼らは、自分たちが集めたデータは自分たちのものだと考えているのです。**」

スノーデンの告発により、Facebook、Google、Yahoo などのインターネット・サービス・プロバイダが諜報機関に協力してユーザのプライバシーを侵害したことが明らかになりました。つまり、ソーシャルメディアは、プライバシーと匿名性保護に関しては政府のファイリング・システム同様信頼できないということです。スパイが「バックドア」を使ってあなたのソーシャルメディアのプロファイルに侵入していないとしても、プライバシーについての一般的なリスクは残ります。サイバー犯罪者やヌードの「自撮り」写真を盗んだり偽造したりする者、荒らし屋、ストーカーは、プライバシー設定や使用条件が必ずしも明確でなく、簡単に理解できないシステムを悪用することができます。Facebook などのテクノロジー企業は、無料でサービスを提供しています。元ドイツ諜報員の Bjorn Rupp は、本報告書の著者とのインタビューで「**お金を払っていなければ、顧客ではない**」と指摘しました。これら

の企業のビジネスモデルは、あなたの個人プロフィールを広告主に販売することで成り立っています。ターゲットを絞り込んだマーケティング・メッセージをユーザのタイムラインに提供するために、より詳細な個人情報を開示するようユーザを引き込もうとするのは当然です。

また、Facebook に諜報機関のための「バックドア」があろうとなかろうと、Facebook は政府にとって役立ちます。たとえば、ドイツ政府の国勢調査官は、国民のライフスタイルに関する標準のアンケートにいくつかの追加質問を加えることを提案しました。しかし、これに対して市民的自由の運動家が猛抗議したため、政府はすぐに追加質問を削除し、Facebook などのソーシャルメディアで公に利用可能なデータから情報を収集することにしたのです。

英国の現状は、税金を支払い、公立学校に通う子供を持ち、国民保健サービスを使用し、学生ローンを借り、公的年金その他の福祉手当を受給している大多数の人々がこれらのサービスを管理するデータベースのネットワークによって追跡されています。政府は、現在の複雑な給付システムを数カ月後（2014～2015 年）にユニバーサル・クレジットに切り替えて、すべてのトランザクションの 82%をオンラインで行うことでオフィス、スタッフ、紙ベースの通信に費やされる公金を節約することを目指しています。政府の「デジタル・バイ・デフォルト」方針も、サービスや情報を求める人々にワンストップ・ショップを提供する公式ポータルサイトの Directgov へと移行しています。これによって、異なるカテゴリのデータを組み合わせることができる、警察やスパイのためのワンストップ・ショップも実現するのでしょうか？数百万ポンドの納税者の血税を無駄にした数多くの IT 災害を経験した今、私たちはこの新しいシステムを信頼できるでしょうか？「デジタル・バイ・デフォルト」プログラムを監督する科学技術委員会のグラハム・ストリンガー議員は、彼が持つ懸念について調査員に語りました。

「セキュリティに関して 2 つの大きなリスクがあります。1 つ目はシステム全体に対するリスクです。診療記録であろうと国民年金記録であろうと、公共サービスにアクセスする場所ならどこでも、データが盗まれ、違法な目的または商業的利益に使用される可能性があります。オープンシステムを本当に安全に維持することは非常に困難です。

2 つ目は、なりすまし犯罪が発生する可能性です。また、システム内で本人確認を行うことの難しさもあります。これらはすべて克服すべき問題です。

私たちは、テクノロジー業界の専門家と協力して、問題を解決する方法を模索しながら、政府には極めて慎重になるべきだと警告しています。**システムのセキュリティを最大限に高めることができても、それを提供している人が何らかの方法で不正を行えば、情報は簡単に漏れてしまいます。」**

サイバースペースにあるデータを、従来の紙の記録と監視カメラが提供する地理的位置情報に加えることで、当局は、疑わしい行動を取っているかどうかにかかわらず、どこでも誰でも追跡することができる手段を手に入れることになります。British Security Industry Authority（英国警備業監督委員会）によって 2014 年 10 月 16 日に発表された調査によると、**英国国民 11 人につき 1 台の監視カメラが存在すると推定されています。**つまり、590 万台もの CCTV カメラが設置されているということです。

全体主義の警察国家であった東ドイツ（ドイツ民主共和国、GDR）でさえ、シュタージ秘密警察（Staatssicherheit）が抱えていた密告者の数は国民 65 人あたり 1 人です。

報道の監視

テクノロジーに精通したごく一部の人々のうちの多くは、大量監視からデータを保護する措置を講じています。本報告書の著者は、盗聴を恐れるがために、人々が携帯電話の電源を切り、モバイルデバイスとコンピュータを使った個人的な会話を避けるようになっていることを示す、直接的かつ個人的な証拠を持っています。これはジャーナリストや、技術および金融業界で働く人々によく見られる行動です。被害妄想と思われるかもしれませんが、ジャーナリストの情報源を明らかにしようとした警察による捜査権限規制法の乱用など、最近発覚した数々の実情を考えれば、このような行動もある程度仕方がないように思えます。

これは、現職の情報コミッショナーであるクリストファー・グラハムによって特定された問題です。グラハムは、2013 年 1 月 7 日のデイリー・テレグラフ紙とのインタビューで、データ保護法の改革案によって、対象となる人物が、ジャーナリストが保持している彼らについての情報にアクセスできるようになるという懸念を表明しました。専門家は、これによって匿名の情報源が暴かれることになると恐れています。

私が不安に感じているのは、知らない間に英国が監視社会になり、国民についてもっと多くの情報が収集され、その情報に英国社会を不安にするほど多くの人がアクセスできることだ…」

「東ヨーロッパやスペインでは、政府の力があまりにも強くなり、国民に関する情報を持ちすぎたらどうなるかということを前世紀に経験している。誰もが他のすべての人の情報をすべて知っており、手動だろうとコンピュータ化されていようと莫大なファイルを所有している状況になったら…」

「私は、人々がこの背後にある問題に気づいているとは思えない。これによって政府は国民の活動の多くについて非常に包括的な実態を把握することができる。私の仕事は、特定の目的のために必要以上の情報が収集されないようにすることだ。」

リチャード・トーマス - 情報コミッショナー、2004 年

グラハム氏はこう述べています。「私たちはデータ保護立法によって報道の仕事が弱体化されないようにすることの重要性と、この法律が表現の自由に影響を及ぼす可能性を認識しています。」

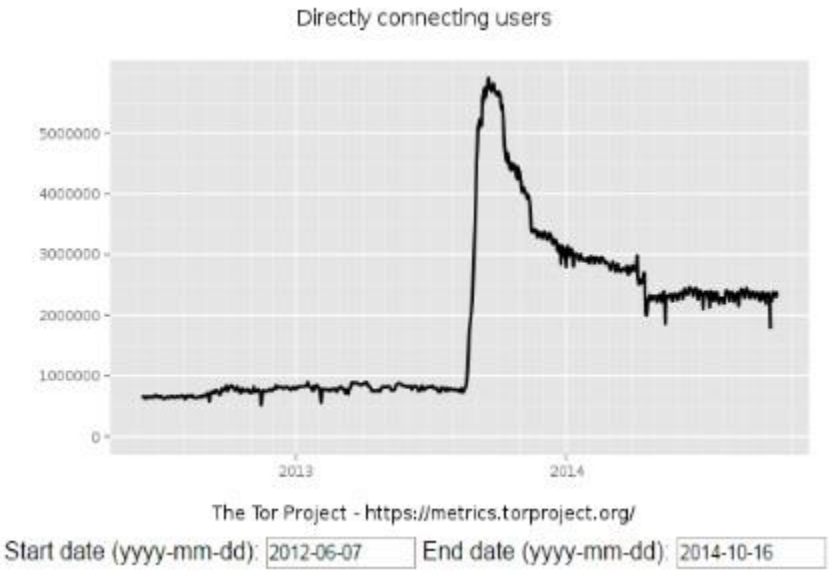
「ジャーナリストの電話ハッキングに対するリーブソン判事の審理が調査報道に与えたであろう「萎縮効果」に関する正当な懸念を考えると、対象人物による情報アクセスは特に難しい問題です。これについては、非常に慎重に検討する必要があります。繰り返しますが、これは利害のバランスの問題であり、最終的には議会で話し合うべき問題です。」

確かに、スノーデンが提供した情報に取り組んでいるガーディアン紙のジャーナリストは、政府による直接的な脅しに直面しても、自らの仕事を続けるために前例はないが正当な対策を取ることを余儀なくされました。

この対策には、窓がない「エアギャップ（ネットワーク隔離）」処理された部屋での、サニタイズ（無害化）された機器の使用が含まれていました。

ガーディアン紙の編集長、アラン・ラスブリッジャーは、セキュリティ・サービス捜査官がやって来て、水が入ったコップでさえ盗聴器になると指摘したことを含め、どのような脅しが行われたかを詳しく公表しています。

恐怖の拡大



政府による監視に対する恐怖はビジネスコミュニティにも広がっており、暗号の使用が急激に増加し始めています。これは Tor（The Onion Router の頭文字から作られた頭字語）という暗号化システムの使用者の急増に加え、NSA と GCHQ の両機関が Google のデータを強制的に収集したというエドワード・スノーデンの告発にもかかわらず、暗号化された Google Gmail の使用が増加したことからも明らかです。

スノーデンの告発によって企業行動に変化が起きていることを示すさらなる証拠は、テクノロジー愛好家やコンピュータ・セキュリティ企業が組織や個人にデータ保護の方法を教える、「暗号パーティー」と呼ばれるイベントへの参加者数が急増したことです。

2014 年 6 月に「Don't Spy on Us」がロンドンのショーディッチ・タウンホールで開催した暗号パーティーのチケットは売り切れとなり、チケットを持たない参加希望者で長蛇の列ができました。その他にも多数の暗号化トレーニング・イベントが英国全土で行われています。その多くは、地元企業の要望で開催されています。

かつて、これらのティーチインに参加するのは技術者とギークだけでしたが、今年のイベントでは、企業や今までテクノロジーに興味がなかった人たちの出席が増えています。

スノーデンの告発は米国のクラウド・コンピューティングに影響を与えました。NSA による監視を恐れた企業によるクラウド・コンピューティングの使用が大幅に減少しており、政府の監視に企業が反発していることは明らかです。

一部の識者によると、このビジネス上の不利益が、NSA のスパイプログラムに対する追加の監視機能と説明責任の仕組み整備を求めて、アップル、マイクロソフト、Google、Facebook、ヤフー、AOL によって 2013 年 10 月に上院司法委員会の主要メンバー宛てに公開書簡を送付することが突然決定した要因の 1 つとなりました。

英国内閣府担当大臣のフランシス・モードは、ビジネスコミュニティにスノーデンの告発が与えている影響と反発の高まりをいまだに認識していません。彼が大臣を務める内閣府はジョン・メージャー政権の下で中央電子計算機局を吸収したことから、議会および政治家がコンピュータの発展に遅れないようにすること、およびコンピュータプログラムを実施する役割を担っています。

「事件については大変遺憾に思っていますが、私たちとの情報交換に対してそれほど抵抗が高まっているとは感じていません。国民は、守ってもらう必要があることを知っています。世間の目に曝されることなく行われた方がいいですが、実際には、私たちのできることには厳しい法的規制がかけ

られており、政府機関が適切な監視・監督の下で行動しているため、人々は安心してこれらの機関が適切に行動していると考えることができると思います」と、モードは PassWord ラジオ番組のために行われた本報告書著者とのインタビューで語っています。

しかし、2014 年 10 月に起きた 2 つの出来事に見られるように、警察にとってこの反発の影響は非常に現実的なものです。1 つ目は欧州サイバー犯罪センター長の Troels Oerting が暗号化通信を取り扱う捜査力の拡大を要求し、また、英国国家犯罪対策庁長官のキース・ブリストウもまったく同じことを要求したことです。両者とも、現在の暗号化の使用が増加していることによって捜査が妨げられており、ますます多くの人々が利用し始めている新たな暗号化システムに隠れている犯罪者の通信に標的を絞って捜査が行えることを求めています。

2 つ目は、英国の警察によるより大きな権限の要求です。その最初のものとして、トップテロ対策捜査員であるクレシダ・ディック警視庁副総監が 2014 年 6 月、「新しい通信技術の発展についていけない」ためにテロに対抗する力が低下していると、述べたのです。

しかし国民の監視は、諜報機関の「黒い要素」と呼ばれる行動だけに限りません。これは、以下のような一貫性のある複数の要素を含む全体像の一部に過ぎません。

・社会全般、特に政治家における技術意識の欠如

・政府による情報収集システムに対する効果的な監督の欠如

・開発している技術の機能と、その技術の欠点を明らかにしようとしないテクノロジー産業

・スヌーピングおよび従業員監視の大企業文化

・非倫理的な方法でデータを使用することに対する、政府内の特定のグループや個人に見られる日和見主義

・CCTV カメラシステムの市街地への設置や、スピード違反を抑止し、交通違反を罰するための交通監視カメラの使用に見られるように、技術によって監視されていることを認識させることで行動に影響を与えるように意図された文化の醸成

諜報機関の技術への依存の増大

「モノのインターネット」の急速な出現により、監視社会がさらに加速しつつあります。「モノのインターネット」では、さらに多くのセンサーが私たちの家や道路、車、ウェアラブル・デバイスに追加され、多くの場合、携帯電話に直接接続されることになります。これは、私たちの生活と身体に対する政府の監視の目がさらに拡大することを意味します。

IT 業界と諜報機関によって再設計される可能性がある監視インフラストラクチャが何の制限もなく開発されているという構図は、私たち国民の自由だけでなく、将来の社会的な発展にとっても非常に現実的な脅威となっています。

CSRI は今現実に起きていることを忠実に描写するため、ローラ・ポイトラスのドキュメンタリー映画、CitizenFour の公開に合わせて調査を実施しました。この映画は、欧米の新聞各紙が、諜報機関による国民監視の実態を詳細に報道するきっかけとなった、スノーデンとガーディアン紙との会合を記録したドキュメンタリーです。

また、自らの決断が招く結果を伝えることなく、テクノロジーコミュニティが人々をこの新しい世界へと誘い込んでいることも明らかにしています。テクノロジー業界にとって、自らの行動が招く結果を一般大衆に知らせない方が都合がよいのです。

前述したように ID カードシステムは成功せず、大衆の想像力を真にかき立てることはありませんでした。しかし皮肉なことに、ほぼ全員が携帯電話という形で ID カードを携帯することを選んだのです。携帯電話は、ID カード方式の開発者が創造もしない程大きな力を持っています。私たちの動きを追跡し、物理的またはウェブ上での行動に関する情報を提供し、私たちの会話を監視、さらには盗聴することさえ可能です。

今、政府の中では、携帯電話はいまや、これまでになかった識別・管理機能となっています。既に実用化されている他の監視技術と組み合わせることで、旧東ドイツの秘密警察シュタージが夢見るような監視の世界をもたらす機能です。かつての監視には、放射性物質の使用や、警察犬が個人の身体の臭いを認識して追跡できるようにするための訓練に使用する「臭い入り容器」を作るために反体制派の下着を回収することなどが挙げられますが、その当時の技術によって制限されていました。もっとも、シュタージは主に、すべての地域、職場、学校に広がる、お金で雇った情報提供者のネットワークを利用していました。ベルリンの壁が崩壊し、東ドイツがなくなってから 25 年経った今でも、濡れ衣を着せられたり、疑いをかけられた多くの人々の傷は消えていません。

Julia Behrends は、イタリア人のボーイフレンドがいたことで、シュタージに目を付けられた女性です。電話でその彼と会話していたとき、最後に「おやすみ、愛しているわ。それから皆さん、おやすみなさい」と、当局の盗聴について冗談を言うことさえありました。しかし、西側のコンピュータ技術にアクセスするためにボーイフレンドの仕事を利用する情報提供者となることを拒否したとき、全体主義国家の真の力を感じました。長い年月の後、「Stasiland（監視国家―東ドイツ秘密警察（シュタージ）に引き裂かれた絆）」の著者のアナ・ファンダーにその経験を語ることでさえ彼女にとっては辛いことでした。

「私に最もダメージを与えたのは徹底的な監視でした。プライベートな部分がまったくなくなるまで人が境界線を踏み越えてくることは分かっています。でも、私は間違いなく心理的に傷ついています。恐らくそれが、男性からアプローチされたときなどに、極端な反応をしてしまう原因でしょう。自分だけの空間に侵入されるかもしれないと感じてしまうのです。」

「監視国家―東ドイツ秘密警察（シュタージ）に引き裂かれた絆」アナ・ファンダー著、Granta Books 発行

今日の大量監視が、英国に住む人々にこのような影響を与えるかどうか結論を出すのは時期尚早です。実際ドイツでは、アンゲラ・メルケル首相の個人用携帯電話が NSA によって盗聴されていたことがスノーデンの告発により明らかになって以来、激しい抗議の声が上がっており、当局は国民のデジタル権を保護する措置を講じています。メルケル首相は、ヨーロッパに新しいインターネットを確立しようと呼びかけてさえいます。

2014 年に CSRI によって英国で行われたインタビューは、省庁が相互に対立する原因となっている「データ派閥」があることを示唆しています。

中でも、省庁の競合する政策のために政府機関同士が対立しており、政府機関は自らのデータにアクセスする料金を別の政府機関に請求しているケースが報告されています。

何年にもわたって CSRI が収集した証拠は、英国民のデータ所有権の文化により、個人データは信頼によって保有される機密情報ではなく、国の財産であると考える「データ強硬派」が生まれていることも明らかにしています。

この見方は、テクノロジーバイブルである Computer Weekly の元調査責任者であるトニー・コリンズによっても裏付けられています。彼は、2002 年にガーディアン紙に掲載された政府の巨大 IT プ

ロジェクトに関する記事で、次のように述べています。「我々は何故心配する必要があるのでしょうか？結局、これらすべてのプロジェクトの運命は、議会に対して責任を負い、最終的には一般大衆に対して責任を負う閣僚達によって決定されます。しかし現実には、重要な意思決定を行っているのは選挙で選ばれた政治家ではなく、役人たちです。確かに、かつては単に影響を与えるだけだった役人が政治を動かしている証拠が増えつつあります。同時に、選出された議員と任期のない官僚の両方に対して、議会が責任を問う力が大幅に弱まっています。」

「政府の仕組みは技術的にますます複雑になっています。この複雑性に追い打ちをかけているのは、政府機関の運営を監督している信じられないほど入り組んだ規制、法律、改正および相互に結びついた慣例で、就任して比較的日が浅い閣僚は、官僚の完全な協力がなければ、自分の政府機関の日常的運営を理解できる望みがないことは明らかです。」

「一言で言えば、複雑性はビッグ・ブラザー（官僚）に有利に働いています。これが原因で任期の短い閣僚の仕事が選挙の心配のなく、任期もない官僚の手に委ねられているからです。」

コリンズは、またこうも指摘しています。「じりじりとビッグ・ブラザー国家になりつつあるこの国を止めようとしている市民的自由の擁護者は、克服できそうもない障害に直面しています。監視技術使用に対する反対論は、テロリズム、詐欺、脱税、不法移民の打倒を唱える賛成論に比べて脆弱です。さらに、政府機関は巨額の予算を獲得し、新しい集中型システムを導入することによってホワイトホールの名声を得ていることも現実です。プライバシーの損失に警鐘を鳴らす市民的自由の擁護者の影響力は、議会に対する官僚の力が強まるにつれ、徐々に薄れていくものとなるでしょう。」

「テクノロジーがますます幅を利かせている世界において、ビッグ・ブラザー国家は、商業目的を追求する企業と、中央権力の統合・拡大を目指す官僚機構の自然な欲求による共生的関係の必然的な結果かもしれません。両者とも、新技術の導入を通して目的を達成することができます。そして、自由主義の利益は脇に追いやられます。」

プライバシー・インターナショナルの創設者であるサイモン・デイビスによると、このことが、公務員がデータとプロジェクトの所有者であるかのような態度を取る原因となっているということです。

真偽のほどは分からないものの、議会において、公職に就く前に開始されていることが多いコンピュータ・プロジェクトの失敗責任を政治家に問える見込みは薄く、また、マルコム・リフキンドの下院情報安全保障委員会などの監督機関が諜報機関の活動に関する報告を十分把握しているようにも思えません。

これは、リフキンド卿のスノーデン疑惑に対する以下のコメントからも明らかです。「我々の調査の焦点は、彼らは法律を破ったか？または法律を破ろうとしたか？ということです。報告書に記載した理由で、いや、破らなかった、というのが、全会一致の率直な答えです。これ以上は GCHQ ではなく、政府と議会の問題となります…このため、我々はもっと広い法的枠組みをじっくり検討する必要があるのです。」

「もちろん、PRISM 疑惑について我々が行った調査は、GCHQ の行為の合法性に関わる新しい捜査権規制法の直接的影響の中で開始されています。光ファイバーケーブルへのアクセスといった問題については、違法に行われたという兆候はありません。それが望ましいかどうか、または正当な公共の利益のためになるかどうかということが問題なのです。」

リフキンド卿の回答は、**GCHQ の活動の監視責任を負う委員会が、GCHQ の活動内容を完全に認識していなかった**ことを示唆しています。通常これは政府内での委員長辞任理由となりますが、この場合は、検討されなかったようです。

諜報機関の技術への依存の増大

ID カードを導入する試みは、政府高官の間で「強硬派」政策があったことを示す証拠として考えることができます。マーガレット・サッチャーによる ID カード再導入の試みは、1996 年にジョン・メージャー首相によって受け継がれました。その計画に反対していたトニー・ブレアはその後 ID カードを導入し、その方式はゴードン・ブラウンによって受け継がれましたが、2010 年に保守党が自由民主党との連立政権を組んだ後、破棄されました。

この強硬データ政策が原因で、テクノロジー業界で個人に関する既知の全データを保存する「単一顧客プロフィール」の政府版を開発することを目的に、個人の単一識別記号を作る数多くの試みが行われました。英国が監視の悪夢に迷い込んだもう 1 つの理由として挙げられたのは、政府全体、特に政治家にテクノロジーに対する理解が欠如していることでした。その結果、英国における国民監視が増加し、政府による「ビッグデータ」監視の機会も増加しています。皮肉なのは、数多くの政府 IT 構想、特に保健省での失敗により、「ビッグデータ」を使用した政府の支出削減を達成する機会が失われていることです。

このような、実用的テクノロジー知識の欠如を示す例が多く存在します。内部の情報源によって得られた最ものっぴきならない証拠は、2000 年に英国電子商取引法案の作成に携わった国会議員が、いくつかの問題を把握するために 2 週間の集中講義を受ける必要があったことです。

この法案で最も物議を醸したのは法執行問題を定めた条項でした。当局が、データを暗号化した鍵を持っていると「思われる」人なら誰でも、令状を発行することを許す文言を盛り込んだため、公民権擁護団体を激怒させました。また、調査を受けている者が、自らのケースについて話すことを防ぐ「ティッピング・オフ（情報提供）」罪も含まれていました。彼らの唯一の救済は、秘密裁判で不服を申し立てることでした。

状況はそれほど大きく変わっていません。2012 年にケンブリッジ大学が発表した報告書は、国会議員の中で科学技術専攻の卒業生が非常に少ないこと、そしてダイアン・コフィとジュリアン・ユペールの 2 人しか博士号を持っていないことを指摘しました。

コリンズが指摘したとおり、IT 分野における政府の欠点は監視分野における技術の進歩について政治的な監視機能が全般的に欠けていることです。これはスノーデンによる暴露によって証明されており、ユペールがこの分野において自由民主党の対応を指揮したことは注目に値します。

「ビッグ・ブラザー」を構築する

英国政府による技術システムの実験の始まりはサッチャー時代に遡ります。当時政府は IT を通じて理解を深めようとしており、マーガレット・サッチャー首相の有名な「ガラクタを入れればガラクタが出てくる」というコメントが生まれました。

サッチャー首相にとって、テクノロジーには見直しが必要であり、データベースを整理して目的に適合するよう作り替えられる必要がありました。1980 年代終盤に物議を醸したのは、ロンドンの中心部にある 40 の政府機関間を接続するシステムの政府データネットワーク（GDN）の発表でした。

「ビッグ・ブラザー」の包括的データベースの始まりであるという反発の可能性を考えた官僚達は、データはそれを「所有する」政府機関にとどまり、どこにも移動されないと急いで付け加えました。

ただし、ある英国政府機関のコンピュータ部門長を努めていた元高官によると、GDN はさまざまな政府機関に保存されている全情報から単に 1 つのデータベースを作成するもので、システムで最高のアクセス許可レベルを使用すれば全体を検索できるというものでした。

この発言の信憑性は、HMRC（税金）システムの開発に携わっていた元公務員による信頼できる証言によってさらに高まります。この元公務員は、これらのシステムはいずれも諜報機関によって完全に合法的に取り調べられることができると指摘したのです。その点は、データ保護委員会の元委員長で、今年亡くなったノーマン・リンドップ卿によって認められました。

死亡記事によると皮肉なことにコンピュータが嫌いだったノーマン卿は、数々のインタビューで、データ保護委員会は政府自身がプライバシーにとって最大の危険であると考えていたと述べました。それにもかかわらず、ノーマン卿は委員会の提言に変更を加えるよう強制されました。その結果、1984 年のデータ保護法で、法律を無視してその活動を追求できる完全な自由を警察権力に与えることになりました。

ノーマン卿の不安は現実のものになりました。委員会の提言の結果設立されたデータ保護登録機関は、現在情報コミッショナー・オフィスと改称されており、**歴代の情報コミッショナーは、市民的自由は今、監視国家によって危険にさらされている**と警告しています。

2004 年、情報コミッショナーのリチャード・トーマスは、英国は知らない間に東ヨーロッパに似た監視社会になっているとし、個人に関するデータを収集する英国政府の権力に対する具体的な懸念を示す声明を発表しました。

同情報コミッショナーは 2006 年、「監視社会に関する報告書」と題された文書を発行しました。本書では、一人ひとりの生活の細部にわたる実態を浮かび上がらせるために様々な情報源から収集された私たちの情報の集積を「データベイランス」と呼び、国がデータベイランスの方向へ進んでいることに対するコミッショナーの懸念が詳細に記されていました。

この報告書は、情報コミッショナーの依頼を受けてサーベイランス・スタディーズ・ネットワークとよばれる研究者グループによって作成され、情報コミッショナー事務局が主催し、ロンドンで開催された第 28 回データ保護・プライバシーコミッショナー国際会議で発表されました。

2010 年、サーベイランス・スタディーズ・ネットワークは内務特別委員会の求めに応じて報告書を 2006 年版に更新しました。この報告書は、いくつかのデータ保護措置が導入されたものの、私たちの私的生活に監視が侵入する可能性は実際に高まっていることを明らかにしました。

2012 年 6 月、エドワード・スノーデンは、名目上米国と英国政府に報告義務を負う諜報機関によって開発された監視技術の高さを暴露しました。データ保護委員会議長ノーマン・リンドップ卿と、リチ

ャード・トーマスおよびクリストファー・グラハムの両情報コミッショナーの懸念が現実になったことが証明されたのです。

次の政府のイニシアティブ

英国政府筋によると、政府は今後数週間以内に（2014 年 11 月）政府サービスへのオンライン・アクセスを提供する一連の手順の最初である、最新のジョイント・イニシアチブを立ち上げます。

金融筋によると、**Government Digital Services Identity Assurance Plan と呼ばれるシステムを使用して、国民が政府サービスにオンラインにアクセスできるようになります**。このシステムは、ボーダフォン、信用照会企業の Experian、郵便局、そしてオランダ企業の Digidentity の 4 組織から本人確認手続きを選ぶことができる選択肢を提供します。

政府は、この方式の第 2 回入札で、本人確認サービス提供企業を増やすことを予定しています。この動きは、アイデンティティの所有権についての議論を激化させることになるでしょう。また、自分の身元を証明するために企業を政府との取引関係に引きずり込むことで、社会における監視利用が増加することも明らかに示しています。このグループにボーダフォンを入れたことは、私たちが使用しているモバイルデバイスによって身元を証明できるという主張につながる可能性があり、特に賛否両論を巻き起こすでしょう。携帯電話を「ポケットスパイ」と捉える考え方につながる可能性があります。

この技術の開発検討に関わった筋が本報告書の著者に語ったところによると、このシステムでは、サービスの利用を希望するユーザは、自分が企業に既に提供しているデータか、または企業が保存しているデータから抜き取られた一連の質問に答えることになります。

与えられた答えにより、その質問に答えている人物が実際に主張している本人であることを示す確率を示すスコアが出されます。このデータが、政府が保持するデータと組み合わされて、総合スコアが算出されます。

英国銀行業界はこの方式に参加することを求められましたが、想定される参照料金が 1 ペニーであり、政府は銀行が結合データを抽出して、信用スコアリングに使用することを許可しないため、参加を辞退しました。

この開発は、公務員によって使用される政府データへの包括的アクセス・システムであるマーガレット・サッチャーの Government Data Network（政府データ・ネットワーク）の恐るべき対称物としての役割を果たします。今回の唯一の違いは、システムが一般大衆によって使用されることです。

ユーザによるインターネット使用の記録が政府によって保存されるかどうかははっきりしませんが、これまでの金融コミュニティとの話し合いは、個人の総合スコアに関するデータを保存することができることを示唆しています。

さらに重要なことに、CSRI と接触した、政府と金融システムに精通した専門家によると、政府ウェブサイトとの情報交換によって生成されるすべての重要メタデータは、スノーデンによって明らかにされた既存のプロジェクトのもと、諜報機関が求めればそれに応じて提供されます。ただし、既に指摘したように、諜報機関は既に公共部門が持つデータへのアクセス経路を多数確保しています。

「GCHQ はネットワーク・トラフィックを監視し、メタデータを非常に長期間保存するため、過去にさかのぼって情報の断片をつなぎ合わせて全貌を得ることができます」と、元政府筋は述べています。

隠すものがなければ、恐れることは何もない？

政府のスポークスマンによると、新たなインターネット・エンゲージメント・システムは、プライバシー・コミュニティを入札に参加させることで、監視に対する不安を和らげるために可能な限り透明な方法を用いて慎重に開発されています。

米国では、個人が本人であることを証明する目的で、Google の認証を使用して同様の ID 認証システムが開発されています。いずれかの政府機関または他のオンラインデータベースが、ある一人の国民について不正確だったり、古かったり、無関係だったりする個人データを取得すると、その間違った情報はシステムに永久に残ってしまいます。

他の欧州連合の国々とは異なり、英国は欧州司法裁判所の「忘れられる権利」判決の遵守を拒否しています。この立場を強化するため、議会は 2014 年の夏休み閉会前に、新しい法律を急いで通過させました。これにより、データを保存し、何年も経った後に再利用する権利が警察、セキュリティ・サービス、および政府機関に与えられます。2 人の国会議員（保守党のデービッド・デイビスと労働党のトム・ワトソン）は、市民的自由運動である「リバティ」の支援を受けて、この法案（DRIP）を覆す司法審査を求めています。

エドワード・スノーデンが初めて機密を暴露したとき、当時の外相ウィリアム・ハーグは大量監視について国民を安心させようと、独特の言い回しを使いました。それは、「隠すものがなければ、恐れることは何もない」というものです。しかし、スノーデン事件の予期されない影響により、数十万の罪のない人々が非常に高度な情報監視システムを恐れる正当な理由があることが証明されました。

リーク記事を執筆しているジャーナリストは、攻撃の的になっていました。スノーデンの伝記執筆者であるジャーナリストのルーク・ハーディングは、CSRI 調査チームに対し、自分のコンピュータが誰かにハイジャックされた経験を語りました。

「私はハートフォードシャーの自宅で原稿を書いていました。NSA が米国のハイテク企業とその財務状況にダメージを与えたというような NSA を非難する記事を書いていると、目の前でカーソルが右から左へと動いて文字を消し、書いていた章を勝手に削除したのです。奇妙な出来事でした。怖いとは言いませんが、変だなと思いました。私はオフラインで作業していたし、セキュリティ対策として、Truecrypt フォルダにすべてのドキュメントを保存していました。

この現象が続いたため、私はついに謎の読者/秘密の編集者に宛てて『おい、君がこれを読んでいるのは分かっているが、どうか削除しないでくれ』というメモを残したほどです。これは約 1 カ月間続き、ガーディアン紙の同僚がこの出来事を新聞に書いた後、止まりました。

今では、あれが NSA の仕業だったのか、私の古い友人であるロシアの仕業だったのか、分かりません（ハーディングはかつてジャーナリストとして働いていたロシアから国外追放されたことがある）。分かっているのは、誰かが私のラップトップに侵入したということだけです。おそらく、お前を監視しているぞという意思表示と、私が書いていた内容の一部を非難することが目的だったのでしょう。」

他のあちこちで、**警察がジャーナリストを捜査権限規制法（RIPA）適用のターゲットにしています**。この法律によって、データを取得する必要性を裁判官に納得させて正式な令状を取らずに、電話、コンピュータ、またはデジタル記録を押収する権利が警察に与えられています。今や、令状の発行を義務づけている「警察及び刑事証拠法（PACE）」よりも、RIPA が好んで使用されるようになりました。ジャーナリストは、英国の報道の自由の基盤である、情報源のプライバシーと匿名性を守らなければならないため、収集したデータを進んで引き渡すことは絶対にありません。Press Gazette 紙は 2014 年 10 月、サフォーク、ケントで各 1 件、テムズバレーで 2 件、警察が関わった事件を報

じています。それぞれの事件で、警察官が令状なしにジャーナリストの通話記録を押収しました。Milton Keynes Citizen 紙の記者は、車に盗聴器を仕掛けられていました。

現代の監視はその性質上、コンピュータ・システムによる機密情報収集を行い、アルゴリズム、人種プロファイリング、またはその他の生活様式の特性に基づいて疑惑がかけられるため、人々が濡れ衣を着せられることになります。最近の例としては、テロ騒ぎがあったバルセロナから飛行機で英国に到着したパキスタンのムシャラフ大統領の個人スタッフ・メンバー5 人が逮捕された事件があります。

この他、同様の事件が起きるのを実際に恐れる必要があるのは、Don't Spy on Us、米国の姉妹組織である Stop Watching.us、アムネスティ、プライバシー・インターナショナルやリバティなどの人権慈善団体、change.org、38degrees、avaaz.org などのような署名サイトかもしれません。デザイン会社 Superflux によって作成されたインタラクティブ・バッジ（写真参照）など、クリエイティブな抗議行動も生まれています。このバッジは、着用した人が Bluetooth 経由でバッジに SMS メッセージを送信すると、そこから当局の注意を喚起する「トリガー」用語が抽出され、点滅表示されます。Superflux Open Informant の詳細については、www.futureintelligence.co.uk/whos-watching-the-watchers を参照してください。

個人レベルで内情に通じているのは、仮想プライベート・ネットワーク（VPN）などの暗号化サービスの購入者、「暗号パーティー」に参加して Truecrypt または PGP メール（PGP は Pretty Good Privacy の略）などのプライバシーおよび匿名ツールの使用方法を学んでいる人です。彼らは、Google、MSN、または Yahoo といった、スノーデンによって GCHQ および NSA と共謀して大量監視の片棒を担いでいた企業の代わりに、Mozilla の Firefox ブラウザを選ぶことになるでしょう。Firefox はまた、Lightbeam という無料アプリケーションを提供しています。このアプリケーションは、インターネット上でユーザが何かを検索するたびに企業がユーザの嗜好についてサードパーティと共有している情報をリアルタイムで可視化します。The Onion Router（TOR）は、匿名性を提供するもう 1 つのオプションです。

技術系企業、警察、および政治家は、暗号化はサイバー犯罪およびテロとの戦いの邪魔になると主張します。彼らは、商業的、政治的、運用上の理由から、私たちの通信すべてに自由にアクセスすることを望んでいるはずです。スノーデンによる告発から 2 年が経ち、インターネット・ユーザは、自分がポケットやバッグにスパイ機器を持ち運んでいるという事実にやっと気づきつつあります。GPS 衛星がユーザを追跡しており、家庭内外のセンサーと何百万もの CCTV カメラがユーザの一挙一動をすべてデータベースに集積しています。今日の英国では、旧東ドイツのシュタージのように市民社会に潜入捜査官を潜り込ませる必要はありません。実際に、私たちは自らを盗聴しているのです。Wifi を有効にしたタブレットとスマートフォンを常にオンにして、ひっきりなしにつぶやいたり、メッセージを送信したり、情報を投稿したり、共有したりすることで、新陳代謝するようにデータを繰り返し残しているのです。

本調査のスポンサーであるフィンランド企業、エフセキュアのマネージング・ディレクターであるアラン・スコットは、自らを「チーフ・デジタル・フリーダム・ファイター」と呼んでいます。「私たちは部族社会に回帰しつつあります。部族社会で人々は人前で裸で過ごしていましたが、私たちは全世界の前

で裸になっているのです。私たちは実際に原点に戻って、**インターネットで自分の行動をすべてむき出しにしている**のです。この状態はあまりにも急速に起きているため、人間はすぐに適応することができません。ティム・バーナーズ・リーがウェブを考案したとき、http は 1 ページだけでした。今や、何百万ものアプリケーション、数十億ビットのデータが存在します。ここ 2 年間で、それまでに全宇宙に存在していたより多くのデータがインターネット上で作成されました。」

次は何が起きるのでしょうか？スノーデンの映画「CitizenFour」は、現在映画館で上映されており、友人や家族と楽しみながら意識を高めるのに適しています。映画鑑賞に加え、私たちのデジタル権利を保護するトレーニングと製品を購入する機会もあります。政治レベルで英国政府は、国民健康サービスの診療記録、ユニバーサル・クレジット、本人確認、およびデジタル・バイ・デフォルトを通してさらに多くのデータ収集に投資しています。ビッグ・ブラザーはさらにビッグになりつつあります。私たちは本当に何も恐れることはないのでしょうか？