特集／AI・サイバーセキュリティと安全保障

〈2〉ポスト・スノーデン時代のサイバー防衛 ― 米国主導の国際協力の現在地 ―

一般社団法人先端技術安全保障研究所（GIEST） 所長 小沢 知裕

1. スノーデン暴露から 12 年 …… 227
2. オバマ大統領の対応 ― PPD-28 発令 …… 228
3. 活発化したサイバー能力構築支援 …… 229
4. 5 年後に始まったハントフォワード作戦 …… 230
5. サイバー情報機関の連携は変化せず？ …… 231
6. スノーデン暴露は「触媒」だったのか …… 232
【年表】 …… 233

1. スノーデン暴露から 12 年

2013 年 6 月に始まったエドワード・スノーデン（Edward Snowden）による大規模な暴露はショッキングなものだった。この暴露によって、米国のサイバー情報機関である NSA（National Security Agency：国家安全保障局）や中央情報局（CIA : Central Intelligence Agency）、捜査機関 FBI（Federal Bureau for Investigation：連邦捜査局）が、通信のメタデータ（誰と誰がいつやり取りしていたかといった情報）や、インターネット上の個人的なデータ、E メールやビデオチャット、保存したファイルの中身、ウェブサイトの閲覧履歴などといった多種多様な情報に個別の司法手続きなしにアクセスできていたことが明らかとなったのである[1]。この当時、スノーデンは NSA の契約社員だったが、内部資料を持ち出して新聞社に提供し、香港へ（後にロシアへ）と逃れていた。

これらの情報が米ビッグテック各社の協力によって、PRISM というシステムを介して提供されていたこともまた世界に衝撃を与えた[2]。例えばマイクロソフト社の Windows は最も普及した PC 用 OS（Operation System : 基本ソフト）であり、大半のパソコンが採用しているし、Google の無料 E メールサービス Gmail を使う人や、同サービスの提供するオンラインストレージ、G ドライブにデータを預けている人たちも多いことだろう。フェイスブックやツイッター（現 X）にプライベートな写真や情報を掲載している人や、iPhone を始めとする米国製のガジェットを使う人々も決して少数派ではない。米情報機関の監視網はインターネットに乗って世界中に広がり、個別の司法判断なく情報が収集され閲覧さ

れていたのである。

また、同組織が収集した膨大な情報を閲覧するために専用の検索システムが用意されており、XKEYSCORE（エックスキースコア）と名付けられていたことも明かされた。スノーデンはその証言の中で、同システムの画面でキーさえ叩けば（そして、その相手の個人的なEメールさえ手元にあれば）、その相手が誰であっても、たとえ連邦判事や大統領であっても盗聴（wiretap）することが可能だったとしている（当時の米下院情報委員長はこれを否定している）[3][4]。

さて、今ではこれらの暴露も、もう既に一昔前のこととなったわけである。とはいえ、その影響は忘れがたく大きなものだったし、その後、世界がどのように変化したかを今振り返ってみると、その大きさが見えてくる。いったい何が変化したかのかを整理しよう。米情報機関による情報収集方法の変化（大量監視の非合法化）はもちろんのことであるが、米欧の個人情報の保護規則の変化もまた、より厳しいものへの変更を迫られた（年表を参照）[5]。この動きは、2018年のGDPR施行を含む数度に渡る米欧間の個人情報共有フレームワークの作り直しへとつながった[6]。

そして、スノーデンの暴露以降、米欧を含む西側諸国のサイバー防衛戦略の変化にも多大なものがあった。本稿では、12年を経た現在地から眺めてその変容を整理したい。まず、米国務省の主導するサイバーセキュリティにおける国際協力（他国に脅威情報共有、能力構築などを行う）の拡大傾向を確認し、それがスノーデンの暴露以降に大きく発展していることを示す。但し、同時にそのような活動自体はスノーデン以前から始まっていたという事実も指摘する。また特に、その方向性における究極の国際協力ともいうべき「ハントフォワード作戦（Hunt Forward Operations : HFOs）」の拡大を紹介する。

また、サイバー空間における信号インテリジェンス活動（SIGINT : Signal Intelligence、インターネットなど通信に関連したスパイ活動）においてファイブアイズ（米国以外は英国、オーストラリア、ニュージーランド、カナダ）やドイツ、日本などとNSAが連携しており、大量監視のインフラを担っていたことを紹介する。この面において、スノーデンの暴露は、一時的に一部抑制する方向で影響を与えたようであるが、促進するものでもなかっただろう。

2. オバマ大統領の対応 ― PPD-28発令

NSAによる市民へ向けられた大量監視（mass surveillance）は問題視されたが、同組織による同盟国や友好国の政府に対する盗聴もまたスノーデンの暴露によって明らかとなり、問題視された。盗聴の対象としては最初にドイツ首相メルケル、そして2年後には日本を含む4か国（ドイツ、フランス、ブラジル、日本）が含まれていたことが暴露された[7][8][9][10]。このとき、各国の首脳たちはトーンこそ異なるものの、それぞれに米国政府を非難している。しかし、その後、ドイツがNSAの指示でフランスを盗聴していたことが判明し、メルケル政権も議会や国民の非難を浴びることとなる[4][11]。スノーデンによる暴露事件は、ホワイトハウスにとどまらず、同盟国の首脳や情報機関といった重要な協力者たちのメンツをも潰すことにもなった。

このような外交的ダメージを踏まえて、当時米大統領を務めていたバラク・オバマは暴露から半年後に大統領令PPD-28を発行した。この大統領令では、米政府機関のSIGINT活動において、市民はその尊厳やプライバシーが尊重されること、この方針は諸外国や外国人にも適用されることなどが謳われている[12]。活動内容が露見した場合のアメリカへのダメージを考え、慎重に対象を選び、米国民はもちろんのこと、外国人に対してさえ不用意にプライバシーを侵すようなことはしないというポリシーを表明するものであった。アメリカはこのとき、政治的な目的のインテリジェンス活動を継続すること自体は撤回しなかったが、そこに一定の節度を持たせることを約束し、火消しに努め、各国との協力関係の維持と再生を図ったのである。

自国民や諸外国からの一連のリアクションを考えれば、必要以上に個人情報を集めることは、暴露の危険性を鑑みた場合に得策ではないことは明らかだった。米国の情報機関は、恒常的かつ無差別にプライベートな情報を収集せずとも、外国情報活動監視裁判所（Foreign Intelligence Surveillance Court : FISC）の承認を得ることによって、必要な個人に対する捜査を行うことができる。そして、それら申請への許可は通常、下りる[13 : 59ページ]。もちろん、この

やり方を取るとなると、以前に比べればプロセス自体は煩雑だろう。しかしこの方法に従う限り、情報機関の手元に残る情報は、万が一暴露されることがあっても、その収集理由の正当性を示すことができるものだけとなる。また、大量の不必要かもしれない情報の中から必要な情報を見つけ出す作業は、情報分析者にとって重荷となるだろう。これは「小麦かもみ殻か」問題などと呼ばれる情報活動における課題の一つである[14：89-90ページ]。収集した理由の正当性を説明できない大量の個人情報を保持し、それが流出しないように保護しつづけるコスト、流出した場合の外交関係へのダメージ、そして情報分析における作業負荷なども考えれば、PPD-28で決定された方針は経済効率的でもあるわけである。

3. 活発化したサイバー能力構築支援

スノーデンの暴露後、米国の情報活動への懸念が高まり、特に米欧間の信頼回復の必要性が訴えられた[15]。信頼回復に向けた措置にはPPD-28のような方針の表明以外にも、情報機関の活動の透明性を示すことなどが考えられる。また、サイバー防衛における国際連携の強化により、米国と諸外国との間で人的交流、専門技術のシェアを進めることもまた、信頼関係の再構築につながるだろう。スノーデンの暴露前後で、米国の諸外国に対する支援活動に変化は見られるだろうか。ここで、主要な支援活動として、サイバー能力構築支援（capacity building）における変化を見ていく。

米国によるサイバー能力構築支援活動はスノーデン事件以前から各国で行われてきている。しかし、スノーデン暴露以後に大きく進展してきている様子も見える。例えば、アフリカにおいては米国務省が中心となって、サイバーセキュリティ関連のワークショップが繰り返し開催されている（表1）。これらは、アフリカ諸国に携帯電話網が広く普及していることを踏まえ、国営のコンピューター緊急対応チーム（CERT：Computer Emergency Response Team）の設置などを課題として、アフリカ諸国数か国を対象として行われたサイバー能力構築支援活動であった。なお、一部のワークショップでは南米諸国も招かれている。

米国務省は司法省などと協力して、アフリカ諸国で、主に使用言語地域別にサイバーセキュリティ及びサイバー犯罪のワークショップを開催してきた。その活動は2011年夏から始まっているが、スノーデンによる暴露の始まった2013年夏までに累計17か国を対象として実施されていた。そして、その後もこの試みは継続され、2017年には倍以上の39か国まで拡大している。

時　期	開催地	参加国（太字は新規参加国）	参　照
2011年7月25日～27日	ケニア首都ナイロビ	**ブルンジ、ケニア、ルワンダ、タンザニア、ウガンダ**	[16]
2012年9月27日～28日	セネガル首都ダカール	**セネガル、ベナン、ブルキナファソ、カメルーン、コートジボワール、コンゴ民主共和国、ギニア、ニジェール、トーゴ**	[17]
2013年1月29日～31日	ガーナ首都アクラ	ケニア、**セネガル**、**南アフリカ**	[18]
2014年6月4日～6日	ボツワナ首都ハボローネ	**ボツワナ**、コンゴ民主共和国、**ガーナ**、ケニア、**レソト**、**マラウイ**、**モーリシャス**、**モザンビーク**、**ナミビア**、**セイシェル**、南アフリカ、**スワジランド**、タンザニア、**ザンビア**	[19]
2015年9月22日～24日	モザンビーク首都マプト	モザンビーク、**アンゴラ**、**ブラジル**、**カーボベルデ**、ガーナ、ケニア、モーリシャス、**ナイジェリア**、**ポルトガル**、**サントメプリンシペ**	[20]
2017年6月12日～15日	モーリシャス	ベナン、ブルキナファソ、カーボベルデ、**ガンビア**、ガーナ、ギニア、**ギニアビサウ**、**象牙海岸**、**リベリア**、**マリ**、ニジェール、ナイジェリア、セネガル、**シエラレオネ**、トーゴ	[21]

表1. 米国務省によるアフリカにおけるサイバー能力（構築）支援活動