警察政策学会資料　第82号
平成27（2015）年 9 月

米国国家安全保障庁の実態研究

警察政策学会

テロ・安保問題研究部会

『米国家安全保障庁の実態研究』のウェブ公開に当って

１　我が国でインテリジェンス強化が議論されるようになって久しい。しかし、残念なことに、インテリジェンス諸活動の中でも極めて重要な、或いは最重要なシギント活動について、国民の関心や知識が向上しているようには見られない。本資料は米国のシギント活動について研究したものであるが、出版から3年目を迎えたので、少しでも国民のインテリジェンス・リテラシー向上に資するために、ウェブ上でも公開することとした。

２　本資料の資料源は、米国政府による開示資料（積極的開示資料と情報公開要求を受けての開示資料)、ウィリアム・スノーデンその他の米国国家安全保障庁勤務員による漏洩資料、これらに基づいた分析報道その他の資料であり、これら資料を総合的に分析したものである。

2015年の本資料発刊後も、新たな資料の開示・漏洩があり、本資料にも加筆すべき部分も多くなってきた。しかし、本資料自体に誤りがある訳ではないので、今回はそのまま公開することとした。但し、次の2点については留意されたい。

（１）「第1部第2章５　NSA の活動の根拠と法的規制の構造」（17～19頁）「第２部第２章１（５）対外諜報監視法2008年改正法等」（40～41頁）の部分については、2017年警察学会資料第94号「米国における行政傍受の法体系と解釈運用」で更に詳細に分析したので、そちらを参照されたい。

（２）「第3部第1章１（２）GCHQ の沿革と UKUSA 協力関係イ」（183頁）については、別紙のように訂正する。

平成30年1月

日本大学 危機管理学部教授
茂田　忠良

（別紙）

第3部第1章１（２）GCHQ の沿革と UKUSA 協力関係

イ　米英協力関係の進展と UKUSA 協力関係の成立（本文183頁）

米英両国は、米国の第二次世界大戦参戦前、1940年前半には既に秘密裡にインテリジェンス（主としてヒューミントと防諜面）の協力を開始し、更に1941年2月にはシギント面での実質的な協力も始まり、大戦中、両国は密接に協力した。そして大戦後の1946年3月に BRUSA 協定という秘密協定を米英両国で締結して、戦後のシギント協力関係を定めた。BRUSA 協定は1954年に英国からの要請により名称を UKUSA 協定と改名し[1]、その後は、一般に1946年に遡って UKUSA 協定と呼んでいる[2]。

また、UKUSA 協力には、カナダ、豪州、ニュージーランド（以下、NZ）の旧大英帝国自治領も参加している。これら諸国と米国との協力関係も第二次世界大戦中の協力に遡る。但し戦後、加豪両国の秘密保全能力に対して米国が危惧を抱いていたため、正式参加は遅れ、カナダの参加は1949年に米国との間の CANUSA 協定締結により実現した。また、豪州は1953年に BRUSA 協定を準用して参加した[3]。豪州のシギント機関には、NZ 政府職員が派遣され、豪州政府のみならず NZ 政府のためにも運営されていた[4]ので、1953年の時点から NZ も UKUSA 協力関係に参加したものと扱われている[5]。ここに、現在にまで継続している UKUSA5か国の協力関係が成立したのである。なお、NZ は、1977年に同国独自のシギント機関を設立したため、同機関は当初豪州の附属組織として参加していたが、1980年に UKUSA 協力関係の直接当事者となった[6]。

---

[1] NSA, "Six Decades of Second Party Relations," Cryptologic Almanac 50th Anniversary Series, updated 28 February 2003, accessed 6 May 2016, https://www.nsa.gov/news-features/declassified-documents/crypto-almanac-50th/assets/files/six_decades_of_second_party_relations.pdf

一部に、BRUSA 協定が1943年に締結され、UKUSA 協定は1946年に締結されたとする説があるが、間違いである。なお、UKUSA 協定への改称は、1954年中の9月以前になされている。

[2] NSA, *UKUSA Agreement Release 1940-1956,* accessed 2 May 2016, https://www.nsa.gov/public_info/declass/ukusa.shtml

[3] Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book I: The Struggle for Centralization, 1945-1960* (Center for Cryptologic History, 1995), 19, accessed 5 May 2016, https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_i.pdf

[4] NSA, *New UKUSA Agreement - 10 May 1955*, accessed 2 May 2016, https://www.nsa.gov/news-features/declassified documents/ukusa/assets/files/new_ukusa_agree_10may55.pdf

特に、本資料中の Appendix J を参照。

[5] Johnson, *op. sit.,* 17.

[6] NSA, "Six Decades of Second Party Relations.
--Johnson, *op. sit.,* 16-19.

まえがき

（１）世界最強のインテリジェンス機関：米国家安全保障庁

米国は、世界最強のインテリジェンス国家である。国家諜報長官 DNI を中心に、中央諜報庁 CIA、国家安全保障庁 NSA、国家地理空間諜報庁 NGA、国家偵察局 NRO、国防諜報庁 DIA、陸海空軍・海兵隊の各軍諜報諸機関、連邦捜査局 FBI 諜報部門を中核とする１７の諜報組織が強力な諜報コミュニティを形成し、世界最強の米国を支えている。世界最強の米軍も、単に優れた兵器・兵站・指揮能力のみではなく、その諜報力に支えられている。米国の外交力も、（他国の国家外交機密の取得を含む）諜報力に支えられている。米国のテロ対策も、その諜報力に支えられている。その経済力にも、諜報力の恩恵が及んでいる。

これらの諜報システムの構築運営のため、米国は長期に亘り膨大な費用と最高の人材を注ぎ込んできた。現在でも、例えば 2014 会計年度の連邦政府の全諜報予算は７０８億ドルで、邦貨に換算すれば８兆円以上の巨費を投じている。また、2009 年 9 月の国家諜報長官の発言によれば、インテリジェンスに従事する職員数は約２０万人であるという。

その諜報力の中心にあるのが、シギント機関の国家安全保障庁 NSA である。元 NSA 職員で NSA 研究家でもあるジェームス・バムフォードによれば、NSA は世界最強のシギント機関であり、世界最強の諜報機関であるという。しかし、その実態は、米国の諜報諸機関の中でも特に秘密のベールに包まれ、部外者、特に米国以外の一般人には知る術も無かった。

（２）エドワード・スノーデンによる告発と機密資料漏洩

ところが、2013 年 6 月、エドワード・スノーデンという NSA に勤務する若者が、NSA に関する膨大な機密資料（トップシークレット）を漏洩し、世界中の誰でもがその多くに接することが可能となった。

エドワード・スノーデンは、2013 年 5 月、勤務地のハワイから香港に無断で出国。６月に至り同地でグレン・グリーンワルド、ローラ・ポイトラス等３人のジャーナリストに会い、インタビューに応じて「米国の諜報諸機関は、国民の知らないうちに、強力な情報収集システムを構築し、米国は監視社会となっている。政府は国民の同意なしに国民のプライバシーを侵害しており、これは民主主義の存続に対する脅威である。」旨告発すると共に、大量の機密資料を提供したのである。その分量は今以て不明であるが、数万件以上（100 万件を超える可能性もある）とされており、米国インテリジェンス史上、最大の情報漏洩事件となった。

この告発と資料漏洩を契機に、英国紙「ガーディアン」米国紙「ニューヨーク・タイムズ」「ワシントン・ポスト」ドイツ誌「シュピーゲル」等の世界のマスメ

ディアが報道を開始した。現在、マスメディアによる報道は若干下火になったものの、多くのウェブサイトで膨大な漏洩資料が掲載され、「インターセプト」等独立系のジャーナリストも参入しての分析報道が続いている。

このため、NSA はインテリジェンスに関心を有する世界中の人々の注目を集めることとなった。

（３）スノーデンの行為の評価と対応

さて、スノーデンによる NSA 告発と資料漏洩をどう評価するべきであろうか。

実は、その評価は、立場によって異なるものであろう。

先ず第１に、米国政府にとっては、スノーデンの行為は、国家機密の漏洩行為であり、国家反逆行為であって、厳罰に処すべき人物であるのは明白であろう。彼は、世界最強のシギント機関 NSA の秘匿されるべき実態、即ちシギントのシステムと活動に関する膨大な機密資料を漏洩したのである。これは当然、諜報対象諸国の防諜や対抗措置の為に有益な情報となり、また、それら諸国のシギント能力向上に資する情報であって、米国のシギント能力、国益に甚大なる損害をもたらすものである。

また、シギントで米国と緊密な関係を有する諸国、即ち、英国、カナダ、豪州、ニュージーランドの UKUSA 諸国にとっても、同様の評価であろう。

なお、米国の中には、彼の行為を、米国人に対する過剰な情報収集や適正なシギントのあり方についての問題提起として高く評価する人々もいるが、必ずしも、彼らの見解が米国民の多数によって支持されているとは見られない。

第２に、中国、ロシア、北朝鮮等、米国の主たる諜報対象国であると同時に、自らもシギントに力を入れ、且つ米国に対して積極的なヒューミントを実施している国々はどうであろうか。常識的に考えれば、スノーデンの行為は高く評価されるものである。彼の行為により、未入手の有益な機密資料を入手できたのであれば、国益に資すること大であるのは明白である。

但し、仮にヒューミントにより既に米国のシギントの実態を相当把握していたとしたら、如何であろうか。既に把握していながら米国がそれを知らない状況であれば、現在のように誰でも知り得る状態で、且つ、米国政府も知られていることを知っている状況よりは、有利であろう。そして、知られぬままに、中国やロシアがヒューミントにより既に NSA の実態を把握している可能性はあるのである。実際、スノーデンによる機密資料の大量持出しですら本人が公然と告発しなければ把握できなかったのである。また、米ソ冷戦時代に、東独の諜報機関が NSA 内部に２人のエージェントを運営していた事実も明らかになっている。

従って、中国やロシアにとっては、仮に既にヒューミントで NSA の実態に相当迫っていたとすれば、スノーデンの行為は有難迷惑ということになり、その損

得は微妙ということになる。

さて第３に、我が国の立場に立ってみればどうか。

先ず、我が国の緊密な同盟国である米国の機密情報が漏洩され、米国が甚大な損害を被ったのであり、これは間接的に我が国にも損害を及ぼしたと言えるであろう。但し、この損害は既に発生してしまったものであり、恢復することは不可能であり、我が国としては致し方の無いものである。

他方、今回の漏洩により、NSA の活動に関する正確且つ多量の内部資料にアクセスできる環境が整ったことは注目に値する。実際、インターネットの世界では、NSA の実態に関する研究が数多く掲示され、更に報道された全ての漏洩資料を分類整理して索引付けして公開しているウェブサイトまで存在するのである。従って、世界の多くの国々、特に英語を解する者にとっては、NSA の実態はアクセス容易な公開情報となったのである。当然、多くの国々ではこれら公開情報を基に NSA の実態研究が進んでいるであろう。

これに対し、我が国の状況は如何であろうか。現在でも、米国のシギントの実態は殆ど知られていないのではないだろうか。一般国民は致し方ないとしても、オピニオン・リーダーや政府高官、更に政治指導者でも、米国のシギントの実態を十分知らないままに、インテリジェンスの議論をしていることがあるのではなかろうか。このままでは、我が国のインテリジェンス・リテラシー（理解力）と諸外国のそれとの格差が更に広がるばかりであろう。現在、世界各国のシギントの実態、そして NSA の実態を知ることは、我が国にとって緊喫の課題である。

そこで、今回の内部資料にアクセスできる環境を活用して、更に米国政府等による開示資料、或は報道資料を使用して、NSA の実態について分析してみることとする。

本稿の成果が、我が国の人々のインテリジェンスに関する背景知識となりインテリジェンス理解力の向上に資することができれば、これこそが筆者の願うところである。

平成 27 年 7 月 21 日

テロ・安保問題研究部会
（日本大学　総合科学研究所　教授）
茂　田　忠　良

＜凡例＞

「インテリジェンス」という単語は通常「情報」と訳されるが、「インフォーメーション」も情報と訳されるため、我が国では両者の区別が付かなくなっている。筆者は、それが「インテリジェンス」を正しく理解する上で支障となっていると感じている。そこで本稿では、若干古風ではあるが、インテリジェンスの訳語としては基本的に「諜報」を使用してインフォーメーションと区別することとした。

なお、筆者はコンピュータについて専門的知見を有しておらず、また、我が国語でのコンピュータ関連用語にも通じていない。そのため、英文のコンピュータ関係用語の翻訳において我が国での通常の用例と異なる用例も多いと思うが、御容赦願いたい。

（一般用語）

Intelligence	諜報
Foreign Intelligence	対外諜報
Counter-Intelligence	防諜
Intelligence Community (IC)	諜報コミュニティ
Signals Intelligence	シギント
Communications Intelligence	コミント（通信諜報）
Electronic Intelligence	エリント（電子諜報）
Human Intelligence	ヒューミント（人的諜報）
Imagery Intelligence	イミント（画像諜報）
Measurement and Signature Intelligence	マシント(計測諜報)
Security Service	セキュリティ・サービス

（米国主要諜報諸組織等の名称）

Director of the National Intelligence (DNI)	中央諜報長官
National Security Agency (NSA)	国家安全保障庁
Central Security Service (CSS)	中央安全保障サービス
Central Intelligence Agency (CIA)	中央諜報庁
National Geospatial Intelligence Agency (NGA)	国家地理空間諜報庁
National Reconnaissance Office (NRO)	国家偵察局
Defense Intelligence Agency (DIA)	国防諜報庁
Federal Board of Investigation (FBI)	連邦捜査局
Foreign Intelligence Surveillance Act (FISA)	対外諜報監視法

「対外諜報監視法」は、元来、米国内での米政府による対外諜報を制限し監

視する法律。一般に外国情報監視法と訳されることが多いが、それでは、監視すべき「外国情報」とは何か不明確であり、同法を諸外国による対米諜報を監視する一般権限法と誤解する可能性、或いは、対外諜報に関する一般権限法と誤解する可能性がある。後述するが、同法は本来、米国の対外諜報のうち米国内で行われる活動であって米国人の権利を侵害しかねないものを監視し規制するものであった。

（セカンド・パーティ諸国のシギント機関の名称）

セカンド・パーティ諸国	英、豪、加、ＮＺ
Government Communications Headquarters (GCHQ)	（英）政府通信本部
Australian Signals Directorate (ASD)	豪信号局
（2013 年に Defense Signals Directorate (DSD)から改称）	
Communications Security Establishment (CSE)	（加）通信保全局
Government Communications Security Bureau (GCSB)	(NZ)政府通信保全局

目次

要旨（Executive Summary）

1　NSA（National Security Agency）概観

（1）沿革

米国の国家安全保障庁 NSA は、1952 年 11 月 4 日に国家諜報機関として発足した。シギント改革のためのブラウネル委員会が、シギントは国家的責務であるとする報告書を提出し、これに基づきトルーマン大統領が指示したためである。

シギントは国家の最高機密であるため、NSA はその存在自体が長らく（1975 年迄）秘匿され、そのため通称 “No Such Agency”(存在しない役所)とも呼ばれた程、機密性の高い組織である。

なお、NSA の他、陸海空軍・海兵隊・沿岸警備隊も作戦支援のためのシギント組織を保有しており、これらシギント諸組織を一体的に運用するため、1972 年中央安全保障サービス CSS（Central Security Service）が設置され、NSA 長官が CSS 長を兼任している。

（2）任務

NSA の任務は、①シギントと②情報保証の二つであり、更に③コンピュータ・ネットワーク作戦（サイバー戦争）の基盤の提供も任務としている。

これは①②とサイバー戦争とが密接に関係しているためであり、NSA 長官は米軍の統合軍の一つであるサイバー軍（2010 年 10 月編成）の司令官を兼任しているが、それもこの三者の密接な関係に拠るものである。

（3）予算・人員・組織

2013 会計年度の国家諜報計画予算によれば、NSA の予算は 108 億ドル、人員は 3 万 4901 人（内軍人は約 1 万 3500 人）である。但し、シギント活動は、CSS 傘下の各軍シギント組織、国家偵察局、CIA 等でも行われており、シギント全体の予算総額は 200 億ドル前後、総人員は 5 万人を超えると推定される。

NSA の本部は、ワシントン DC 郊外のフォートミード基地に所在するが、米国内に 4 つの地方本部を有し、更に世界中に多くの施設を有する。世界の施設の設置場所には米軍施設や米国大使館などがある。

（4）組織運営

NSA は国防長官傘下の機関であるが、国防総省の単なる一機関ではなく、国家諜報機関である。即ち、各軍の作戦支援任務は保持しつつも、大統領など政府最高指導部や国防総省以外の省庁を含む政府全体のためのインテリジェンスを荷なう機関である。その組織運営の基本は国家安全保障法が規定している。

① 任務付与（Tasking）：国家諜報長官が、NSA を含む諜報コミュニティの目標と優先順位を定めると共に、ナショナル・インテリジェンスの情報要求と優先順位を決定し、収集・分析・作成・配布のタスキング（任務付与）を指揮

する。（国家安全保障法 102A 条(f)）

② 情報配布：NSA は、シギントの収集、処理、分析、作成、配布を任務とする。配布対象は、諜報コミュニティ内の組織と人であるが、その手続は、国家諜報長官が国防長官と調整の上で司法長官の承認を得て定めることとされている（大統領命令 12333 号）。当然、政府要人には必要なシギント情報が提供されている。

③ 人事：NSA 長官は、上院の承認を得て、大統領が任命する。大統領による任命の前には、国防長官が候補者を推薦するが、それには国家諜報長官の同意が必要である。（102 条、 106 条（ｂ））

④ 予算：NSA 予算を含む国家諜報計画予算に関して、国家諜報長官が、作成の指針を提示し、作成し、決定し、大統領に提出する。（102A 条（ｃ））

（５）活動の根拠と規制

シギント活動の基本的な根拠法令は、大統領命令 12333 号である。即ち、大統領の行政権には、憲法上、国家安全保障のための広汎な権限が含まれ、対外諜報はその一部と解釈されている。従って、対外諜報は、法律の根拠なしに、米国の内外に於いて大統領の行政命令によって行うことができる。

しかしながら、米国史上では、行政府が度々この権限を濫用したため、1978 年に対外諜報監視法（Foreign Intelligence Surveillance Act）が制定された。これは、本来、米国内で行われる対外諜報活動、特に電子的な諜報収集に制約を課したものである。ところがその後、本法律は度々改正され、単に米国内での対外諜報活動を規制するものから、米国内で行う対外諜報のために民間事業者に協力義務や守秘義務を課すなど強制権限の根拠規定の色彩を強めている。

２　NSA の戦略

（１）シギント戦略 2012 年～2016 年

2012 年の NSA 内部資料では、現状認識として、世界の相互依存と情報時代の到来によって、シギント活動領域が劇的に拡大した結果、現在は「シギントの黄金時代」であると述べた上で、シギントの達成目標として、「シギント技術の向上と自動化を進めて、世界ネットワークに対する支配を劇的に拡大する」「必要なシギント・データを誰からでも、何時でも、何処からでも獲得する」としている。

（２）2007 年時点での戦略的任務リスト

2007 年時点では、継続的標的国として、中国、北朝鮮、イラク、イラン、ロシア、ベネズエラを挙げると共に、個別任務分野として、テロ情報、米国国土安全保障、大量破壊兵器と生物化学放射性物質の計画と拡散、海外展開中の米軍の安全と作戦支援など１６の任務分野を挙げている。

日本に対する関心は、個別分野では、科学技術、外交政策、経済的安定と影響力の３分野で示されている。

（３）UKUSA 協定諸国との協力

米国のシギント力は、UKUSA 協定（1946 年締結、1952 年改定）に基づくセカンド・パーティ諸国機関との特別な協力関係によって支えられている。これらの諸機関は、英政府通信本部 GCHQ、加通信保全局 CSE、豪信号局 ASD、ＮＺ政府通信保全局 GCSB である。これら諸機関との協力関係は密接且つ恒常的であり、米国 NSA を中心としてシステムや運営の一体化が進んでいる。

（４）サード・パーティ諸国との協力

NSA は、その他の諸国とも個別にギブ&テイクの協力関係を持っており、これら諸国はサード・パーティと呼ばれる。2013 年時点では３３のサード・パーティがあるが、協力度合は多様である。東アジアのサード・パーティには、日本も含まれているが、シンガポールと韓国が主要国であるとされる。

この他、関係国が参加する国際協力の枠組として、アフガン・シギント連合、欧州シギント首脳会議、太平洋シギント首脳会議が設定されているが、日本は何れにも含まれていない。

３　NSA の収集態勢（シギント・プラットフォーム）

NSA がシギント・データを収集する主要なプラットフォームは次の通りであり、世界中のサイバー空間に於いて収集態勢を構築している。

なお、収集態勢構築においては、「特別資料源作戦」SSO という民間の情報通信企業の協力を得て行う作戦が大きく貢献しており、米国他の主要企業の協力を得ている。

３－１「プリズム」計画

「特殊資料源作戦」の一つであり、対外諜報監視法に基づき米国の情報通信企業のデータセンターから必要データを入手するものである。協力企業は、マイクロソフト、ヤフー、グーグル、フェイスブック、パルトーク、ユーチューブ、スカイプ、AOL、アップルの 9 社。

本計画では、FBI の協力を得て、企業のデータセンター内に FBI が設置したデータ取得用システムを介して必要データを取得している。取得方法は、データセンターに既に蓄積されているデータを取得する方法と、リアルタイムで対象を監視するため通信と同時にデータを取得する方法がある。後者では、対象の E メールやチャットなどのインターネット活動がデータセンターで検知されるとデータ要求者に対して自動的に通知が来るようになっている。2013 年現在テロ対策でのリアルタイムの監視対象は 11 万以上に及ぶ。

プリズム計画の費用は年間 2 千万ドル程度であるが、その効果は極めて大きい。

現在プリズムは NSA の最大の資料源であり、全情報報告の 7 分の 1 以上の資料源がプリズムである。また、大統領ブリーフィングでも全体の１８％がプリズム由来である。このように成果が大きい背景は、米国が世界のインターネット通信の中心地であり、また現在フリーメール、オンライン・ストレッジ・サービス、ソーシャル・ネットワーク・サービスなどが盛んであるが、これらのデータを記録する米国企業のデータセンターが米国内に多く所在するためである。

３－２　通信基幹回線からの収集

NSA は、約２０の計画により、世界のインターネット通信基幹回線の主要ポイントにおいて膨大なデータを収集している。これら約２０の計画には、米国の内と外、収集の法的根拠、民間企業の協力の有無、米国外の場合に他国の諜報機関の関与の有無、具体的な取得データの中身など、様々なものが含まれており、一様ではないが、収集拠点数は 50～60 ヶ所にも及ぶと見られる。NSA はこの収集態勢を大きく 3 種類に分類している、

（１）民間企業の協力によるもの

対外諜報監視法及び大統領命令の規定に基づき､主として米国内において米国民間事業者の協力を得て行うもの。但し、一部米国外での収集もある。

① 「ブラーニー」計画～複数の企業の協力を得て、米国内で収集。主たる対象には、外交施設、外国政府がある。

② 「フェアビュー」計画～国際通信の基幹回線、ルーターやスイッチにアクセスできる米国企業の協力によって、世界の通信を収集するもの。主対象は米国外の当事者同士の通信。

③ 「ストームブリュー」計画～米国企業 2 社（内 1 社はベライゾン）の協力によって、米国内の主要ポイント 7 ヶ所で収集している。

④ 「オークスター」計画～企業の協力を得て行うもので少なくとも 8 つの小計画からなる。小計画の多くは米国外に於ける収集である。

（２）外国政府と協力して行うもの

ア 「ウィンドストップ」計画～セカンド・パーティとの共同収集。４つの小計画からなり、その内２つは次の通り。残りの 2 つは詳細不明。

① 「マスキュラー」計画～英国 GCHQ との共同事業。グーグルやヤフーなどのデータセンター間通信回線に侵入してデータを収集。

② 「インセンサー」計画～英国 GCHQ との共同事業。北米と欧州を繋ぐ通信基幹回線の多くが英国を経由することに着目し、経由地の英国で大量にデータを収集するもの。

イ 「ランパート A」計画～サード・パーティとの共同収集。多数の小計画で構成される。2013 年時点では、本計画に基づく収集拠点は 13 ヶ所あり、その内 9

ヶ所が運用中。ドイツ、デンマーク、スウェーデン他の協力国が指摘されている。
（３）単独（一方的）事業
米国外で NSA が単独に（相手国との共同事業ではなく一方的に）実施するものであり、５つの計画がある。その内３つの計画名が「ランパート I/X」「ランバート T（CLANSIG)」「ミスティック」であることが判明している。

＜エピソード１＞「ミスティック」計画
他の計画とは少し毛色が異なる興味深い計画である。
本計画は、外国政府に対して、表向きは通信事業会社の合法的な商業サービスの提供という形を採りながら、その裏で必要なシギント・データを収集するもの。外国政府との関係は麻薬取締局 DEA、CIA や豪信号局が仲介をしている。2013 年時点では、バハマ他５ヶ国で計画が動いている。アフガニスタンでも行われている可能性がある。
バハマを例に採ると、NSA はバハマの国内通話を含む携帯電話通話の全メタデータと全通話内容を記録し 30 日間保存できるシステムを構築しているという。それが可能となったのは、バハマ政府が国際犯罪捜査のために通信傍受設備を設置しているが、DEA の仲介により設備の設置管理を契約した米国系民間通信会社がバハマ政府に対して秘密裡に DEA と NSA とに協力していると考えられる。

３－３　衛星通信の傍受
衛星通信の傍受は、２０世紀からシギント・データの主要な収集プラットフォームであったが、２１世紀のインターネット時代にあっても依然として主要プラットフォームの地位を維持している。具体的な収集拠点は、次の二種類である。
（１）主要傍受施設～大規模な傍受設備を使用する。世界中で 12～13 ヶ所
（２）特別収集サービス（SCS）～約 40 ヶ所

３－４　特別収集サービス（SCS）
特別収集サービス（SCS）は、NSA と CIA の共同事業である。以前は、一方で NSA が大使館を拠点に独自のシギント活動を行い、他方 CIA も大使館を拠点に盗聴器を使用するなどして技術的情報収集を行っていた。しかし、これでは非生産的であるとして、1970 年代末に両者の機能を統合して、SCS を設置したという。
現在、世界中の米国大使館、領事館、利益代表部等の外交施設８０ヶ所以上に、暗号名「ステートルーム（特別室)」という拠点を設置している。拠点では、建物の屋上や上層階に（電波透過率の高い）ポリエチレンやセラミックで作った偽装工作物を設置して、その中に各種の高性能アンテナを秘匿設置すると共に、建物内にはデータ処理や分析のための部屋を確保している。

セカンド・パーティ諸国（英国、カナダ、豪州、ニュージーランド）も同様に大使館等に収集拠点を設置しており、これらも「ステートルーム」と呼ばれる。UKUSA５カ国の大使館、領事館などがそれぞれの地の利を生かして共同して活動していると考えられる。

SCS では単にデータを収集するだけではなく、地の利を生かした分析も行っている。大使館等に駐在して任国情勢を熟知した分析官が、シギント資料を得てより実態に迫る正確な情勢分析を行い、米本国の大統領以下の国家的情報需要に応えると共に、駐在大使への情勢報告にも活用されている。また、NSA 内部資料には、「シギントを進めるヒューミント、ヒューミントを進めるシギント」という標語も掲げられている。これは、一方で、外交官や CIA 要員が傍受すべき携帯電話番号を収集するなどして、シギントの資料源開拓に貢献し、他方、シギントで得た情報を利用してヒューミント（例えば協力者獲得工作）を行うなど、シギントとヒューミントの密接な協力関係の存在を伺わせるものである。

３－５　CNE（コンピュータ・ネットワーク資源開拓）

CNE(Computer Network Exploitation)とは、ハッキングによってコンピュータ・ネットワークに侵入し、システム資源やデータ資源を開拓することである。手法としては、遠隔地からインターネット網を介して行う侵入(remote access)と近くからの直接的な侵入(close access)の二つの手法がある。

（１）TAO（Tailored Access Operation）とその成果

NSA 内で CNE の責任部署は TAO である。1997 年発足したが、定員は急速に増加しており、2013 年度会計予算では 1870 人となった。

現在までの成果としては、各種システムに対する操作可能なマルウェアの累計注入件数(implants)が、2008 年では 2 万 1252 件、2011 年では 6 万 8975 件であり、2013 年度会計年度中には 8 万 5 千から 9 万 6 千件に及ぶ見込みであった。

（２）遠隔侵入(remote subversion, remote access)

遠隔進入は、ネット侵入、ソフトウェア注入等とも呼ばれる。担当は、遠隔作戦センターROC である。ROC のモットーは、「君らのデータは我らのデータ、君らの機器は我らの機器。何時でも、何処でも、どんな手を使っても。」であり、正にその任務を象徴している。

嘗ては、NSA もマルウェアを仕込んだスパムメールの送付を主軸としていたようであるが、その成功確率が極めて低くなり、今や成功率は１％にも満たないとされる。そのため、現在では、コード名「クオンタム」計画という「側面者攻撃」が中心であり、その他「中間者攻撃」他の侵入方法もとっている。

遠隔侵入が一般のハッカーと異なるのは、上記の「通信基幹回線からの収集」のため世界各地に設置した「ターモイル」等の機器設備を活用しており、NSA

のシステム力が貢献している。

＜エピソード２＞「ショットジャイアント作戦」（対・華為）

TAO は 2007 年から華為のシステムに侵入する作戦をしていたが、2009 年からその努力を抜本的に強化したようである。その成果として、華為の広東省深圳市にある本社のシステムへの侵入に成功し、顧客リスト 1400 を入手したほか、Ｅメールの保管サーバーへのアクセスに成功（2009 年 1 月からメール取得可能）、更に華為の各種製品のソースコードまで入手したという。

（３）物理的侵入（physical subversion、close access）

物理的侵入は、近接侵入、或はネット外侵入(Off-net)と呼ばれる。要するに対象機器や施設に接近してマルウェアを注入したりするものである。担当は、AT&O（Access Technologies & Operations）である。これには、サプライ・チェーン工作や在米の外国公館からの情報収集が含まれる。

ア　サプライ・チェーン（配送経路）介入

海外の標的組織が、コンピュータ・ネットワーク関連製品を発注した場合、製品を配送途中で一旦確保して、これにマルウェアを注入し或はマルウェア入りハードウエアを装入した上で、配送経路に戻して発注先に届ける方法である。2010 年の NSA 内部資料によれば、シリア通信事業機構のインターネット基幹部分に使用する製品に対して介入を実施した結果、シリアのインターネット通信の基幹部分に侵入できたという。必要な場合は FBI や CIA の作戦支援を受ける。

イ　在米大使館、国連代表部からのデータ収集

2010 年の NSA 資料によれば、TAO は様々な機器を設置するなどして各国の在米大使館や在ニューヨークの国連代表部からデータを収集している。収集対象公館は３８とされており、日本の国連代表部も対象となっている。

＜エピソード３＞中国による CNE 作戦の解明

コンピュータ・ネットワーク資源開拓 CNE は、NSA に限らず世界中のシギント機関が行っていることであり、米国に対しては、中国、ロシアその他の諸機関が積極的に CNE 作戦を実行している。そこで、これら他国機関による CNE 作戦から自国を守る CNE 対策が必要になるが、その第一歩は当該機関の CNE 作戦の実態を解明することである。そこで、一例として、中国の CNE 作戦に対抗する NSA の解明作戦を見てみたい。

NSA は、中国による CNE 作戦全体に対して「ビザンチン・ヘデス」とのコード名を付けてその解明と対策に当たっているが、中国による CNE 作戦は種々あり、少なくとも１２の作戦グループが存在すると見られる。各作戦グループの標

的は、主として米国であるが、一部は日本も標的にしている。

NSA はその作戦グループの一つである「ビザンチン・カンダー」を解明しているが、解明の経緯は次の通りである。2009 年国防省のネットワークに対する侵入が探知され、その通報を受けた TAO グループが解明に乗り出した。侵入者は、多くの作戦中継機を経由し且つ発信端末自体の IP アドレスも度々変更されるため、発信端末の特定は困難を極めたが、各種技法を凝らして、遂に中国人民解放軍総参謀部第三部が使用するユーザー・アカウントを特定することが出来たという。そして 2009 年 10 月には「ビザンチン・カンダー」グループの５つのコンピュータ端末への侵入に成功した。その端末には CNE 作戦の責任者のものも含まれるという。これによって同グループの構成員情報、技術概要、取得データ、将来の攻撃目標（米国や外国政府職員の個人情報等）などに関するデータを入手することが出来たという。

これらの CNE 解明作戦によって判明した「ビザンチン・ヘデス」（中国の CNE 作戦全体）によって米国が受けた被害の見積りは次の通りであるという。即ち、国防総省のシステムに対する侵入事案は、少なくとも３万件以上、重大な侵入事案が 500 件以上、1600 台以上のネットワーク端末が侵入されている。これら侵入によるネットワークの損害の見積り・修復のために１億ドル以上の費用を要している。窃取されたデータは、３万人以上の空軍軍人の個人情報、３０万件以上の海軍のユーザーID とパスワード、原子力潜水艦や海軍防空ミサイルのデザイン情報、国防企業から B2 爆撃機、F22 ステルス戦闘機、F35 戦闘機等に関する機密情報であり、貴重な情報が大量に窃取された実態を解明したとしている。

４　NSA の収集分析その他の活動

NSA がそのシギント・プラットフォームを使って実際に何を収集しどのように分析しているかの一端を紹介する。

４－１　メタデータ分析

（１）メタデータとデータベース

メタデータとは、通信内容を除く通信に付随する情報の全てである。

具体的には、携帯電話通話であれば、通話当事者の電話番号、携帯端末識別番号、利用者識別番号、回線識別符号、通話日・時刻、通話時間、テレホンカード番号、携帯端末位置情報等である。

また、インターネット通信であれば、E メール活動の内メールの内容以外の全て、即ち、当事者のメールアドレス、IP アドレス、通信日・時刻等、SNS 活動の通信内容以外の情報、その他ネットワーク上の活動（ウェブサイト訪問履歴、ログイン時刻、地図検索履歴等）情報が該当する。

メタデータには、通信内容そのものは含まれていないが、極めて有用な情報資

料であり、NSA は専用のデータベース～電話通話用「メインウェイ」、インターネット通信用「マリーナ」～を構築している。

（２）各種分析手法

① 接触連鎖分析～把握しているテロ容疑者・関係者が誰と連絡を取り合っているか、その連絡者は更に誰と連絡を取り合っているかなど、人間関係を自動的に分析し解明する。2012 年中は、分析の結果テロ関係容疑者 500 件の情報が FBI に提供されたという。

② 人物分析～メタデータ分析により、その人物像、友人知人関係、組織団体関係、生活習慣や行動履歴、更には関心興味に至るまで把握することができる。

③ 位置情報データベースと各種分析～メタデータの中でも携帯電話・スマートフォンから取得する位置情報を活用することにより、監視対象者の行動把握、不審人物の割出が可能であり、更に、諜報機関の海外エージェントに対する現地当局等による監視の有無を検索する手法まで開発されている。

（３）「IC リーチ」プログラム

メタデータ分析が極めて効果的であるため、「IC リーチ」という諜報コミュニティ全体のための通信メタデータの分析システムがある。これは、NSA が責任部署として管理運営し、中核組織は NSA の他 CIA、FBI、DIA（国防諜報庁）、DEA（麻薬取締局）の５機関であるが、2010 年現在、利用できる分析官は米国政府 23 機関の 1000 人以上に及ぶとされる。

４－２　エックスキースコア XKeyscore

XKeyscore とは、NSA が大量に取得するデータの一次記憶装置であり、また、この装置から必要なデータを検索抽出し分析するための分析システムである。

NSA はそのシギント収集態勢により世界中でデータを収集しているが、その世界中の収集拠点約 150 ヶ所にサーバー700 以上を設置して XKeyscore システムを構築している。その記憶装置は、所謂「ローリング・バッファ」方式を取っており、収集拠点毎にサーバーの記憶容量の範囲内で、常に、新しいデータで古いデータを上書きしつつ、最大量のデータを保管しているとされる。データの保存目標期間は、コンテンツ・データで３日間、メタデータで３０日間である。

このシステムを使用することにより、メールアドレスやユーザー名など対象を特定できる「ストロング・セレクター」がある場合だけでなく、通信内容中のキーワード検索や通信形態など「ソフト・セレクター」から通信データを検索抽出することができるなど、極めて有効なシステムであるとされる。

４－３　暗号対策

NSA において暗号対策は、CES （暗号解読・資料源開発サービス)が担当して

いるが、その 2013 年度予算は、１０億ドル（１千億円）以上の巨額に及んでいる。

暗号攻略には、高等数学やスーパーコンピュータを使用した暗号解読は当然含まれるが、その他にも次のように各種資源を活用し多様な取組をしている。

- CNE（コンピュータ・ネットワーク資源開拓）、即ち、所謂ハッキングにより暗号解読資料を入手する。
- 「物理的侵入」による情報機器への工作
- 諜報コミュニティの協力～ヒューミント資源を活用し、可能であれば、暗号資料の協力者からの入手、或は窃取なども行う。
- セカンド・パーティ諸国との協力～～特に英 GCHQ との協力関係は緊密。
- 民間への働き掛け、民間企業の協力～NSA には民間ソルーション・センター(Commercial Solutions Center)という民間企業との窓口があるが、ここは、民間商用暗号のソフトウェアと機器に関して（解読し易いように）働き掛ける、或は、民間商用暗号の詳細を入手するなどを行う窓口になっているという。

このような総合的な取組によって、ネットワーク通信に関しては、TLS／SSL、HTTPS、SSH、VPNs、暗号化 VoIP、暗号化 Chat その他の暗号に対して、相当の解読能力を保持している。

こうして、NSA は、その内部に「暗号鍵提供サービス」という各種民間暗号鍵の内部データベースを構築しており、これにより自動的に通信の暗号解読をするようにしているという。また、必要な暗号鍵がデータベースにない場合には、要求が「暗号鍵入手サービス」に送付され、暗号鍵入手の努力がなされるという。

４－４　幾つかの興味深い収集事例

（１）「標的データベース」に掲載された世界の政府首脳

一国の政治の最高責任者は、当然に諸外国の政治の最高責任者について関心を持つものであり、従って当然これら外国の首脳は NSA の諜報対象（標的）になっている。実際、NSA の「標的データベース」には 2009 年時点で（セカンド・パーティ諸国を除く）世界の政府首脳 122 人が掲載されている。

幸いにして、日本関連では当時の麻生首相が掲載されている。インテリジェンスの論理を理解しない一部の者は、米国の同盟国日本の首相が諜報対象とされていることに違和感を持つかも知れないが、同盟国であろうと他国である限り（相互の利害が 100%一致することはあり得ないので）諜報対象にするのは当然である。寧ろ、仮に麻生首相が対象とされていなかったとすれば、日本は首相を諜報対象とする程の価値も重要性もない国と評価されていることを示すものであり、その方が極めて問題である。

なお、オバマ大統領は、2013 年 7 月「諜報機関というものは全て、米国だけでなく、欧州諸国でもアジア諸国でも諜報機関が存在する限り、世界をもっと理

解しよう、各国の首都で何が起きているかを理解しようとしている。それをしないようであれば、諜報機関としての価値はない。」と発言している。

（２）金融取引データの収集「Follow the Money」

諜報機関が対象とする様々な活動には、金の動きが伴うものである。違法武器取引にしろ、抑圧的政権への支援、経済制裁破り、テロリスト支援、薬物密輸など、殆どの活動には金の動きが付随する。そこで、国際的な金の動き自体に着目して関連データを収集分析することによって、有効な諜報活動ができることとなる。

そのため、NSA には「Follow the Money」と呼ばれる金の流れに関するデータを収集分析する部門が存在する。ここでは、国際銀行間通信協会（SWIFT）の通信システムに侵入して銀行間送金決済情報を取得したり、クレジット・カード取引データを取得したりして、世界中の金融取引データを大量に収集し「トラックフィン（Tracfin）」というデータベースを構築して分析に活用している。

（３）スマートフォン攻略

スマートフォン端末にある記録情報は「宝の山」と言われる。それは、端末には諜報機関が興味を持つ持主の個人情報が集積されるからである。便利であるが故に、持主がスマートフォンを愛用し活用すればする程、持主の生活記録、個人情報がスマートフォンを経由し、またその上に記録されることなる。即ち、交友交際情報、行動と位置情報の履歴、（検索履歴等から）興味関心、写真、時にはクレジット・カード番号やパスワード情報まで、スマートフォンを通過し、また記録される。

そこで、NSA では、アイフォンと iOS、アンドロイド、ブラックベリーの基本ソフトに対して、それぞれ専門の分析チームを置いて侵入方法やデータ抽出方法等を分析して来たと言う。

なお、NSA や GCHQ は、携帯端末のマイクを持主の知らぬ間に起動して収集した音声を送信させるなどの技術も有している。

（４）ウェブカメラを使用した監視

ウェブカメラは、現在は、多くのパソコン端末に標準装備され、ビデオチャット（画像付きの通話）などに利用されている。

NSA が、ウェブカメラを装備したパソコン端末をハッキングして、そのウェブカメラを使用して持主の行動監視に使用できることは、当然である。

なお、ウェブカメラを使用した情報収集は、幅広く行われているようである。欧州企業ガンマ・グループ社は FinFisher という監視用ソフトウェアを世界中の諜報機関や治安機関に販売しているが、その製品は、秘密裡に標的の情報システムに侵入して、ウェブカメラとマイクを起動してのリアルタイム監視が可能であるとしている。

＜エピソード４＞中国によるウェブカメラとマイク使用の情報収集

2009 年にカナダ・トロント大学が発表した研究報告書によれば、2008 年から2009 年にかけて海外チベット人社会に対する中国によるサイバー諜報活動を研究したところ、中国海南島を拠点とするグループが、ダライ・ラマ事務所とチベット人諸組織に対する情報収集を行うために、世界 103 カ国に所在するチベット諸組織関係の 1295 台以上のコンピュータ端末に侵入していたことを発見したという。そして、そのマルウェアには、秘密裡にパソコン端末を起動してウェブカメラとマイクを使用する能力があったとしている。

5　コンピュータ・ネットワーク作戦（CNO）と NSA

（1）CNE、CNA、CND の三位一体関係

NSA の任務には、コンピュータ・ネットワーク作戦 CNO（ネットワーク戦争）の基盤の提供が挙げられている。且つ、NSA 長官は米サイバー軍司令官を兼任している。その理由は、CNO を構成する CNE（コンピュータ・ネットワーク開拓）CNA（コンピュータ・ネットワーク攻撃)、CND（コンピュータ・ネットワーク防禦）の三者が密接不可分の関係にあるからである。

第 1 に、CNE は、シギントの重要構成要素であり NSA の任務そのものである。

第 2 に、CNA については、NSA によるシギント活動がその基盤をなしている。攻撃するには攻撃対象の実態が分かっていなければならないが、対象の実態把握は、NSA のシステムとシギント活動に依存するところが大である。また、NSA のシギントのためのネットワークのインフラ自体が、攻撃のためのインフラともなるのである。

第 3 に、CND については、先ず、攻撃からの防禦システムの構築・運用には、常日頃 CNE という矛を運用している NSA のノウハウが基礎になる。次に、攻撃を受けた場合に、敵対勢力による CNA の発信源に対して反撃し、攻撃を停止させる、或いは、攻撃を事前探知して防禦態勢を構築する、状況によっては予防的先制攻撃を行うためには、普段から、CNE 対策を実施して潜在敵の攻撃能力を把握し、無害化する準備をしておかなければならない。更に、NSA のシギントシステムは、また、防禦 CND のためにも利用できる。

このように、CNE、CNA、CND の三者は一体であり、それだけシギント機関である NSA の関与が重要である。

（2）Tutelage システムによるダイナミック防衛

Tutelage トュートリジ・システムとは、NIPRNet（国防関係情報通信ネットワーク）に対する侵入攻撃を、シギントを活用して事前に探知し、その攻撃を阻止し或は無害化して監視するなど、ダイナミックな防禦システムである。

NIPRNet は、秘密情報未満の機微な或は部内用の情報を扱うネットワークであるが、インターネット網と接続されている。その結果、インターネットを経由したサイバー攻撃を頻繁に受けている。

インターネットとの接続点は、米国内外に 10 ヶ所以上あり、これら接続点にはファイアウォールが設置され、既知のマルウェアや攻撃は遮断している。しかし、未知の攻撃は即時に遮断できず、ネットワーク内に侵入を許してしまう事例も多い。そこで、従来は、接続点を通過した全通信を記録した上で、事後的に分析して、マルウェア等の容疑通信を抽出、侵入報告を作成し、標的端末の管理者に通報して対策を求めていたという。しかし、この分析報告には数日間を要し、損害が発生する前に、侵入報告が関係者に到達し対策を取り得るか、課題があった。

そこで、Tutelage システムでは、ネットワークに侵入されてから対処するのではなく、シギント能力を活用してシステムに侵入される前から対抗措置を採るところに特徴がある。即ち、攻撃者がマルウェアを作成している段階で、シギント活動により攻撃者の道具や技術を探知して、これに対する対処対抗手段を開発してインターネット接続点に配置する。更に、攻撃者の意図や標的を探知して、実際に侵入攻撃が実施される場合には、インターネット接続点で侵入攻撃に対処するというものである。

2009 年までには導入され、2010 年時点で攻撃阻止の成果を挙げている。

米国の防禦システムとしては、この他、連邦政府一般官庁用のシステム Einstein 3　があるが、2009 年その実施が決定され、現在既に設置されていると見られる。また、米国のサイバー空間全体に対する防禦システム MasterMind というプログラムがある（但し、現在どれだけ進行しているか不明である）。何れにしろ、サイバー空間の防禦システムとしては、単に、端末機器や個別ネットワークを防禦しようとするのではなく、政府全体或は国全体のサイバー空間をシギント力を活用しながら防禦しようとしていることが注目される。

（３）大統領政策指令第２０号「サイバー作戦政策」と標的リスト作成

2013 年１月米国政府は、大統領政策指令２０号の骨子を公表した。それによれば、「同指令は、サイバー作戦の原則と手続を定めて、サイバー作戦を使用可能な国家安全保障のための諸手段に統合するものである。作戦の原則と手順の目的は、我々の有する能力のより有効な計画、開発、使用を可能とすることである。」と述べて、サイバー作戦が実用段階に達していることを示唆した。

また、同年１月、国防総省は、サイバー軍の規模を（当時の）900 人から数年間で 4900 人程に大幅に増強する決定をした。

内部資料によれば、同指令では、サイバー作戦の原則、防御的サイバー作戦、攻撃的サイバー作戦、継続的な悪意あるサイバー活動への対処などの手順を定めているが、特に攻撃的サイバー作戦については、国防長官、国家諜報長官と CIA

長官は６ヶ月以内に、潜在標的（システムやインフラ）を特定し、攻撃発動の要件を定める作戦計画を立案し提案することとされている。

＜エピソード５＞北朝鮮による「ソニー映画」攻撃と米国の対応

ソニー・ピクチャーズ（以下、ソニー映画）は、北朝鮮の独裁者・金正恩の暗殺を主題としたコメディ映画を製作していたが、これに対して北朝鮮外務省は、同映画は絶対に容認できないとの声明を発していた。

そして 2014 年 11 月 24 日、ソニー映画のコンピュータ数千台からあらゆるデータが消去され、システム全体の運用を停止せざるを得ない状況となった。更にそれから数日間に亘り、事前にシステムから窃取していたとみられる膨大なデータの中から、有名俳優に関するゴシップ情報、未公開映画のコピーや台本などの情報が流布され、ソニー映画に大きな損害を与えた。

これに対し、迅速に捜査を開始した FBI は、12 月 19 日北朝鮮の犯行と断定する広報資料を発表した。

ところで本件に関し、NSA 長官は 2015 年 1 月国際会議で、北朝鮮の犯行であるとする十分な自信があると述べると共に、捜査に於いては、NSA の技術力だけではなく、NSA が提供したデータも貢献している旨を述べている。この発言により、NSA は、その技術力の他、保有するデータにおいても、捜査に貢献していることが分かる。具体的内容は不明であるが、先ず、XKeyscore などの NSA のデータ収集分析システムが貢献した可能性がある。また、NSA による CNE 対策も貢献したものと見られる。NSA は北朝鮮による CNE 作戦の解明のために本事件前から北朝鮮のシギント部隊のネットワークにも侵入していたとされる。

そのため、今回の北朝鮮による攻撃を事前に探知するまでには至らなかったが、事後的な分析により、北朝鮮が 2014 年 9 月にはスピア・フィッシングという手法によってソニー映画のシステム管理者の権限を盗んだこと、それを使って 9 月中旬から 11 月中旬に掛けて、ソニー映画のネットワークを調査して、重要なデータファイルを特定し、また、コンピュータやサーバーへの攻撃方法を計画してきたことが判明したとされる。

ここから分かるのは、国家レベルのハッキングの解明に於いては、NSA という強力なシギント機関のシギント情報による支援が必要であったということである。

６　セカンド・パーティ、英国との特殊関係と興味ある活動

（１）GCHQ（Government Communications Headquarters）の特徴

英国のシギント機関である政府通信本部 GCHQ の予算額は、約 10 億ポンド（1800 億円）、人員は約 6100 人である。この他に、他省庁分として計上された中から支出されるものがある。その金額は、2011 年度は 1 億 5 千万ポンド（邦貨 200

億円以上）と相当額に上る。供出元は、内務省、国防省、米国 NSA の 3 機関であるが、内務省が最大の供出元であるとされている。この事実や GCHQ の活動目的に「重要犯罪の防止と探知の支援」が明記されていること等から考えると、GCHQ は治安維持目的の活動に相当関与していると推定して間違いないであろう。

GCHQ の担当大臣は外務大臣である。しかし、GCHQ は外務省の外局ではなく附置機関でもない。外務大臣が直率する組織であり、GCHQ 長官は外務次官と同格である。また、予算は外務省予算の一部ではなく、他の諜報機関と共に首相府の統合諜報会計に位置付けられている。当然 GCHQ 長官は、直接、首相にも報告する。英国は、内閣官制を採りながらも諜報機関の秘密保持と有効機能のために、極めて特徴ある制度を採っている。この位置付けは、秘密諜報機関 SIS も同じである。

（２）英米特殊関係

世間に良く「米英特殊関係」と言われるが、筆者は、その根幹には制度的基盤があり、UKUSA 協定に基づくシギント協力がそれではないかと考えている。

このシギント協力によって、米国も利益を得て来たが、英国の得て来た利益は米国を上回る膨大なものである。何しろ、米国の強大なシギント力を、英国の国家利益のために利用できるのである。

英国のインテリジェンスは、相対的に小さな組織でありながら、合同情報委員会を中心に効率的に運用されていると評価されている。日本も英国に学ぶべきであると主張する有識者も多い。しかし、英国のインテリジェンス力の背景には、UKUSA 協力に依拠する膨大且つ正確・有用なシギント情報があるのを忘れてはならない。英国政府は、UKUSA 協定によるシギント協力によって、GCHQ に対する投入資源を遥かに凌駕するインテリジェンス成果物を享受しているのである。

それ故、GCHQ は「GCHQ の国際同盟及び協力関係」という文書で、UKUSA 協力関係が、英国の世界における地位と影響力を維持する助けとなっていると主張している。

（３）「ロイヤル・コンシェルジェ」

「ロイヤル・コンシェルジェ」とは、政府高官のホテル宿泊予約の探知通報プログラムである。本プログラムの対象ホテルは約 350 軒あり、政府高官が宿泊しそうな世界中の高級ホテルを対象としている。これらホテルの予約用メールアドレスと諸外国政府のＥメール・ドメイン間の通信を監視しており、ホテルから諸外国政府宛の予約確認メールが送信されると、これを探知して GCHQ 担当官に通報するものである。通報を受けた担当者は、これを基に次の作戦を考えることができる。具体的には、

- 宿泊ホテルが、「友好的」な場合は、ホテルの協力を得て、対象者が宿泊する部屋の電話やファックスの傍受、或は、ホテルネットワークに接続したコンピュータ監視を行う。
- 「技術的攻撃(Technical Attack)」～ホテルの協力を得られない場合、或は傍受設備が無い場合で、情報価値の高い標的に対しては、技術専門チームを派遣して工作を行う。
- 借上車工作（盗聴マイクの設置が考えられる。）
- ヒューミント発動
- その他の方策として、宿泊ホテルの選択に影響を与えられないか、或は訪問そのものを中止させられないか、も検討事項として掲げられている。

世界中の政府要人の外国訪問を探知して、探知した場合に、国外に於いてさえ通信傍受等の作戦をしようという英国の意欲に注目すべきである。

（４）「オンライン秘匿活動」

「オンライン秘匿活動」とは、単なるサイバー空間からのデータや情報の収集ではなく、現実の効果を生じさせることとされ、ヒューミントの世界で言えば、「積極工作」に該当するものである。

GCHQ は「オンライン秘匿活動」に積極的に取り組んでおり、2010 年時点で既に GCHQ の全作戦の 5%を占めていたとされる。2012 年の計画によれば、2013 年初めまでに 150 人以上の要員を養成し、この他、基礎教育を 500 人以上に施す予定とされている。

「オンライン秘匿活動」の類型としては次の三つがある。

① 妨害活動(Disruption)～DOS 攻撃などにより標的サーバーを通信不全に陥れるなどの技術的妨害と、一定の情報を送達することにより対象の信用を失墜させるなど妨害の効果を生む情報作戦が含まれる。

② 影響力活動(Influence)～オンライン世論調査の結果を操作して世論形成に影響を与えたり、或は偽情報を流布させるなど欺瞞戦術を駆使して関係者の行動に一定の影響を与えるなどの情報作戦である。

③ オンライン・ヒューミント～サイバー空間で展開するヒューミント活動であり、担当官がネット上で何者かに成り済まして、標的人物と交流をするなどして、一定の効果を生み出そうとするものである。

GCHQ は「オンライン秘匿活動」のため、種々の道具・技術も開発しており、サイバー空間の拡大、重要性の増大に伴い、サイバー空間での「積極工作」が急増していると見られる。

7　セカンド・パーティ、カナダの興味ある活動

（１）CSE（Communications Security Establishment）の特徴

カナダのシギント機関である通信保全局 CSE は、人員約 2000 人、推定予算 5 億ドル未満の組織である。

任務には、①シギントと②政府のコンピュータ・ネットワーク保護の支援に加えて、③連邦法執行機関とセキュリティ機関の支援がある。興味深いのは、③のための通信傍受やデータ収集は、支援対象の諸機関が法律に基づいて与えられた権限を専門能力を有する CSE が執行するものとして構成されており、その執行に際しては、令状の取得など支援対象諸機関が必要な法的手続きを履行するとしている点である。

（２）サイバー・セキュリティ対策

カナダ政府のセキュリティ対策の一つに「フォトニック・プリズム」計画がある。政府ネットワークのセキュリティの保持のため、CSE は、カナダ政府機関が受信或は発信する全てのＥメールを収集分析している。収集した E メールにマルウェアが添付されていないか、マルウェア添付容疑メールを発見抽出するシステムが「ポニーエクスプレス」と呼ばれ、このシステムの運用により、毎日平均４件のマルウェア付きメールを検出して、メール送付先の政府機関に通報しているという。

また、2011 年時点では「カスケード」という将来構想があった。これは、2015 年までにシギントと IT セキュリティの両者の目的を統合した巨大センサー・システムを構築しようとするものである。具体的には、インターネット通信でカナダ国内と国外を接続するインターネット基幹回線の通り口の全てに、通信事業者の協力を得てセンサーを設置するというものである。これにより全ての国際通信のデータ収集が可能となり、収集データは、シギント目的にも IT セキュリティ目的にも使えるようになる。米国の Tutelage システム（国防関係情報通信ネットワークのセキュリティ・システム）の全国拡大版の様であるが、その後の実施状況は不明である。

（３）テロ容疑者発見プロジェクト「レヴィテーション」計画

過激派は、無料ファイル共有サイト（Free File Upload sites）を利用して、ビデオや文書で過激思想の宣伝を行い、更に、爆弾製造教本などテロ訓練実施のマニュアルを拡散させている。そこで、CSE は、無料ファイル共有サイトを監視することによって、そこから潜在的なテロリストを発見する「レヴィテーション」計画を運用している。

対象とする無料ファイル共有サイトは世界の 102 のサイトであり、これらサイトに掲載されている過激ビデオや過激文書の膨大な件数のダウンロードを分析して、月に 350 件程度の「興味深い」ものを発見、その IP アドレスを取得している。これら IP アドレスについては、更にその使用者についてのデータ収集分析を行い、テロ容疑者と判定した場合には、更にテロ担当の専門部署に資料を提供して調査を進めることとなる。

「レヴィテーション」はテロ容疑者発見のためのプログラムの一つであり、米NSA 初め諸シギント組織は、テロ容疑者発見のため諸々の分析プログラムを運用していると考えられる。

８　サード・パーティ、フランスとの関係

（１）DGSE（la Direction générale de la sécurité extérieure）の特徴

フランスのシギント機関は、対外安全保障総局 DGSE の中に置かれている。DGSE は、ヒューミント、シギント、イミント（衛星画像）、オシントを包含する対外諜報の総合機関である。人員は 5000 人弱、正規予算は約 6 億ユーロである。

DGSE のシギント部門は、米英などと比べれば遥かに小さな組織であるが、その DGSE の力となっているのが旧国営企業のフランス･テレコムとされる。フランス・テレコムは DGSE に対してその通信ネットワークとデータフローに自由且つ完全にアクセスさせているとされる。また、暗号解読などの IT 技術でも協力しているという。如何にもフランスらしい協力と言えよう。

なお､DGSE がフランス･テレコムから入手したデータは､DGSE だけではなく、フランスの諜報コミュニティの各組織が利用できるようになっている。

（２）米国 NSA との関係

米国とフランスは近年協力関係が進展し、「Lustre」計画という共同事業を行っている。これは､一方で､仏 DGSE が収集しているインターネットのデータを NSA に提供し、他方、NSA はフランスがインテリジェンス網を持っていない地域の情報を提供する関係であるという。

しかし、このような米仏の協力関係は、お互いを標的とするインテリジェンス活動を何ら妨げるものではない。NSA は、フランスの首都パリの米国大使館には特別収集サービス（SCS）の拠点を置いて情報を収集している。また、在米のフランス大使館や国連代表部からも情報収集している。更に、仏外務省の VPN（仮想専用ネットワーク）を攻略してデータを収集している。また、仏系企業を標的とした情報収集も行っている。

他方、フランスもやられっ放しではなく、当然、米国初め UKUSA 諸国に対するシギントを含む諜報活動を行っている。米国の 2007 年シギント「戦略的任務リスト」では、フランスは対米諜報活動に取り組む外国として特記された 10 ヶ国の中に含まれている。また、カナダ CSE は「スノーボール」と名付けたマルウェアを解明してきたが､これはフランスが作成したもので､UKUSA 諸国を含む諸外国に対する CNE 作戦に使用していると見られる。

このように一方でギブ＆テイクで協力しながらも、互いに諜報活動の対象にするのが、普通のサード・パーティ関係である。

９　サード・パーティ、ドイツとの独特な関係

（１）BND（Bundesnachrichtendienst）の特徴

ドイツのシギント機関は、連邦諜報庁 BND の中に置かれている。BND は DGSE 同様にヒューミント、シギント、イミント、オシントを包含する対外諜報の総合機関である。人員は約 6500 人、予算は 6 億ユーロ強である。

ドイツは NSA にとって欧州大陸に於ける最重要拠点であるが、また同時に、第二次世界大戦での旧敵国であり、東西冷戦では冷戦の前線国家であったという歴史的経緯もあり、米国 NSA との関係は、密接且つ微妙で独特である。

（２）NSA と BND の中の東独スパイ

冷戦終結前には、東ドイツは NSA の中にスパイを 2 人、BND シギント部門の中に１人持っていた。そのため、東独当局は、NSA の実態や米独のシギント関係を良く把握していた。それによれば、冷戦時代、ソ連圏に対するシギント収集について、NSA は西ドイツに依存することはなく、全て独力で強大な収集態勢を構築していたという。

ここで興味深いのは、NSA 内部や BND 内部に東独のスパイが居た、それも、長期に亘り発覚しなかったという事実である。過去にあった事は、現在でもあり得る。現在でも、NSA の中に外国機関のスパイがいる可能性は否定できない。或は退職後の職員が工作を受けて現職中の知識を提供しているかも知れない。既に、一部の外国諜報機関が、ヒューミントによって NSA のシギント収集態勢やシギント技法の多くを学び、自らの態勢構築に邁進している可能性がある。この可能性を軽視すべきではないのである。

（３）９/１１後の協力関係

９/１１の米国同時多発テロ事件では、ドイツ・ハンブルグにあったアル・カイダの細胞が深く関与していた。このため、これを契機に米独のシギント協力は強化されてきた。

ドイツ国内では、2007 年 9 月イスラム過激派ザウアーラント・グループによる大規模テロ計画が未然に探知され防止されたが、これは NSA のシギント情報が端緒であったいう。過去１０年以上、本件を含めドイツ国内でのテロ事件の殆どで、その防止や捜査に、NSA からの情報が貢献してきたとされる。

こうした経緯もあり、テロ対策に関するシギント協力で、米 NSA と独 BND に加えて、ドイツのセキュリティ・サービス機関である BfV 連邦憲法擁護庁との三者の協力強化が進み、NSA は、2013 年 3 月にはテロ対策での BfV との公式協力関係の樹立と、また、XKeyscore のソフトウェア（極めて有効な分析ツール）の提供を決定している。

このような状況下、2013 年 6 月に、スノーデンによる告発と内部機密資料の大量漏洩があり、ドイツでは本件に関して大量の報道がなされていることもあり、米独関係にも影をさしている。

第１部　ＮＳＡ概観

第１章　国家安全保障庁 NSA 実態研究の意義

米国の国家安全保障庁は、世界最強のインテリジェンス機関であるが、その実態は、特に我が国では知られていない。そこで先ず、NSA の実態を知ることに如何なる意義があるかについて、確認しておきたい。

１　実態研究の意義

（１）インテリジェンスの視点から

世界最先端、最強のインテリジェンス国家である米国、その中核をなすシギント組織 NSA の実態を知ることにより、第１にシギントとは何かを知ることができる。第２にシギントを通じてインテリジェンスとは何かを知ることができる。第３にインテリジェンス（諜報）コミュニティとは如何なるものかを知ることができる。

我が国は米国と安全保障条約を結ぶ同盟国であり、インテリジェンス面でも協力関係にあるのは自明のことであろう。他方、同時に、我が国は米国のインテリジェンスの対象、標的でもあり、米国のインテリジェンス能力は我が国にも向けられている。米国と協力するにしろ、我が国の秘密保全を考えるにしろ、米国のインテリジェンスの実態を知ることが不可欠である。

また、中国やロシア、更にはお隣の韓国を含む世界の国々は、技術的には米国を手本として（一部諸国は非合法手段を含めて米国の情報を収集しつつ、且つ米国とは異なり法律の制約なしに)、自らのシギントシステムの能力向上を図っており、その能力は我が国にも向けられているであろう。従って、米国の実態を学ぶことは、その他の諸国との対応においても有意義であろう。

なお、我が国でも「インテリジェンス・コミュニティ」という言葉に触れる機会が増えてきたが、筆者は、この言葉を使う者が本当に諜報コミュニティとは如何なるものかを知っているのか、疑問を感じることがある。幾つかの情報関係組織を集めて諜報コミュニティと呼べば、諜報コミュニティが成立する訳ではない。コミュニティという名称には、その名に相応しい(インテリジェンスの目標設定、収集、分析、配布等の各分野で）具体的且つ密接な協力関係の存在が前提とされている。NSA の実態の分析を通じて、真の諜報コミュニティの姿を知るのも有意義であろう。

（２）サイバー・セキュリティの視点から

現在、我が国でもサイバー・セキュリティの重要性が認識され、サイバー・セキュリティ対策に政府を挙げて取り組んでいると見られる。ところで、米国を含

む諸外国では、サイバー・セキュリティの責任部署或いは実際の中核的部署はシギント機関である[1]。それは、サイバー諜報（シギントの一部）、サイバー・セキュリティ、サイバー攻撃の三者は、実は相互に深く関連して三位一体の関係にあるという事実に基づいている。従って、我が国でもサイバー・セキュリティに効果的に取り組むためには、諸外国のシギント機関の実情を知り、この三位一体関係を理解した上で、推進する必要があるのである。

（３）テロ対策等のセキュリティ対策の視点から

テロ対策、スパイ対策そして薬物対策は、世界的には単なる治安問題に止まらず、国家安全保障上の大きな課題と捉えられている。そして、この対処には一般警察機関と共に、所謂セキュリティ・サービス（治安諜報機関）[2]が当たっている。セキュリティ・サービスは、通常、当該国のシギント機関と緊密な協力関係を有し、シギント情報を活用しているが、近時、シギント情報への依存が増大していると見られる。

実際、NSA と FBI の協力の深化には目を見張るものがある。また、NSA 自体が、その公式「６０年史」において、過去数十年に亘って、スパイ対策に加え、国際テロ対策や薬物対策のための情報収集に力を入れてきたと明言している[3]。そして現在、米国の全てのテロ対策において NSA が中心プレーヤーである、とさえ言われている[4]。

1　諸外国では、シギント機関が、その技術力を生かして実質的にサイバー・セキュリティの中核部署として機能している場合が多いが、シギント機関の秘匿性の要請から、必ずしも公式にその位置付けがなされている訳ではない。但し、オーストラリア、ニュージーランド或いはカナダのシギント機関（それぞれ、ASD、GCSB、CSE）の様に、その公式ウェブサイトで、サイバー・セキュリティ全般についての政府責任部署であることを公表している組織もある。http://www.asd.gov.au/; http://www.gcsb.govt.nz/; http://www.gchq.gov.uk/what_we_do/Pages/CESG.aspx 参照。

2 所謂「セキュリティ・サービス」とは、スパイ対策、テロ対策、政府転覆活動の防止などを目的として主として国内で活動する諜報機関である。確立した行政分野であり、通常治安担当大臣の指揮下にある。諸外国の機関には、英国セキュリティ・サービス、フランス内務省対内安全保障総局、ドイツ連邦憲法擁護庁、豪セキュリティ・インテリジェンス・サービス、米国 FBI などが存在する。我が国では現在、警察の警備公安部門と公安調査庁が、（諸外国と対比して極めて限定された権限の下）セキュリティ・サービスとしての機能を担っていると言えよう

3 US NSA/CSS, *60 Years of Defending Our Nation*, 55,74, accessed 26 August 2014, http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf

また、NSA 本部のシギント総局分析部門には、国際犯罪及び薬物に関する専門部署も存在している。”NSA’s organizational designations,” *Top Level Telecommunications*, 10 January 2014, updated 2 July 2015, accessed 9 July 2015, http://electrospaces.blogspot.jp/2014/01/nsas-organizational-designations.html

4　元米国の国家テロ対策センター長は、「NSA が傑出した選手或いは中心選手でないテ

今や諸外国の国内治安諜報の実態を理解するためにも、シギント機関の実態とその能力を知ることが不可欠となっている。

（４）一般治安維持の視点から

必ずしも広く知られていないことであるが、シギント情報は、米国その他の諸外国では、治安維持や法執行に大幅に利用されていると推定され、シギントの実態を知ることは諸外国との捜査協力や将来の我が国の捜査の在り方を検討する際の基礎知識としても不可欠であると考えられる。

例えば、米国政府の解釈では、シギント機関が対外諜報（フォーリン・インテリジェンス）[5]として一旦適正に収集した情報は、（対外諜報情報ではない国内情報も含めて）政府所有情報となり、これを犯罪捜査目的に使用することに制約はないと言い、この利用は連邦憲法修正第４条の令状主義の適用外であるとされている[6]。　また、対外諜報に関して、米国の国家安全保障法は、NSA 等の諜報諸機関は、連邦政府の法執行機関の要請に応じて、（捜査目的を含めて）その支援のため情報を収集できると規定している[7]。

ロ捜査というのは考えられない」と語っている。
--Dana Priest, “NSA growth fueled by need to target terrorists,” *The Washington Post*, 21 July 2013, accessed 21 October 2014, http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/...

[5] 米合衆国法典では、対外諜報（フォーリン・インテリジェンス）の対象となる外国勢力（フォーリン・パワー）には、外国政府又はその一部、主として外国人が組織する団体、外国政府が指揮統制する組織、国際テロ団体、外国に拠点を置く政治団体などが含まれる。US Code, Title　50, Chapter 36, Section 1801.

[6] 2014 年 3 月米司法省の報道官は、「一旦適法に収集され既に政府保有となった情報については、その情報内容を検索するのは憲法修正第 4 条で規制される捜索には当たらない」旨述べている。また、FBI 自体が、これらの情報をテロ対策やスパイ対策のみならず、一般犯罪捜査のためにも利用しており、その件数は相当量になっているという。
--Spencer Ackerman, “NSA searched data troves for 198 ‘identifiers’ of Americans’ information,” *The Guardian,* 30 June 2014, accessed 3 July 2014, http://www.theguardian.com/world/2014/jun/30/nsa-data-troves-identifiers-information.

なお、シギント活動から犯罪や犯人に関する情報を得た場合でも、情報源を秘匿するため、これらがそのまま裁判に証拠として提出されることはないと考えられる。必要な場合には、通信傍受を含め個別の令状を取って裁判に提出可能な証拠を取得しているのではないかと考える。米国に於けるシギントの捜査利用の事実が我が国で広く知られていないのは、このためと考えられる。

[7] US the National Security Act of 1947, amended through August 2007, Sec. 105A. 但し、国防総省関連の諜報機関で、対外諜報で支援を要請できるのは、国家安全保障庁 NSA，国家偵察局 NRO，国家地理空間諜報庁 NGA、国防諜報庁 DIA の４機関に限定され、陸海空軍海兵隊それぞれの諜報組織は除外されている。

（５）軍事作戦の視点から

軍事では情報は常に重要であったが、現代戦においてはシギントの重要度が益々高まっており、作戦遂行のため必須のインテリジェンスである。そして、NSA は、その正式名称 NSA（国家安全保障庁）/CSS（中央安全保障サービス）が示すように、NSA に CSS（各軍のシギント組織を調整統制する中央組織）が併設された組織である。この事実が示すのは、CSS を一体化した NSA が、米軍の作戦にとって極めて重要で不可欠な役割を担っているということである。

また、米軍は 1990 年代以降、戦争を情報の収集・送付・処理等の一連のプロセスの観点から捉えて、情報戦争（味方の情報・情報システムを防護し、敵のそれを攻撃する）に力を入れているが、この情報戦争の中心をなすのは言うまでもなくシギントである。

更に、現在、サイバー空間は、陸、海、空、宇宙に加えて第５の戦闘空間と認識されている。そのサイバー空間に於ける軍事作戦に NSA は不可欠であり、寧ろその主役であるとさえ言い得る。

従って、日本の同盟国である米軍と協力するためにも、NSA とシギントの実態を知ることが不可欠であり、NSA とシギントを知らなければ、現代の軍事作戦は語り得ないのが現実である。

（６）国家的リーダーの視点から

諸外国では、諜報機関そしてシギント機関は、外交国防治安を含め一国の行政機能の中で大きな位置を占め且つ行政全般にも大きな影響力を有している。他方、我が国では、諜報機関が極めて弱体であるため、政治指導者や幹部公務員を含め政府機関職員も諜報機関を意識することが少なく、且つ知識も決定的に不足している。（諜報機関に関する我が国のガラパゴス現象と言えよう。）　今回も NSA がドイツのメルケル首相の携帯電話を盗聴していたことが暴露されたが、世界の諜報機関の活動は友好国の首脳を含め全方位に向かっていることは、世界の常識である。我が国の指導的立場にある者、行政に係わる者にとっても、諸外国の諜報機関の実態に対する基本的知識は、その必須の基礎教養と言えるであろう。

（７）現代人の基礎知識としての視点から

最後に、現在、インターネット通信は人々の活動に不可欠なものとなっており、従って、諸外国のシギント機関のインターネット空間に於ける活動は、政府機関のみならず民間企業活動にも影響を及ぼし得るものであることである。

先ず米国については、民主主義国家としての法的制約や対外諜報戦略に基づく資源配分の制約を一先ず度外視して、純技術的に考えれば、NSA の能力は極めて

広汎に及び得るものである。即ち、インターネットでメールを遣り取りする者は、高度な暗号を使わない限り、その通信は NSA が読み得るものである、と覚悟しなければならない。また、G メール等のフリーメールや G ドライブなどのオンライン・ストレッジ・サービスなど広義のクラウド・サービスを利用する者は、その情報は NSA が読み得るものである、と覚悟しなければならない。更に、スマートフォンを持ち歩く者は、そのスマートフォンは NSA が監視用マイク、カメラ、位置情報発信機として使用できるものである、と覚悟しなければならない。そして、「仮に NSA に監視対象に選定されてしまったら、相当高度な技術的対策を採らない限り、何をしようとその監視の目を逃れることはできない」[8]ことを覚悟しなければならない。

他方、シギントに力を入れているのは米国だけではない。本稿は、研究資料の入手の観点から NSA 及びその友好機関を研究対象としているが、中国やロシア、北朝鮮、更にはお隣の韓国を含む世界の国々は、技術的には米国を手本としながら、しかし、米国の民主主義法制と比べればより少ない制約の下、或は全く制約無しに、シギントシステムの能力向上とシギント活動に邁進していると考えるのが妥当であろう。そして、その能力・活動は当然我が国にも向けられているのである。

我々はこういう世界で暮らしているのである。「現代人の基礎知識」の一環として、シギントの世界の実態を知ることには、極めて意義があると言えよう。

2　分析資料

分析に当たって使用した主な資料は次の①～④の通りである。

① 米国等の各国政府による各種公表資料

特に米国では情報公開が進み、NSA 関連情報についても NSA 公式ウェブサイト等で驚く程の量の情報が開示されている。また、従来から公表されていた各種資料の他、今回の漏洩事件を契機に秘密指定が解除されて、公表されたものもある。

② スノーデン資料（ス資料）

○ スノーデンが NSA の情報システムから持ち出し漏洩して報道された機密資料[9]。これには、NSA 作成資料、他の米国諜報機関の作成資料、後述する

---

[8] Jon Swaine and Jemima Kiss, "Edward Snowden discusses NSA leaks at SXSW: 'I would do it again'," *The Guardian*, 10 March 2014, accessed 12 March 2014, http://www.theguardian.com/world/2014/mar/10/edward-snowden-nsa-leaks-sxsw

[9] 2015 年 7 月 1 日時点でウェブサイトでアクセスできるスノーデン資料は、約 5700 頁とされる。
--"NSA Snowden Releases Tally Update - *5728 Pages," *CRYPTOME*, 1 July 2015, accessed 2 July 2015, http://cryptome.org/2013/11/snowden-tally.htm.

セカンド･パーティ諸国シギント機関の作成資料などが含まれる。米国 NSA とセカンド・パーティ諸国機関の間では、調整や経験交流等のため定期的に会合が開催されており、その際の説明資料の多くが NSA のデータベースに保管されていたものと見られる。

報道された機密資料は、Snowden Archive、IC Off the Records、The Intercept、Cryptome など多くのサイトで掲載されている。特に、Snowden Archive は今まで報道された漏洩資料を分類整理して索引が付されており、特定資料の検索には便利である。

本稿の脚註にスノーデン資料自体を引用する場合には､「ス資料」と記載して、読者の理解の資とした。

○　なお、未報道のスノーデン資料全体は、その漏洩の経緯から、グリーンワルド、ポイトラスの両人、英紙「ガーディアン」米国支局、米紙「ニューヨーク・タイムズ」、米国ニュースサイト「プロパブリカ」、独誌「シュピーゲル」が保有していると見られる。

③　エドワード・スノーデンの各種インタビュー

④　スノーデン資料等に基づく各種報道・分析記事、出版物

○　スノーデンの意向が、関係国の報道機関にはその国に関連する NSA 資料が提供されるべしというものであったとされ[10]、最初に機密資料の提供を受けたグリーンワルド、ポイトラス両氏、或いは英紙「ガーディアン」を通じて多くの国の報道機関に資料が提供されたようである[11]。このスノーデン資料を基にして、各国の安全保障問題担当のジャーナリストや研究者による分析報道が大量になされている。

また、これに触発されて、インテリジェンス関係者からの匿名取材、或は資料提供を基にした報道もなされている。

○　本事件に関する出版物としては、グリーンワルド、ルーク・ハーディング両氏の著作がある[12]。但し、グリーンワルドの著作については　既に NSA 資

---

[10] Luke Harding, *the Snowden Files* (New York: Vintage Books, 2014), 145.

[11] 資料提供の条件として、スノーデンは、報道前に関係国政府当局に記事を提示することを課したという。その目的は、政府による検閲を受けることではなく、報道によって活動中のヒューミント要員を危険に晒したり、誰かが殺されたりすることのないようにするためであると語っている。
--Edward Snowden, interview by Runa A. Sandvik on 8 May 2015, Forbs, 10 May 2015, accessed 26 May 2015,
http://www.forbes.com/sites/runasandvik/2015/05/10/what-edward-snowden-said-at-the-nordic-media-festival/

[12] Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014) 及び上記 Harding, *Files*。

料の解釈誤りが数点指摘されている[13]。また、ルーク・ハーディングの著作は、漏洩事件自体を描写したもので、NSA の実態に関する記述は殆どない。他に、ドイツで出版された Der NSA-Komplex が優れていると言われるが、残念ながらドイツ語版しかないので、参照していない。

①～③は一次資料（或いは擬似一次資料）ではあるが、②のスノーデン資料は NSA を初めとする諜報機関の内部資料である。そのため、諜報機関独特のコード名や隠語が多用されており、その解釈は必ずしも容易ではない。また、④の報道記事や出版物は、分量は膨大であるが、その内容は報道する記者や著者の知識や理解力の程度によっては正確ではないものもある。これらの報道記事では、分析根拠としてスノーデン資料を抜粋表示してあるものもあれば、そうでないものもある。そこで、これらについては合理的に判断してより真実に近いと考えられるものに依拠した。

そのため、NSA についての記述は、全体像については概ね実際を反映したものとなったと考えるが、細部においては誤解や解釈の誤りがある可能性がある。現在でも、スノーデン資料自体の報道が徐々に進んでいるので、今後も実態研究を継続したいと考えている。

[13] グリーンワルド氏の報道記事や著作に関しては、同氏が米国政府批判に急な余りスノーデン資料の解釈において極端に走る傾向があり、その解読には特に注意する必要がある。2013 年 6 月の当初の報道キャンペーンの一部を荷なった Global Informant（後述）に対する同氏の解釈にも問題が指摘されている。

第２章　国家安全保障庁ＮＳＡ概観

NSA の収集能力や活動の実態の分析に進む前に、理解のための基礎知識として、NSA とは如何なる組織であるかについて、主として NSA による開示資料を基に、概観してみたい。

１　シギント機関と諜報諸機関

NSA はシギント機関であるが、諜報諸機関の中で如何なる位置付けにあるのだろうか。

先ず、インテリジェンスの諸機能は、大きく、次の三つに大別できる。

① 対外諜報活動～～国家運営に必要な諸外国に対する諜報活動である。これを諜報活動の方法により区分すると、主要な活動方法として、ヒューミント、シギント、イミントの三つが挙げられる。米国おけるそれぞれの主たる担当組織は次の通り。

ヒューミント（人的な諜報）：　中央諜報庁 CIA
シギント（信号諜報）　　：　国家安全保障庁 NSA
イミント　（画像諜報）　　：　国家地理空間諜報庁 NGA

② 軍諜報活動～～戦争・戦闘を前提に、潜在敵国の戦力組成を初め軍事力の現況等を把握し、戦争・戦闘を効果的に遂行するための諜報活動である。米国では、国防諜報庁 DIA 及び陸海空軍海兵隊の各諜報組織がこれに当たる。

③ セキュリティ・サービス（国内治安諜報活動）～～国家の基本秩序を、スパイ・テロ・政府転覆活動など違法な侵害から守るための諜報活動である。米国では、FBI の諜報部門がこれに当たる。

一般に対外諜報については、ヒューミントが意識されることが多く、米国の CIA、英国の SIS（秘密諜報機関）、或いはイスラエルのモサドなどが有名である。しかし、世界の先進民主主義国家では、対外ヒューミント機関に加えて（或は、対外ヒューミント機関を持たない場合にも）、シギント機関が整備されているのが通例である。そして、シギント機関である NSA は、米国の諜報コミュニティを構成する１７の諜報機関の中でも、最大最強の諜報機関であると見られている。（但し、シギントは特に情報源の秘匿のために極めて高度な秘密保持が課されており、その重要性にもかかわらず、余り知られていない。）

他の先進国のシギント機関としては、英国の政府通信本部 GCHQ、オーストラリアの豪信号局 ASD、ニュージーランドの政府通信保全局 GCSB、カナダの通信保全局 CSE、イスラエルのシギント国家部隊 ISNU（別名 8200 部隊）などがある。また、ドイツやフランスでは、シギントの独立機関を設置せず、それぞれ対

外諜報機関である連邦諜報庁 BND や対外安全保障総局 DGSE の一部局として設置されている。

２　NSA の沿革

（１）米国シギントの成果の歴史

NSA の発足は、1952 年であるが、米国はそれ以前から陸海軍がシギントに力を入れてきた。NSA の「５０年史」[14]によれば、その成果には次の例がある。

- 1923 年ワシントン海軍軍縮交渉で、日本の外交暗号を解読して、交渉を有利に進めた。
- 第二次世界大戦時、日本の外交暗号を解読。また、海軍暗号を解読して、珊瑚海海戦、ミッドウェー海戦に貢献した。
- 第二次世界大戦後、ソ連 KGB と在米ソ連大使館の間の暗号通信の一部を解読し、米国内に広汎に張り巡らされたソ連スパイ網の解明に貢献した。

（２）NSA 発足

第二次世界大戦後、1949 年に陸海軍シギント組織は統合され、軍安全保障庁（AFSA）が発足した。しかしながら、軍安全保障庁は、1950 年から始まった朝鮮戦争で（第二次大戦時と比べても）十分に機能を発揮できず、各軍が不満を持った。また、軍安全保障庁は国防総省の統合参謀本部の隷下にあり、これには、国務省と CIA が軍事的側面が強過ぎて国家的側面が不十分だとして不満を持ったという。

そこで、1952 年、時のトルーマン大統領は、CIA 長官と国務長官からの働き掛けを受けて、シギント改革のための委員会（ブラウネル委員会）を設置した。ブラウネル委員会は、シギントは国家的責務であるとする報告書を提出し、これに基づいたトルーマン大統領の指示より、1952 年 11 月 4 日に国家安全保障庁 NSA が国家諜報機関として発足した[15]。発足時の NSA の職員数は、7600 人であった[16]。

但し、シギントは国家の最高機密であり、これらの事実は NSA の存在自体を含めて極秘事項とされた。そのため、NSA は通称「No Such Agency」（存在しない役所）と呼ばれ、その存在が公認されたのは発足後 20 年以上経った 1975 年の

---

[14] US NSA, *Cryptologic Excellence: Yesterday, Today, and Tomorrow,* accessed 2003, http://www.nsa.gov/....

[15] US NSA, *Cryptologic Excellence.*

[16] US NSA, *60 Years of Defending Our Nation*, 3, accessed 1 September 2014, https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf.

ことであった。

なお、NSA を初め、米国のシギント諸機関にはセキュリティの名を冠している例が多い。これは、当初その存在と任務を秘匿するため、シギント名称を避けたためと考えられる。結果として、米国政府ではセキュリティの単語が、国家安全保障とシギントと二義的に使われている[17]。

（３）CSS 附置[18]

米国のシギント中央機関 NSA は、このようにして発足したが、陸海空軍海兵隊は戦闘を支援するための組織としてそれぞれ諜報組織を保有しており、各軍のシギント組織も存続し続けた。

しかし、シギント組織が、中央機関 NSA と各軍の諸組織に分散しているのは非効率であり、統合が模索された。当初は、単純に NSA に各軍のシギント組織を吸収統合する案も検討されたが、その場合、新組織が各軍指揮官の戦術的要請に十分応え得る組織となるか、不安が表明された。そこで、結局、NSA への組織的統合は見送られ、各軍のシギント諸組織の活動を調整して一体化するための中央組織を設置し、この長を NSA 長官が兼務することによって、実質的な一体化を目指すこととされた。

このために 1972 年 2 月設置されたのが、中央安全保障サービス CSS（Central Security Service）である。これは各軍のシギント組織の活動を調整し一体化するための組織である。長は NSA 長官であり、事務局が NSA 本部内に置かれている。NSA は、その「６０年史」で、NSA と CSS の併設は、各軍シギントの基準や教育を向上させると共に、NSA と各軍シギント諸組織の中央集権強化の基礎となったと評価している。

（４）サイバー司令部併設[19]

２１世紀に入ると、デジタル・ネットワークへの依存が増大しサイバー空間の重要性が認識された。そこで、米国防総省では 2005 年に「ネットワーク戦争」用の部隊を編成し NSA 本部に配置して、NSA 長官に司令官を兼任させた。ところが、2008 年外国諜報機関から送られたマルウェアが軍情報通信網に感染する事案が起きたが、その際に、これへの対処で NSA の技術力が発揮された。これを契機に 2010 年 10 月米軍の統合軍の一つとしてサイバー軍（司令官は大将）が編

---

[17] National Security Council は字義通り「国家安全保障会議」であるが、National Security Agency は、寧ろ「国家シギント庁」と訳した方が適切であろうが、本稿では通例に倣い「国家安全保障庁」の翻訳名を使用している。

[18] US NSA, *60 Years*, 53.

[19] US NSA, *60 Years,* 101-102.

成され、司令部はNSAと同じフォート・ミード内に置かれ、司令官はNSA長官が兼任することとなった。

サイバー軍は、平時には、国防総省の情報システムの保全等に当たるが、有事には正にサイバー戦争の担い手となる組織である。(サイバー戦争とシギントの密接な関係については後述。)

こうして現在、NSA長官は、同時に米軍サイバー軍司令官であり、また、CSS長でもある。そして、サイバー司令部もCSS司令部も共にNSA本部のあるフォート・ミードに位置している。(CSS司令部は実質的にはNSA本部の一部となっている。)

なお、スノーデンの告発を契機とした米国内のNSA改革論議の中で、2013年中にはサイバー軍司令官とNSA長官を分離すべしとの意見も一部で主張されたが、2014年に至るとその議論は急速に収束した。サイバー軍とシギント組織の密接な関係が理解されたためと考えられる。

3　任務

NSAの任務は、シギントと情報保証の二つであり、また、コンピュータ・ネットワーク作戦（サイバー戦争）を可能とすることであるとされている[20]。

（1）シギント（シグナルズ・インテリジェンス、信号諜報）

NSAは、国家的任務及び各省庁の任務を支援するため、「対外諜報」及び「防諜」目的[21]で、シギントの収集、分析、作成、配布を行う。また、NSA長官は、CSSの長として、各軍のシギント組織が行うシギント活動を統制する。

更に、NSA長官は、米国の全てのシギント活動の実質的責任者（Functional Manager）として、（CIAやFBIが行うものも含めて）その全体戦略・方針・基準の策定、教育訓練、活動の調整などに責任を有する[22]。

ところで、シギントの主要分野は、コミント（コミュニケーションズ・インテリジェンス、通信諜報）とエリント（エレクトロニック・インテリジェンス、電子諜報）の２つである。

---

[20] US NSA/CSS, *The NSA/CSS Mission,* accessed 26 August 2014, http://www.nsa.gov/about/mission/index.shtml.

[21] 国家安全保障法の定義によれば、「フォーリン・インテリジェンス（対外諜報）」とは、外国政府、外国組織若しくは外国人（以下「外国勢力」）の能力・意図・活動に関する情報、又は国際テロ活動に関する情報。「防諜（カウンターインテリジェンス）」とは、外国勢力によるスパイその他の諜報活動、破壊活動若しくは暗殺、又は国際テロ活動から防禦するための情報及び活動である。The National Security Act of 1947, amended through August 2007, Sec. 3参照。

[22] US EO 12333, amended through 2008, Sec.1.3.(b)(12)参照。

コミントは、第一次世界大戦の頃から既に盛んに行われてきたが、無線通信、電話電信、衛星通信などの通信を傍受し分析して情報を得る活動である。分析の手法としては、暗号解読（クリプト・アナリシス）が良く知られている。重要な通信文は暗号化されている場合が多いため、これを解読することにより通信内容そのものを知ろうとするものである。このほかに通信状況分析（トラッフィク・アナリシス）という手法も有力である。これは、（通信文の暗号解読ができない場合を含め）何処から何処に何時通信をしたかという外形的な通信状況を精密に分析することにより情報を得ようとするものである[23]。

エリントは、レーダーなどの電磁波を傍受し分析して情報を得ようとする活動である。これは、第二次世界大戦中から始まったが、兵器その他でレーダーの使用が一般化したことに伴い、その後更に重要性が増した新しいシギント分野である。例えば、レーダーの電磁波を精密に分析することにより、（その特定のレーダーを使用する）対空機関砲や対空ミサイルの配備状況を調べることができる。

この他シギントには、フィシント（フォーリン・インスツルメント・シグナル・インテリジェンス）という分野もあるなど、極めて広汎且つ専門性の高いインテリジェンスである。但し、本稿で扱うのは、インターネットを中心とするコンピュータ・ネットワークを対象とする情報活動であるので、コミントの一部ということになる。

（２）情報保証（Information Assurance）

NSA は発足以来、通信保全（COMSEC）を所掌しており、暗号や暗号通信機や秘匿電話機の開発管理に当たってきた。これは、攻撃方法を知っている者が、同時に有効な防禦方法を開発することができるからであり、合理的な任務付与であろう。

その後、時代と共に通信方法が多様化し、インターネット等が発展すると、単なる通信保全ではなく、情報システム保全（INFOSEC）に任務が拡大した。更に、これが現在の米国政府では、情報保証という任務に発展している。

NSA は米国政府の情報保証に関する責任部署である。即ち、NSA 長官は、大統領命令第 12333 号により、米国の国家安全保障システム（National Security System）の責任者(National Manager)として指定されている。国家安全保障システムとは、米国のインテリジェンス、軍事、秘匿情報など国家安全保障に係わる

---

[23] Donald A. Borrmann, et. al., *The History of Traffic Analysis: WW I -Vietnam,* Center for Cryptologic History, NSA, 2013, accessed 10 October 2014, https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/traffic_analysis.pdf

通信情報システムのことである[24]。　NSA のシギント活動では、日頃から他国のインターネットやコンピュータなどの情報通信システムに侵入しており、いわば矛を磨いている。そのような矛を磨いている組織こそ、同じシステムの防禦＜盾＞を担うに相応しいのである。

NSA は情報保証の基準として、システムが備えるべき５つの項目を示している。即ち、

① Confidentiality（秘密保持力）（機密性）
② Data integrity（データが改変されないこと）（完全性）
③ User authentication（ユーザー認証機能）（真正性）
④ Transaction non-repudiation（通信履歴保持力）（否認防止）
⑤ System availability（システムが利用できること）（可用性）

要するに、秘密が守れて、信頼でき且つ使い易い通信情報システムであるが、そのためには多層防禦（保全技術やサービスを積み重ねて、敵対者と重要システムの間に多数の障碍を設定すること）が重要としている[25]。

なお、参考ながら、このような思想の下、米国の通信情報システムは、秘匿度に応じてネットワーク自体も概ね３段階に区分されている[26]。即ち、①トップシークレット情報を扱えるシステム（国防総省 JWICS、NSA の NSANet、国務省 INRISS、FBI・SCION），②シークレット情報を扱えるシステム（国防総省 SIPRNet, 国務省 ClassNet、FBI・FBINet）、③秘密情報以外の機微な或いは部内用の情報を扱えるシステム（国防総省 NIPRNet、国務省 OpenNet、情報機関用 DNI-U）である。③だけがファイアーウォールを介してインターネットに接続されている[27]。

---

[24] US EO 12333, amended through 2008, Sec. 1.7.(c)(6)参照。
米国の国家安全保障に係わる情報通信システムの保全に関しては、当初 1990 年に国家安全保障通信情報システム保全委員会（NSTISSC）が設置されていたが、2001 年これが国家安全保障システム委員会（CNSS）に改組された。同委員会の任務は国家安全保障に係わる情報システムに関する政策、指針、基準等の策定・指導であり、参加省庁は２１に及ぶ。NSA はその責任部署である。

[25] US NSA, *Cryptologic Excellence*

[26] "US military and intelligence computer networks," *Top Level Telecommunications,* 11 March 2015, accessed 12 March 2015, http://electrospaces.blogspot.jp/2015/03/us-military-and-intelligence-computer.html

[27] 我が国では、内閣の情報セキュリティ政策会議が、「政府機関の情報セキュリティのための統一規範」（平成 23 年 4 月 21 日決定、26 年 5 月 19 日改定）や「政府機関の情報セキュリティのための統一基準」（平成２６年版、26 年 5 月 19 日決定）を定めている。
これらによれば、政府の情報には全て「機密性」「完全性」「可用性」についての格付けを付すこととされている。米国の例を見ても分かるように、機密性とか完全性、可用性というのは、本来的にはシステムが保持すべき機能であって、個別の情報にこれらの格付けをし、記載することは想定されていない。今回スノーデンによって開示された機

（３）コンピュータ・ネットワーク作戦（Computer Network Operation サイバー戦争）の基盤

サイバー戦争自体は、米サイバー軍の任務であって、NSA の任務ではないが、NSA 長官がサイバー軍司令官を兼務している事実が示すように、両者は密接に関連している。

即ち、サイバー戦争（或いは戦闘）を遂行するためには、普段から、潜在的な攻撃対象の実態・弱点を把握して、いざとなれば攻撃できる態勢を構築しておく必要がある。これは、正にシギント活動で得られるものである。また、防禦面でも、平時から高度な情報保証が実現していれば、いざとなった時も防禦能力が高いことになる。更に、積極防禦では、敵対者のサイバー攻撃の資源・発信元を攻撃して無力化する準備も必要である。

こうして、普段のシギント活動と情報保証の二つの任務を遂行すること自体が、そのために構築したインフラストラクチャを含めて、必然的にコンピュータ・ネットワーク作戦（サイバー戦争）を可能とする基盤作りとなるので、その役割が与えられているのである。後述するが、NSA の脅威作戦センター（NTOC）は、このための重要な作戦部署の一つである。

４　予算・人員・組織

（１）予算

米国の諜報関係予算は、国家諜報計画（National Intelligence Program）と軍諜報計画（Military Intelligence Program）に分かれ、それぞれ、1990 年代から総額が開示されるようになった。それによれば、2014 会計年度の国家諜報計画予算が 522 億ドル、軍諜報計画予算は 186 億ドル、合計 708 億ドルと 8 兆円以上の巨額に及んでいる[28]。

密資料にも、当然のことながらトップクレットやシークレットの秘密区分の記載はあっても、機密性、完全性、可用性などの記載はない。

我が国でも、秘密区分や秘密情報へのアクセス権限付与などの制度手続の統一的整備は当然の前提として、更に、インターネット接続の可否、回線の秘匿強度基準などシステムが保持すべき保全機能の定義が待たれるところである。

[28] US Office of DNI, *DNI Releases Updated Budget Figure for FY 2014 Appropriations requested for the National Intelligence Program,* New Release, 27 June 2013, accessed 22 July 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/888-dni-releases-updated-budget-figure-for-fy-2014-appropriations-requested-for-the-national-intelligence-program.

—— US Department of Defense, *DOD Releases Revised Military Intelligence Program Request for Fiscal Year 2014,* New Release, 27 June 2013, accessed 22 July 2013,

しかし、諜報予算の内訳は、現在でも秘密とされている。ところが、スノーデン資料により、2013 年度の国家諜報計画予算の内容が判明した[29]。

内部資料によれば、2013 会計年度の国家諜報計画予算は 526 億ドル、軍諜報計画予算 192 億ドル、合計 718 億ドルに上る。

国家諜報計画の内、主要な組織毎の予算は多い順に、CIA 予算 147 億ドル、統合シギント予算（NSA）108 億ドル、国家偵察局（NRO）予算 103 億ドル、国家地理空間諜報庁（NGA）予算 49 億ドルである[30]。

NSA 予算は、ヒューミントを中心とする CIA 予算より少ないが、実際のシギント予算は、この統合シギント予算以外の予算にも分散して計上されており、依然として、諜報予算中最大であると言えるであろう。即ち、①国家偵察局は人工衛星による情報収集を担当しているが、これにはシギント衛星関係費用が総額 103 億ドルのうち相当額（数十億ドル以上）含まれていると推定できること、②CIA 予算の中に NSA との共同シギント事業が少なくとも 6 億ドル程度は計上されていること[31]、③軍諜報計画予算 192 億ドルの詳細は不明であるが、その中には、陸海空軍・海兵隊・沿岸警備隊のシギント予算が相当額含まれており、数十億ドルは下らないと推定できること、これらの点を勘案すれば、米国政府のシギント予算総額は、200 億ドル前後にも及ぶのではないかと推定される。即ち、シギントは、邦貨で２兆円規模の巨大行政機能であるということになる。

（２）人員

米国の諜報機関の現在の人員数は、開示されていない。少し古い数字になるが、国家諜報長官によれば、2009 年 9 月時点の諜報機関全体の人員数は、（国家諜報計画、軍諜報計画を合わせて）約 20 万人とされている[32]。

---

http://www.fas.org/irp/news/2013/06/mip-2014.html.

[29] ス資料 *FY2013 Congressional Budget Justification Vol. Ⅰ : National Intelligence Program Summary*, February 2012, accessed 20 August 2014, http://fas.org/irp/budget/nip-fy2013.pdf.

[30] 本文に記載した他、国家諜報予算の内訳は、総合軍諜報（国防諜報庁等）予算４４億ドル、司法省（FBI）予算３０億ドル、インテリジェンス・コミュニティ運営（国家諜報長官室）予算１７億ドルと続いている。

スノーデン資料 *National Intelligence Program Summary* 135 頁を合理的に解釈すると、これらの予算が連邦政府予算全体として公表される際は、NSA の予算は、CIA、NGA、NRO 予算等と同様に、国防総省予算の中に見えない形で吸収されていると見られる。

なお、小林良樹『インテリジェンスの基礎理論』第二版（立花書房、2014 年）217－218 頁は、NSA 予算を軍諜報計画に含まれると解釈しているが、NSA 予算は国家諜報計画に含まれる。軍諜報計画に含まれるのは、陸海空軍等のシギント予算である。

[31] *National Intelligence Program Summary*, 161.

[32] US Office of DNI, *Media Conference Call with the Director of National Intelligence Mr. Dennis C. Blair, 2009 National Intelligence Strategy,* 15 September 2009 ,

今回の内部資料によれば、2013 年会計年度の国家諜報計画による全職員定数は、10 万 7035 人である[33]。この内訳は、シビリアンが 8 万 3675 人、軍人が 2 万 3400 人である。この他、常時勤務の契約職員が 2 万 1800 人いる[34]。（なお、この契約職員には、一般的に特定の任務或はプロジェクトのために民間企業から派遣される職員は含まれないとされる。そこで、スノーデンは、外数の企業派遣職員であって、契約職員には含まれないと見られるが、その点は必ずしも明確でない。）

NSA の職員定数は、3 万 4901 人であり、次に多い CIA 職員定数 2 万 2206 人を抑えて、国家諜報計画では一番職員数が多い。NSA の内、シビリアンは約 2 万 1500 人、軍人が約 1 万 3500 人である[35]。

但し、これがシギントに係わる全職員数ではなく、予算と同様に、NSA 外でもシギントで活動する人員は多い。特に、CSS 傘下のシギント組織（実質的に NSA が統制する陸海空軍、海兵隊、沿岸警備隊のシギント組織）の人員は相当数に及ぶと考えられる（約 1 万 2000 人との推定値があるが根拠は定かでない[36]）。更に、NSA 本体で勤務する契約職員もおり、シギント全体で勤務する人員は、少なくとも 5 万人程度には及ぶと見られる[37]。

（３） 組織

公表資料によれば、NSA の組織は、先ず、NSA 長官（軍人）と副長官（シビリアン）の下に各部局が置かれている。また、NSA 長官は同時に各軍シギント組織全体を指揮統制する CSS の長でもあり、CSS には副長として軍人（一般的に少将の階級にある者）が配置され、そのための司令部も置かれている。

更に、NSA は本部の他に、米国領土内にミニ NSA とも呼べる地方本部（RSOC: Regional Security Operations Center）を四つ設置している。ハワイ州、コロラ

---

http://fas.org/irp/news/2009/09/dni091509-m.pdf.

[33] *National Intelligence Program Summary*、134.

[34] "The Black Budget: Funding the intelligence program," *The Washington Post*, accessed 18 November 2013, http://www.washingtonpost.com/wp-srv/special/national/black-budget/

[35] *National Intelligence Program Summary*, 134,137.
職員数で NSA と CIA に次ぐのは、統合軍諜報予算（国防諜報庁等）が 1 万 7239 人、司法省（FBI）が 1 万 5072 人、以下、国家地理空間諜報庁 8519 人、国家偵察局 2904 人と続いている。

[36] "NSA's organizational designations," *Top Level Telecommunications,* 10 January 2014, updated 25 August 2014, accessed 28 August 2014, http://electrospaces.blogspot.jp/2014_01_01_archive.html

[37] グリーンワルド氏は、NSA の為に働く民間企業社員総数を約 6 万人と推定しており、仮にこれが正しいとすれば、NSA/CSS に勤務する全従事者は正規職員と合わせて 10 万人を超えることとなる。しかし、6 万人の根拠は示されていない。
Greenwald, *No Place,* 101.

ド州、ジョージア州、テキサス州である。

NSA 本部の内部組織は、スノーデン資料を含めて分析したとする資料[38]によれば、NSA 長官の下、長官室の他、次の３つの総局、５つの局、２つのセンターで構成されている。

- 総局：　シギント総局、情報保証総局、技術総局
- 局　：　教育訓練局、施設兵站局、人的資源局、保全防諜局、調査研究局
- センター：国家安全保障作戦センター（NSOC）、NSA/CSS 脅威作戦センター（NTOC）

この内、NSA/CSS 脅威作戦センター（NTOC）の任務は、世界のネットワーク上の活動を監視することにより、ネットワーク上の脅威を発見して米国と同盟国のネットワークを保護することであり、いわば NSA のサイバー防衛のための作戦基地である。また、国家安全保障作戦センター（NSOC）は、シギント及び情報保証のため、毎日 24 時間、世界の状況を包括的に把握する作戦センターであり、いわばシギントによる世界の現況監視センターである[39]。

なお、NSA 長官は、大統領が上院の同意を得て任命する。これは、国家諜報長官や CIA 長官と同じ位置付けである。

５　NSA の活動の根拠と法的規制の基本構造

本稿の目的は、世界最強の諜報機関である NSA の実態を探求することであり、その諜報活動の適法性、違法性の議論自体はテーマとはしていない。しかし、NSA の活動の根拠と法的規制の基本構造を理解しておくことは、今後の議論、そして米国における議論を理解する上で、有益であろう。

即ち、重要な点は、フォーリン・インテリジェンス（対外諜報）監視法は、NSA によるシギント活動の根拠法ではなく、基本的には米国内でのシギント活動に対する制限法であったということである。

（１）大統領命令 12333 号（Executive Oder12333）：根拠法令

米国のシギント活動の最大の根拠法令は、大統領令である。即ち、大統領の行政権には、憲法上、国家安全保障のための広汎な権限が含まれる[40]と解釈されて

---

[38] “NSA‘s organizational designations,” *Top Level Telecommunications.*

[39] US Office of the DNI, *National Intelligence: A Consumer's Guide 2009,* 43, accessed 9 September 2014, https://archive.org/details/nationalintelligenceconsumersguide.

[40] 合衆国憲法第２章第１条の大統領就任時の宣誓文“Ｉ…will, to the best of my ability, preserve, protect and defend the Constitution of the United States."には、その趣旨が体現されていると解釈されている。James G McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview,* (2009), accessed 29 August 2014,

おり、対外諜報はその一部と理解されている。従って、基本的に、対外諜報は、法律の根拠なしに、米国の内外に於いて大統領の行政命令によって行うことができる[41]。

対外諜報に関する現在有効な行政命令が、大統領命令 12333 号「合衆国諜報活動」である。これは、1981 年 12 月レーガン大統領によって制定され、累次の改正（直近の改正は 2008 年ブッシュ大統領による）を経て現在に至っている。

大統領命令 12333 号は、諜報諸機関の任務、権限と活動の基本を定めており、諜報諸機関はこれに基づき（個別の法律の根拠を必要とせず）、対外諜報を行っている。

（２） 対外諜報監視法（Foreign Intelligence Surveillance Act）

しかしながら、米国史上では、行政府が権限を濫用したことが度々あり、特に米国がベトナム戦争を戦った 1960 年代には、FBI や CIA や陸軍諜報機関が、法律の根拠なしに反戦運動や反戦運動家に対して広汎な情報収集を行った。更に、1972 年にはニクソン大統領によるウォーターゲート事件が惹き起こされた。

これに対して、1976 年上院のチャーチ委員会は、諜報諸機関の活動に関し「如何なる諜報機関も、法律の根拠なしに国内諜報活動に従事してはいけない」「対外諜報のためであっても、NSA は国内通信を傍受してはならない」等の勧告を行った。

この勧告を踏まえて、1978 年対外諜報監視法が制定された。これは、本来、米国内の対象を標的として米国内で行われる諜報活動、特に電子的な諜報収集に制約を課したものであり、このため、対外諜報監視裁判所が設置された。即ち、米国内で対外諜報及び防諜のためのシギント活動を行うには、原則として監視裁判所（秘密審議）の令状を要することとなった。但し、本法律は、米国外での活動は規制対象外であり、米国外での活動（米国内から行う外国標的に対する対外諜報を含む）は、依然として大統領の裁量に委ねられている。

その後、本法律は改正され、物理的捜索やビジネス記録の提出等の規定が加わった。更に 9/1 1 テロ事件後の 2001 年の愛国者法制定、2008 年の対外諜報監視

---

http://www.flect.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/foreign-intelligence-surveillance-act. html.

要するに、対外諜報を含む国家安全保障の活動については、本来、大統領は法律の根拠なしに（実力の行使を含めて）行うことができる。但し、その分野であっても、連邦議会が制定した法律があれば、その範囲で法律が拘束力を有することとなる。

[41] US White House, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, 64, 69. Accessed 29 August 2014, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

法改正（702 条）などにより、（FBI を含む）諜報諸機関の権限が拡大され、単に、米国内での対外諜報活動を規制するものから、米国内で行う対外諜報（米国内から行う国外標的に対する諜報を含む）について、民間事業者に協力義務や守秘義務を課すなど強制権限規定の色彩も帯びてきている。

6　国家諜報機関（National　Intelligence）としての発展

NSA は、前述の通り、国家諜報機関として発足したものであるが、国防長官傘下の機関であることもあり、これを単に国防総省の一諜報機関と理解する者もいるようである。しかし、これは正しくない。

米国では、第二次大戦直後から既にインテリジェンスの区分として、国家諜報（National Intelligence）と省庁諜報（Departmental Intelligence）の違いが意識されてきた。省庁諜報とは、特定の省庁や軍の任務達成のために必要な諜報活動であり、これに対して国家諜報とは、特定省庁或いは軍の関心や能力を超えて、国家政策や国家安全保障の幅広い観点を包含する諜報活動とされている。但し、1948 年時点では、国家諜報を作成配布する責任部署は、CIA のみであった[42]。

NSA は、こういう状況下に、不完全ながらも 1952 年に国家諜報機関として発足し、その発展と共に、益々、ナショナル・インテリジェンスとしての性格を強めて、現在、国家諜報機関として任務を十分果たせるようになったと評価できる。即ち、陸海空軍海兵隊の作戦支援任務は維持しつつも、大統領などの政府最高指導部や国防総省以外の省庁を含む政府全体に対する諜報支援を果たし得る組織に発展している。

その経緯を、法令や（秘密指定を解除された）国家安全保障会議インテリジェンス指令など米政府による公開情報から概観してみたい。

（１） 1952 年 NSA 発足時とその後

NSA はブラウネル委員会の報告書を基礎に設置された。同報告書は「コミント（当時）は、（特定の軍や省や庁の責務とは異なり）国家的責務である。従って、その活動は、参加省庁と政府全体にとって最適の結果を生むように、参加省庁の全ての資源を有効活用するように組織運営されなければならない。」としている[43]。これに基づき、1952 年 10 月にトルーマン大統領によるメモランダム[44]と国家安

---

[42] US NSCID No.3（国家安全保障会議インテリジェンス指令第 3 号）, “Coordination of Intelligence Production,” 13 January 1948, accessed 1 September 2014, https://history.state.gov/historicaldocuments/frus1945-50Intel/d426

[43] US NSA, *Cryptologic Excellence.*

[44] Harry S Truman, *Communications Intelligence Activities*, 24 October 1952, https://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/1950s/documents/19521024_1950_Doc_3978766_Comms.pdf

全保障会議インテリジェンス指令第 9 号[45]が発出され、NSA が発足した。

このように NSA は国家諜報機関を目指して発足した。しかしながら、当初からナショナル・インテリジェンスの性格が十分に強かった訳ではない。即ち、同指令第 9 号（1952 年）とこれを引き継いだ同指令第 6 号（1958 年）[46]によれば、次の通りである。

① 任務付与（Tasking）その他運営：中央諜報長官が主催する合衆国コミント委員会（USCIB: United States Communications Intelligence Board、後にインテリジェンス委員会と改称）が運営に当たることとなった。その構成員は、中央諜報長官と NSA 長官の他、国務省、国防総省、FBI、陸海空軍省、CIA 代表である。同委員会の勧告は拘束力があるとされ、国家的性格が担保された。1958 年には、シギントの目標、情報要求、優先順位についても、同委員会が定めることが明示された。

但し、NSA はまだ国防省内の一組織としての位置付けが強く、運営事項に対する勧告の相手は国防長官であり、また、勧告案に国防総省が反対の場合は、同委員会の上級組織である国家安全保障会議コミント特別委員会（国務長官と国防長官の 2 人が委員、CIA 長官が参与）に上訴できることとなっている。（なお、緊急時の上訴先は大統領。）

このように国家諜報機関としては不十分な点はあるものの、本改革前の軍安全保障庁 AFSA は統合参謀本部指揮下、即ち、完全に軍の指揮系統内にあったのであり、それがこの改革によって、シビリアンの国防長官に直結することとなり、各軍からの独立は実現されたと言える。

② 情報配布：完成された情報の作成配布はあくまで関係省庁の所掌であり、NSA はそのための素材情報を作成するものとされていた。即ち、コミント委員会参加の軍諜報諸組織、国務省、FBI、CIA への素材情報の提供に限定されていた。（1958 年時点）

③ 人事：NSA 長官は、統合参謀本部と協議の上で、国防長官が指名するとされ、依然として国防総省内の一部局としての扱いであった。また、職員の採用に関しても、独立した権限は付与されていなかった。

④ 予算：基本的には、国防総省内の陸海空軍省からの持ち寄り（一部国務省や

---

[45] US NSCID No.9（国家安全保障会議インテリジェンス指令第 9 号）, “Communications Intelligence,” 24 October 1952,
https://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/1950s/documents/19521229_1950_Doc_3986605_NSCID9.pdf

[46] US NSCID No.6（国家安全保障会議インテリジェンス指令第 6 号）, “Communications Intelligence and Electronics Intelligence,” 15 September 1958,
https://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/1950s/documents/19580915_1950_Doc_3987508_NSCID6.pdf

CIA からの拠出可能性あり）であり、独自の予算編成権限は付与されていなかったと推定される。

しかしながら、実際の運用の必要性から、1959 年に、人事面では、NSA 独自の採用解雇権が認められ、予算面では、統合シギント予算（Consolidated Cryptologic Program)が開始されて NSA 関係予算は NSA に一元化されるなど、人事・予算面での独立性が強化されてきた。

また、アイゼンハワー大統領の指示で、クリティークという国家緊急情報制度システム（世界中の緊急重要情報を、事態認知後 10 分以内に大統領初め政府首脳に速達するシステム）を構築し、1963 年に完成させた。

更に、1961 年のキューバ危機では、ホワイトハウスに NSA 職員が常駐しシギント情報を提供するなどして、シギント情報の価値が高く評価され、1960 年代を通じて、シギントは単なる素材情報の提供から分析成果を配布するようになっていった[47]。これに伴い、「サニタイズ」（情報化に当たって資料源を秘匿するための技法）も発展し、徐々に情報の配布対象が拡大されたと推定される。

（２） 1972 年 CSS 附置時とその後

上記の発展を受け、1972 年の CSS 発足時は、国家安全保障会議インテリジェンス指令第 6 号（1972 年）に見られる通り、更にナショナル・インテリジェンスの性格が顕著になっている[48]。

① 任務付与：シギントの目標、情報要求、優先順位については、米国の全てのシギント活動について、中央諜報長官が、合衆国インテリジェンス委員会の助言を得て、制定することとされた。この点で、ナショナル・インテリジェンスの形式が完成されたと言えよう。

② 情報配布：NSA は完成された情報の作成配布は依然として認められていないが、シギント情報の作成「配布」が認められ、実質的にシギントというシングル・ソースとしてのナショナル・インテリジェンスの地位が認められた。

③ 人事：NSA 長官と副長官の指名は、依然として国防長官であるが、大統領の承認が必要とされ、更に、任期は大統領が定めることとされた。

④ 予算：中央諜報長官が、統合予算準備の基礎として、シギントの需要と成果をレヴューすることとされており、NSA が作成する統合シギント計画に対する関与が明文化された。（但し、その関与の詳細は不明である。）

---

[47] US NSA, *60 Years*, 16-22, 29-35.

[48] US NSCID No.6（国家安全保障会議インテリジェンス指令第 6 号）, “Signals Intelligence.”17 February 1972, https://www.nsa.gov/about/cryptologic_heritage/60th/interactive_timeline/Content/1970s/documents/19720217_1970_Doc_3984040_NSCID6.pdf

この後、シギントの活動領域は拡大し、1974 年にはキッシンジャー国務長官（当時）の海外暗殺計画を未然に探知した他、1970 年代は、テロ関連の誘拐、暗殺、ハイジャック対策への関与が増大し、その情報は掛け替えがないものとなったという。

また、1980 年代には、薬物対策が重要となり、米国への密輸入の防止のための諜報にも力を入れるようになった[49]。

なお、1981 年制定の大統領命令 12333 号では、NSA 予算を含む国家対外諜報計画（当時）の予算に関して、中央諜報長官は、予算を「開発」し、予算を大統領と連邦議会に提出するとされているが、予算を「決定」する権限は記載されていない。また、同予算については国家安全保障会議の審査と大統領による修正に従うとされている。NSA 予算に対して、国防総省との関係では大統領府の権限が拡大しているのは明白であるが、中央情報長官に決定権があるとまでは言えない状況であった[50]。

（３） 現在

CSS 附置後も、NSA には諸々の発展があり、ナショナル・インテリジェンスの色彩を強めてきたが、2001 年の９/１１テロ事件を契機に、2004 年に「インテリジェンス改革・テロ防止法」が制定され、国家諜報長官職が新設されるなど、諜報コミュニティの組織が大幅に改編された。これに伴い、NSA に限らず、米国の主要諜報機関は国家諜報機関としての性格が強化されたが、特に NSA の国家諜報機関としての構造は、ほぼ完成形になったと言える。

① 任務付与（Tasking）：国家安全保障法[51]中に、国家諜報長官が、諜報コミュニティの目標と優先順位を定めると共に、ナショナル・インテリジェンスの情報要求と優先順位を決定し、収集分析作成配布のタスキング（任務付与）を指揮すると明確に規定された。（102A 条(f)）

② 情報配布：NSA は、シギントの収集、処理、分析、作成、配布の任務が規定された[52]。配布対象は、諜報コミュニティ内の組織と人であるが、その手続は、国家諜報長官が国防長官と調整の上で司法長官の承認を得て定めることとされている[53]。当然、政府要人には必要情報が提供されている。

③ 人事：NSA 長官は、上院の承認を得て、大統領が任命することとなった[54]。

---

49 US NSA, *60 Years*, 55, 73.
50 US EO 12333 of 4 December 1981, Sec. 1.5 (n), Sec. 3.4(g) 参照
51 US National Security Act of 1947, amended through August 2007.
52 US EO 12333, amended through 2008, Sec.1.7(c).
53 US EO 12333, amended through 2008, Sec. 2, 3.
54 US National Security Agency Act of 1959, amended through 2014, Sec.2

大統領による任命の前には、所管の国防長官が推薦するが、それには国家諜報長官の同意が必要とされた。（102 条、106 条（ｂ））

④ 予算：NSA 予算を含む国家諜報計画予算に関して、国家諜報長官は、作成の指針を提示し、作成し、決定し、大統領に提出すると明示された。（102A 条（ｃ））

第２部　ＮＳＡの戦略、収集態勢と活動

第１章　ＮＳＡの戦略

１　シギント戦略

（１）2013 会計年度・国家諜報計画の前文

スノーデン資料の中で、現在の NSA のシギント戦略が明示されている文書に、2012 年 2 月の 2013 会計年度・国家諜報計画予算案の説明文書[1]がある。これは、国家諜報長官が連邦議会に対して国家諜報計画予算案を説明した機密文書であり、その前文には国家諜報長官の陳述が付されている。

国家諜報長官は、その前文（陳述）の冒頭で、「諜報コミュニティは、国家の安全確保にとって決定的に重要である。」「米国の政策決定者、軍、法執行諸組織、同盟諸国に対して最良のインテリジェンス支援を提供することによって米国の安全を守ることが、我々の最高の優先事項であり、・・・諜報コミュニティは、技術と創造性において世界最高のインテリジェンス能力を保持し続ける。」と述べた上で、前文を「インテリジェンスは国家防衛の第一線である。」として締めくくっている。

また、同前文では、2013 会計年度予算案では、予算削減の必要性から諸々の予算削減策を提示しているが、同時に投資すべき六項目中の最初の二つに NSA 関係予算を挙げており、米国インテリジェンスに於けるシギントの重要性の増大が顕著に現れている。即ち、投資すべき二つの分野は、次の通り[2]。

① シギント：　外国の指導者[3]を含む高優先度の目標に対する秘匿シギント収集能力を強化する。また、敵対者の秘匿暗号に勝利してインターネット通信から情報を得るための能力を飛躍的に向上させる。

② サイバー・セキュリティ：　サイバー脅威の増大に対応して「包括的国家サイバー・セキュリティ対策(Comprehensive National Cybersecurity Initiative) 」予算を維持すると共に、サイバー処理需要の増大に対応してフォート・ミード（NSA 本

1　ス資料 *FY 2013 Congressional Budget Justification Vol. I , National Intelligence Program Summary,*　February 2012,　accessed 19 September 2014, http://fas.org/irp/budget/nip-fy2013.pdf.

2 *National Intelligence Program Summary,*　2.

なお、投資項目の第３は、防諜であるが、監視及び攻撃的防諜対象として例示されているのは、中国、ロシア、イラン、イスラエル、パキスタン、キューバ（例示の順）である。また、投資項目の第５は、弾道ミサイルの情報収集であるが、対象国として例示されているのは、北朝鮮、イラン、中国、ロシア、パキスタン（例示の順）である。

3　後述するように、漏洩した NSA 内部資料により、NSA がアンゲラ・メルケル独首相を初め（友好国を含む）世界の政治指導者を情報収集標的としていたことが明らかとなったが、国家諜報長官が提出する国家諜報計画前文にその旨が明記されていたことは注目に値する。

部所在地）に二つ目の高性能のコンピュータセンターの建設を開始する。

（２）シギント戦略 2012 年～2016 年

更に、NSA の戦略をより詳細に記載しているのは、同じく 2012 年 2 月の「シギント戦略（2012～2016 年）」[4]である。これは、2012 年から５年間を俯瞰した NSA のシギント戦略文書である。同文書では、NSA が重要と考える諸点が記載されているが、これは、これから具体的に NSA のシギント収集態勢を見ていく上で、その背景にある考え方が分かる文書である。その中でも、重要と考えられるものを抜粋して要約すれば、次の通りである。

① ビジョン～米国の国家安全保障を全方面に亘って推進するに於いて、決定的な優位をシギントが提供することを確実にする。

② 任務～シギントの優位を通じて、我々の敵対者の秘密にアクセスして解読して、国家を守る。

③ 状況認識

○ シギントは、数十年間に亘り、諸々の敵対者に深く粘り強くアクセスすることによって、歴代大統領、軍司令官、政策立案者そして秘密任務の政府職員に情報を提供し、彼らの行動と意思決定を導いてきた。世界は変化し、全世界的な相互依存と情報時代の到来によって、我々の対象とする空間の性格は変容したが、我々はこれに革新的且つ創造的に対応し、現在は「シギントの黄金時代」であると評価される迄に至った。

（註：スノーデン資料に基づく報道[5]によれば、米大統領に対する毎朝の定例情報報告、即ち大統領が知るべき最重要情報の情報源の過半数は、シギントであるとされる。）

○ この評価の背景には大変な努力があったのであるが、これを維持するには、シギントの戦闘空間を形作り続けるダイナミックな且つ加速度的に市場の影響を受ける諸要因を把握していなければならない。そして、資料源の発見、アクセス、収集、分析、協力関係等に於いて、我々がその環境（註：即ち、サイバー空間）を支配するように事前に先手を打って行動しなければならない。

○ シギントの任務空間は、これから何年間にも亘り、急速に拡大し続けるであろう。

○ ユビキタス・コンピューティング（コンピュータ環境の普遍化）は、人々を情報源と通信手段の制約から解放し、人々の相互交流の在り方を根本的に変革するであ

---

[4] ス資料 *SIGINT Strategy: 2012-2016*, 23 February 2012, accessed 19 September 2014, http://www.documentcloud.org/documents/838324-2012-2016-sigint-strategy-23-feb-12.html

[5] Scott Shane, “No Morsel Too Minuscule for All-Consuming N.S.A.,” *The New York Times*, 2 November 2013, accessed 26 September 2014, http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html

ろう。そして、世界のサイバー空間で人々が相互交流する際に残す痕跡が、対象を探知し分析し理解する能力を規定するであろう。

○　サイバー攻撃は、潜在的敵対者に対して、米国の圧倒的に優勢な通常戦力に対抗する手段、しかも発見し追跡することが極めて困難な方法で対抗する手段を提供している。サイバー攻撃は、核攻撃のような大量の死傷者は出さないかも知れないが、核攻撃と同様に米国社会を麻痺させる力がある。

④ 2012～2016 年のシギント達成目標

上記の状況認識等を踏まえて、五つの目標を設定しているが、特に次の三つが重要である。

④－①　分析に大変革を起こす。即ち、情報ユーザーと協力者の参加を得て、情報の作成から情報の探知へと重点を変革する。

○　シギント技術の向上と自動化を進めて、世界ネットワークに対する支配を劇的に拡大する（dramatically increase mastery of the global network）[6]。

○　情報時代に於いて如何に人々が交流するか、その有様を反映する情報空間を分析する。

○　データを早期に配布し、大量データを共有し、ユーザー自身がユーザー特有のニッチな分析需要に対応できるようにする。

④－②　NSA 内外の協力関係を最大限に活用して、標的を発見し、それらの弱点を探知し、それらのネットワークと通信の防御に打ち克つ。

○　最重要な暗号解読の挑戦に対して、使用できる武器を強化する。

・　暗号解読を可能とするため、通信中間点及び端末に対する能力も統合活用して、多面的に能力を活用する[7]。

・　普遍的、高強度な商業ネットワーク暗号の挑戦に対抗する。

・　各国独自の暗号計画に対して、それぞれの産業基盤を対象に、全ての利用可能なシギントとヒューミントの能力を活用して対抗する[8]。

・　世界的な商業暗号市場に対しては、商業的関係、ヒューミント、そしてセカンド・パーティ、サード・パーティの協力諸国を通じて、影響を与える[9]。

6　正に、NSA は世界ネットワーク支配を目指しており、それは今後の収集態勢等の記述で明らかであろう。また、ここで「分析の自動化」を挙げているのが注目される。サイバー空間においては、NSA の入手可能なデータ量が余りにも膨大であって、人力に頼った分析では対処しきれず、価値あるデータの探知分析の自動化に力点をおいていることが明らかにされている。

7　暗号解読において、単にスーパーコンピュータを利用する様な一面的な取組ではなく、通信中間点に於けるデータ収集、或いはコンピュータ端末からの直接データ収集など、多面的な方法を組み合わせて、総合的に当たるべきことを記載している。

8 ここでも、諸外国の暗号計画に対抗するに当たり、ヒューミントの活用が明記されており、この収集においては、当然のことながら、CIA 等の協力、或いは CIA 等との共同作戦が想定される。

9　後述するが、暗号の国際基準で、2006 年に米連邦機関（US Institute of Standards and

・　国家の卓越した暗号解読能力を維持するため、継続して、高性能コンピュータのための産業基盤に対して投資をし、芸術の域にある技術を推進する[10]。

○　必要なシギント・データを、誰からでも、何時でも、何処からでも獲得する（in order to acquire the SIGINT data we need from anyone, anytime, anywhere）ため、敵対者のサイバー・セキュリティ施策を打ち負かす。

○　任務遂行に重要な標的とする人物、ネットワーク、アクセス、信号そして技術を探知するために、データ収集アーキテクチャに於ける探知能力と高度な技術を可能とする。

④－③　資料源開拓、サイバー防衛とサイバー作戦（攻撃）[11]の諸観点から、従来アクセスできていない標的に到達するため、端末や通信中間点に於けるデータ収集、民間協力、暗号解読能力を統合して対処する。

○　（サイバー侵入や攻撃を）探知し、反応し、警告を発するため、シギント・システムとセンサーの国家ネットワークを統合する[12]。

（３）「宝地図」（トレジャー・マップ）

シギントは、元々インテリジェンスの主要分野であったが、近年、その重要性が益々増大し、上記のように、現在は「シギントの黄金時代」と言われる迄になった。米国は、シギントに対して長きに亘り膨大な費用と人材を注ぎ込んできたが、国家諜報長官名の前文にもあるように、シギントをインテリジェンスの主正面として更に資源を注ぎ込もうとしている。

そこで目指すものは、「世界ネットワーク（インターネット等）に対する支配を劇的に拡大」して、「必要なシギント・データを、誰からでも、何時でも、何処からでも獲得」できる態勢の構築である。

これが、単なる夢や理想ではなく、実現目標であることは、後述するシギント・プラットフォームの実態を見れば分かるが、ここでは、傍証として、NSA の「宝地図」システムをその内部説明用パワーポイント[13]を基に紹介しておきたい。

NSA の「宝地図」システムは、端末機器を含むインターネットの世界地図を作成し

Technology）が制定し、後に国際基準に採用されたものは、実は NSA が働き掛けて、秘密の弱点を挿入させたものであると報道されている。

[10] コンピュータは、開発当初から暗号解読に活用されていたのであり、高性能コンピュータの開発と暗号解読との密接な関係は良く知られている。

[11] サイバー（コンピュータ・ネットワーク）作戦には、通常、資料源開拓（CNE）、防禦（CND）、攻撃（CNA）の三者が含まれるが、ここでいうサイバー作戦は、資料源開拓、防禦と併置されているので、サイバー攻撃を指していると解釈できる。

[12] この項目を見ても、サイバー攻撃計画では、国家シギント組織が中心的に関与する必要があることが分かる。

[13]　ス資料　US NSA, NOTC, “Bad guys are everywhere, good guys are somewhere!” undated, accessed 22 September 2014, http://www.spiegel.de/media/media-34757.pdf

利用しようとするもので、世界中のインターネット通信網の構造についての膨大な情報を集めて相関地図をニア・リアルタイムで作成し、その探索と分析を可能とするエンジン（謂わば、インターネットのグーグル・マップ）である。このため、このシステムは、世界地図の情報レイアーの上に、光ケーブル通信回線などの物理的ネットワークの情報レイアー、その上に、論理的ネットワークの情報レイアー、即ちインターネット網を構成する「自律システム（インターネット事業者や企業内の自律的ネットワーク）」やルーターなどの論理的ネットワークの情報レイアー等を設定し、更に、パソコンやスマートフォン等の端末機器の情報レイアー、その利用者の情報レイアーを設定表示する。地図作成に必要な膨大な情報は、日々、一般公開情報や研究機関の情報、商業的購入、更にシギント活動によって取得している[14]。

このシステムを使用することにより、味方や敵対者のネットワークの現況を把握し、各種ネットワークを偵察し、サイバー攻撃にもデータ収集の計画にも利用できる。それのみならず、このシステムでは、NSA が既にアクセスできる「自律システム」を表示するようにもなっている[15]。

14　「宝地図」のためには種々のシギント活動からの収集データが利用されているが、その一例として「宝地図」パワーポイントに記載されているものに、世界中のデータセンターへの秘匿サーバー（PackegedGoods）の設置がある。秘匿サーバーの設置場所として示されている諸国は次の通り。

アジア地区：マレーシア、シンガポール、台湾、中国２箇所、インドネシア、タイ、インド
欧州ロシア地区：　ポーランド、ロシア、ドイツ、ウクライナ、ラトビア、デンマーク
アフリカ地区：　南アフリカ
南米地区：　アルゼンチン、ブラジル

なお、次の分析報道によれば、NSA はこれら１６の秘密サーバーから、「MoreCowBell」計画と呼ばれるデータ収集を行っている。即ち、インターネットでは、DNS（Domain Name System）サーバーがドメイン名を含むアドレスとＩＰアドレスとの対応関係を管理しているが、秘密サーバーから世界中の DNS サーバーに対して膨大な接続要求を 1 日 24 時間継続的に出して、アドレスの存否を把握或は確認しているという。この接続要求に使用するアドレスは、NSA が既に各種ウェブサーバーやＥメールや各種データベース等から収集したアドレスを元に可能性のあるものを自動的に作成しているという。これによって、世界中のアドレス情報をＩＰアドレスとの対応関係と共に収集している。収集データは、15 分から 30 分間隔で NSA 本部に送信され、本部のデータベースを更新しているという。
--Jacob Applebaum, Monika Ermert, Laura Poitras and Matthias Wachs, “MoreCowBells: New revelations about the NSA’s practices,” *Le Monde*, 24 January 2015, accessed 26 January 2015,
https://translate.google.com/translate?hl=en&sl=fr&tl=en&u=http%3A%2F%2Fwww.lemonde.fr%2Feconomie%2Fvisuel%2F2015%2F01%2F24%2Fcowbells-nouvelles-revelations-sur-les-pratiques-de-la-nsa_4561547_3234.html&sandbox=1

15　独誌シュピーゲルの報道によれば、ドイツ関係では、ドイツ最大の事業者であるドイツテレコム（インターネットの世界では、世界で十数社しかない最上級「ティア１」の大規模事業者の一つ）や地域の小規模事業者も、そのネットワークが NSA からアクセス可能となっている。
--Andy Mueller-Maguhn, et. al., “The NSA Breach of Telkom and Other German firms,” *Spiegel Online,* 14 September 2014, accessed 16 September 2014,

このようなシステムは、「必要なシギント・データを、誰からでも、何時でも、何処からでも獲得」するには不可欠のシステムであろう。

前NSA長官のケース・アレクサンダーのモットーは、「全て収集しろ（Collect it all）」であったというが、NSA自体も「全て収集しろ」をその方針としており[16]、正にそのような方針が反映しているシステムである。

２　戦略的任務リスト

スノーデン資料には、2007年１月現在の「戦略的任務リスト」がある[17]。これは、米国シギント体制にとって戦略的に重要な諜報対象（標的）を列挙したものである。これは、諜報コミュニティ国家諜報優先事項機構（Intelligence Community National Intelligence Priority Framework）の検討等を基礎にして、シギントの作業グループが半年毎に策定更新する文書であり、策定時点から12ヶ月乃至18ヶ月間の任務の優先順位を定めるものとされる。

本内部資料は、2007年１月時点のものであるので、現在の任務リストは相当変化していると考えられる。しかし、これが現在入手可能な最新リストであり、且つそこで示されている任務設定の基本思想は現在でも有効であると考えられるので、ここにその骨子を紹介して、シギントに付与された任務を理解する資としたい。

リストは、２部から構成され、第１部は分野別の優先目標１６を規定し、第２部はその戦略的重要性から全体的且つ継続的に標的とすべき国６つを挙げている。

（１）任務分野

必ず収集する重要標的を、優先順に記載している。

① テロ情報（テロに対する世界的戦争に勝利する）

米国、米国権益及び同盟国を攻撃する能力と意図を有する特定テロ集団、及び米国権益攻撃を計画実行しているテロ集団

（註：当然のことながら、テロ対策が米国シギント・システムの第１の優先任務に挙げられているのが、注目される。）

② 米国国土安全保障

---

http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html.

[16] Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014)、95-97.

[17] ス資料 *United States SIGINT System: January 2007 Strategic Mission List,* accessed 6 November 2013,
http://www.nytimes.com/interactive/2013/11/02/world/documents-show-nsa-efforts-to-spy-on-both-enmies-and-allies/...

国境警備、テロ攻撃からの直接防御、病気・伝染病・世界的伝染病、大統領等の幹部警護等

③　大量破壊兵器と生物化学核放射性物質の計画と拡散

- 生物化学核放射性物質の開発、取得、使用
- 大量破壊兵器と弾道・巡航ミサイルに関する国家計画
  （対象国：中国、インド、イラン、北朝鮮、パキスタン、ロシア、シリア）
- 大量破壊兵器とミサイルの拡散
  （対象国：中国、イスラエル、北朝鮮、パキスタン、ロシア）
- 大量破壊兵器とミサイルの取得
  （対象国：中国、インド、イラン、パキスタン、サウジアラビア）
- 大量破壊兵器の保管管理　（対象国：パキスタン、ロシア）

④　海外展開中の米軍の安全と作戦支援

⑤　国家の安定及び政治的安定

- イラク、アフガニスタン、パキスタン、サウジアラビア～米国が体制継続に利益を有する国々での指導部存続の脅威となり得る国内政治活動
- 北朝鮮、スーダン、キューバ、コソボ、トルコ、ナイジェリア、レバノン、ベネズエラ、シリア、ボリビア、パレスチナ等の危機となり得る国内政治活動

⑥　戦略的核ミサイル脅威に関する警告情報

ロシア、中国、北朝鮮三カ国の核戦力が具体的に指定されている。

⑦　地域紛争・危機と戦争発火点（紛争や危機に拡大し得る地域的緊張）

アラブ・イラン対イスラエル紛争、朝鮮半島、中国対台湾、インド対パキスタン、ベネゼエラ､ロシア対グルジア～～米国の戦略的利益に相当の脅威となり得る地域的発火点[18]

⑧　情報作戦（サイバー空間の支配と米国の重要情報システムへの攻撃防止）[19]

- コンピュータ・ネットワーク防禦支援
- コンピュータ・ネットワーク攻撃支援
- 外国諜報諸機関によるサイバー脅威活動対処

（対象として、中国、ロシア、イラン、アルカイダが列挙されている。）

- 電子戦支援（対象として、中国、ロシア、イラン、北朝鮮に加えて、イラクとアフガニスタンでの手製爆弾が列挙されている。）
- 影響力作戦（Influence Operations）支援～～軍による欺瞞作戦や宣伝作戦等を

---

[18] 筆者は、現在は、尖閣列島問題や東シナ海の南沙諸島問題も掲載されているのではないかと考えている。

[19] 現在は、サイバー攻撃やサイバー防衛の重要度が増しており、この情報作戦の分野は、この文書が作成された 2007 年時点より更に優先順位上位に位置付けられていると推定される。

支援する[20]。（対象として、テロ組織、中国、北朝鮮、イラン、ベネズエラが列挙されている。）

⑨　軍近代化（外国の軍の近代化計画を早期に把握する）

- 中国、北朝鮮、ロシア、イラン、シリアの軍近代化計画
- 中国、ロシアによる衛星システム及び衛星攻撃システム

⑩　戦略的科学技術（軍事、経済、政治面で戦略的優位となりうる重要科学技術～～高低エネルギー・レーザー、コンピュータ・情報技術の進展、指向性エネルギー兵器、ステルス・反ステルス技術、電子戦技術、宇宙観測・遠隔観測技術、電子光学、ナノテクノロジー、エネルギー物質）

対象国として、ロシア、中国、インド、日本、ドイツ、フランス、韓国、イスラエル、シンガポール、スウェーデンが列挙されている。

⑪　外交政策（米国の外交的優位を確保する）

対象国として、中国、ロシア、フランス、ドイツ、日本[21]、イラン、イスラエル、サウジアラビア、北朝鮮、アフガニスタン、イラク、国連、ベネズエラ、シリア、トルコ、メキシコ、韓国、インド、パキスタンが列挙されている。

⑫　エネルギー安全保障

対象国として、イラク、サウジアラビア、ベネズエラ、イラン、ロシア、ナイジェリアが列挙されている。

⑬　米国に対する諜報、防諜、欺瞞・心理活動

対象国として、中国、ロシア、キューバ、イスラエル、イラン、パキスタン、北朝鮮、フランス、ベネズエラ、韓国が列挙されている[22]。

⑭　薬物と国際的な犯罪組織とネットワーク（麻薬密輸組織や国際犯罪シンジケート等による米国益に対する影響を軽減する。）[23]

- アフガニスタン、メキシコ、コロンビアの薬物密輸組織
- ロシアの国際犯罪シンジケート
- コロンビア、メキシコ関係の犯罪収益の洗浄

---

[20] 2007年時点では、影響力作戦は、未だNSA自体の任務ではなく、軍に対する支援任務であったようであるが、後述するように現在、英国GCHQではオンライン秘匿活動の一環として相当重要な任務となっている。米国NSAでも、現在は本体任務となっていると推定される。

[21] 日本の優先順位の位置付けが、科学技術開発では独仏より上位であるが、外交政策では独仏の下位に置かれている。米国にとっての日本の評価が反映されていると言えよう。現在の順位付けがどうなっているか、関心が持たれるところである。なお、国連も対象とされており、これがNSAによる国連の情報システムへの浸透の背景であろう。

[22] 米国の同盟国或いは実質的同盟国の中で、イスラエル、フランス、韓国が記載されているのが注目される。これら諸国は、それだけ積極的な対米諜報活動を行っているとの、米国による評価が示されている。

[23] 犯罪情報自体が重要標的となっているのが注目される。公然化はしていないものの、シギントを端緒とする犯罪検挙も相当なものとなっていると推定される。

○　イラン、北朝鮮の国家的マネー洗浄

⑮　経済的安定と影響力（米国の経済的優位と政策戦略を確保する。）

対象国として、中国、日本、イラク、ブラジルが列挙されている。[24]

⑯　世界の信号状況の認識（中核的通信インフラ及び世界的ネットワークに関する情報）

軍事・非軍事の通信インフラについてその位置、性格、使用状況、現状に関する知識を獲得する。重点として、世界的な（信号や通信）環境の知識、信号状況に関する知識、ネットワークに関する知識、標的に関する知識が列挙されている。

以上、重要標的分野の骨格を紹介した。いくつかの分野で日本が諜報対象として掲載されている。これに対し、同盟国を諜報対象にすることに反発を感じる者もいるであろうが、公式見解は如何なるものであれ、諜報の世界では同盟国・友好国であろうとも諜報対象となることは常識である。

例えば、オバマ大統領はスノーデンによる告発のあった後の 2013 年 7 月 1 日には次のように発言している。即ち、「諜報機関というものは全て、米国だけでなく、欧州諸国でもアジア諸国でも諜報機関が存在する限り、世界をもっと理解しよう、各国の首都で何が起きているかを理解しようとしている。それをしないようであれば、諜報機関としての価値はない。」[25]　また、オバマ大統領は、2014 年 1 月 17 日には次のようにも演説している。即ち、「米国の歴史を通じて、インテリジェンスは米国と自由を守ることに貢献してきた。・・・我々の諜報機関を一方的に武装解除する訳にはいかない。」[26]

なお、標的としての日本の位置付けを見ると、2007 年時点では相当高い優先順位が与えられていたことが分かる。それは当時の日本の国力・重要性を反映したものであろう。寧ろ、現在の日本の位置付けが案じられるところである。

---

[24]　米国の公式見解では、中国は産業的利益のために直截なスパイ活動をするが、米国はこれと異なり、米国企業のための産業スパイはしていないと主張している。本件に関する元 NSA 長官マイケル・ヘイデン氏のインタヴューは次の通り。

--Michael Hayden, interview by Marc Hujer and Holger Stark, *Spiegel Online,* 24 March 2014, accessed 31 March 2014,
http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389.html

[25] Dan Roberts, "Obama tries to ease NSA tensions and insists: Europe spies on US too," *The Guardian*, 1 July 2013, accessed 24 September 2014,
http://www.theguardian.com/world/2013/jul/01/obama-europe-monitoring-data-surveillance

[26] "Through American history, intelligence has helped secure our country and freedom. We cannot unilaterally disarm our intelligence agencies."

--"Transcript of President Obama's Jan. 17 speech on NSA reforms," *The Washington Post,* 17 January 2014, Accessed 24 September 2014,
http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html

（２）継続的標的国

継続的標的国として次の６カ国が列挙され、それぞれについて更に詳細な諜報関心が規定されている。

① 中国、②北朝鮮、③イラク、④イラン、⑤ロシア、⑥ベネズエラ

中国が標的としての優先順位第１位であるのは理解し易いが、ベネズエラがわざわざ提示されていることが注目される。2007 年当時のベネズエラはチャベス大統領に率いられており、米国の裏庭たるラテンアメリカの反米政権が米国からどう評価されていたかが分かる。

３　セカンド・パーティ、サード・パーティ、多国間協力

NSA のシギント戦略において不可欠なものが関係国との協力関係である。インターネットを支配すると言っても、NSA 単独では実現不可能であり、同盟諸国等との協力関係が重要である。この点で最も重要なのが、セカンド・パーティ諸国との特殊な協力関係である。その他にも、NSA はサード・パーティという位置付けの諸国と協力関係を築いている。

（１）セカンド・パーティ

米国は、シギントに於いて、英国、カナダ、オーストラリア及びニュージーランドと、特殊な、即ち密接且つ恒常的な協力関係を結んでおり、英国等の４カ国をセカンド・パーティと呼んでいる。

この協力関係は、第二次世界大戦中の米英のシギント協力に起源を持つが、大戦が終結しても協力関係は停止されることなく恒常化された。最初 1946 年に BRUSA 協定という秘密協定が米英間で締結されたが、これが米国のシギント組織改編等を受け 1952 年に UKUSA 協定に改定された。これら協定自体は米英二カ国による協定であるが、英連邦諸国の参加を前提としており、参加国は大戦中の経緯からカナダ、オーストラリア、ニュージーランドの三カ国とされた[27]。

セカンド・パーティのシギント諸機関は、現在、英政府通信本部（Government Communications Headquarters: GCHQ）、加通信保全局（Communications Security Establishment :CSE）、豪信号局（Australian Signals Directorate:ASD）、ＮＺ政府通信保全局（Government Communications Security Bureau: GCSB）である。

---

[27] これらの経緯は、次の NSA の開示情報に示されている。
US NSA/SCC, *UKUSA Agreement Release　1940-1956,* accessed 25 September 2014, https://www.nsa.gov/public_info/declass/ukusa.shtml
なお、UKUSA 枠組での実際の協力関係の開始は、カナダは 1949 年、豪州とニュージーランドは 1956 年とされる。

米国とこれら４カ国のシギント機関は、NSA の部内資料では「五つの眼」（Five Eyes，FVEY）と示されることが多いが、今回スノーデンにより漏洩された一連の内部資料を見ると、その協力関係は極めて密接であり、単なる情報交換というようなレベルではなく、共同の収集分析、或いは NSA の資金提供による共同のシステム構築などにも及んでいる。（少なくとも NSA の側から見れば）統合運用と言えるレベルの協力関係といえるであろう。この協力関係の調整のため、NSA との間ではリエゾン代表者を相互の本部に派遣常駐させている。

この関係があるため、NSA はセカンド・パーティの地理的優位性等を活用して、世界を覆うシギント・システムを構築することが可能となり、他方、他の四ヵ国は自国だけでは到底入手することのできない豊富な且つ正確な情報を入手できることとなる。世にいわゆる米英特殊関係というのも、その基礎は間違いなくこのシギント協力にあると思われる。英国の国力に UKUSA 協定関係から得られるシギント力が大きく貢献しているのは疑いがない事実であろう[28]。

なお、これら５カ国間では、お互いにはスパイ活動はしないという紳士協定があると言われている。他方、それぞれのシギント機関は、民主主義国家の対外シギント機関として、自国内での自国民に対する諜報活動は基本的にはできないこととされているが、自組織ではできない自国民の情報収集をセカンド・パーティ国に依頼して脱法的に情報収集を行うことがあるとも言われている[29]。

（２）サード・パーティ

サード・パーティは、NSA が個別に協力関係を持っている諸国である。協力関係の内容や親密度はそれぞれの国によって異なっている。NSA にとっては、標的にアクセスするための地理的な利点、当該国の特定シギント分野での専門性、或いは地理的分析力などを入手することができ、他方、サード・パーティ諸国にとっては米国の技術資金或いは提供されるシギント情報に価値があると見られる。

2013 会計年度において米国内で承認されたサード・パーティ諸国は、NSA 内部資料によれば次の３３ヶ国である[30]。

（欧州）　独、仏、伊、西、蘭、ベルギー、デンマーク、ノルウェー、スウェーデン、フィンランド、オーストリア、ポーランド、チョコ、ハンガリー、クロアチア、ギ

28　英国の諜報体制が議論される際には、その合同情報委員会がスタッフが少人数であるにも拘わらず良く機能しているとしばしば注目される。しかし、それが機能する前提として、この UKUSA 関係による正確多量なシギント情報の存在が理解されているのか疑問である。

29　但し、NSA は、他国機関を使った米国民に対する情報収集はしていないと主張している。参照、US NSA, *The National Security Agency: Missions, Authorities, Oversight and Partnerships,* 9 August 2013, 6, accessed 28 September 2014, https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf

30 Greenwald, *No Place,* 123.

リシャ、マケドニア、ルーマニア

（アジア）　シンガポール、韓国、タイ、インド、日本、台湾、パキスタン[31]

（中東・アフリカ）　イスラエル、トルコ、ヨルダン、サウジアラビア、アラブ首長国連邦、アルジェリア、チュニジア、エチオピア

（３）多国間協力枠組

セカンド・パーティ、サード・パーティの協力枠組の他に、これら諸国の内の一部で構成する多国間協力、或いは国際組織との協力の枠組がある。2013 年度時点では次の４つが挙げられている[32]。

○　AFSC（アフガン・シギント連合）：アフガニスタンに関連するシギント協力のための組織。参加国は下記 SSEUR と同一。参加各国が任務分担をして、それぞれが作成したシギント情報報告と収集した通信メタデータ（後述）を共有している[33]。

○　NATO（北大西洋条約機構）（註：協力関係が、加盟国全体に及ぶのか、機構自体に留まるのか不明）

○　SSEUR（欧州シギント首脳会議）：UKUSA 諸国の他、９ヶ国の欧州諸国が参加している。９ヶ国は、独、仏、西、伊、蘭、ベルギー、デンマーク、ノルウェー、スウェーデン。

SSEUR は、1982 年、当時のソ連に対するシギント活動の効率化のために開始された協力枠組であり、SIGDASYS（Sigint Data System）と呼ばれる一定のシギント・データ共有のためのシステムを構築していたという。そして、このシステムは 1990 年から 91 年の湾岸戦争で効果を発揮したとされる[34]。現在でも、この SIGDASYS は運用されている[35]。

---

[31] 下記分析に引用されている NSA 内部資料によれば、アジアに於ける「サード・パーティ」中の主要国は、シンガポールと韓国とされる。
--"Five Eyes, 9-Eyes and many more," *Top Level Telecommunication*, 15 November 2013, updated 22 January 2014, accessed 13 February 2015, http://electrospaces.blogspot.nl/2013/11/five-eyes-9-eyes-and-many-more.html

[32] "NSA's Foreign Partnership," *Top Level Telecommunications*, 4 September 2014, accessed 4 September 2014, http://electrospaces.blogspot.jp/2014/09/nsas-foreign-partnerships.html

[33] ス資料、NSA, *NSA Intelligence Relationship with Germany-Bundesnachrichtendienst,* 17 January 2013, accessed 20 June 2014, http://www.spiegel.de/media/media-34053.pdf

[34] "14-Eyes are 3rd Party partners forming the SIGINT Seniors Europe," *Top Level Telecommunications,* 15 December 2013, accessed 23 March 2015, http://electrospaces.blogspot.jp/2013/12/14-eyes-are-3rd-party-partners-forming.html

[35] ス資料、NSA, *Talking Point Topics Proposed,* (circa April 2013) , accessed 20 June 2014, http://www.spiegel.de/media/media-34119.pdf. なお、2013 年２月に米国のＩＴセキュリティ会社マンディアントが発表した中国のシギント部隊に関する報告書は、このシステムを使って関係機関には NSA から事前配布されていたとされる。

また現在、SSEUR にはテロ対策連合（CT coalition）というテロ対策の下部組織が設置され、半年毎に協議会合が開催されている[36]。

○　SSPAC（太平洋シギント首脳会議）：UKUSA 諸国の他、５ヶ国の欧州及びアジア諸国が参加している。５ヶ国は、韓国、シンガポール、タイ、仏、インド[37]。

協力枠組の目的と内容は不明である。

---

[36] ス資料、“ Secret document on the cooperation between the NSA, BND and BfV in the fight against terrorism,” *Spiegel Online*, 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/media/media-34046.pdf。テロ対策下部組織の略称は SISECT。

[37] ス資料 NSA、Foreign Affairs Directorate, *NSA　Intelligence Relationship with New Zealand,* (April 2013), accessed 12 March 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/1683920/nzodnipaperapr13-v1-0-pdf-redacted.pdf

第２章　収集態勢（シギント・プラットフォーム）

NSA は、そのシギント・プラットフォームによって膨大なデータを収集している[1]。2011 年 4 月の内部資料[2]によれば、その時点で NSA のシギントシステムは常時２ペタバイトという膨大なデータを保有しており、且つ 2011 年末には毎秒１テラバイトのデータを取得するようになる見込みであった。そして、シギント総局分析部長は「現在の収集態勢の質と量は､我々に最良のインテリジェンスを生産する空前の能力を付与している」と述べている。他方、分析官の間では、データ過多に溺れおり[3]、分析麻痺[4]に陥っているという声もある。そこで、現在の分析の課題は、膨大なデータの中から如何にして有効なデータを検索抽出するかとなっており、調査研究局には「情報過多対処室（Coping With Information Overload Office)」[5]が設置され、また、2013 年会計年度の予算には「情報過多対処」予算として 4861 万ドルが計上されている程である[6]。

それでは、このように膨大なデータを収集している NSA のシギント・プラットフォームの全体像を見ていきたい。

１　収集態勢の概観

収集態勢について参考となるスノーデン資料二つあり、一つは、世界のシギント・プラットフォームを説明した資料、もう一つは、NSA の地方本部が情報化した資料源の分類資料である。

（１） 世界シギント・プラットフォーム[7]

---

[1] Peter Maass, “Inside NSA ; Officials Privately Criticize 'Collect It All' Surveillance," *The Intercept*, 28 May 2015, accessed 29 May 2015, https://firstlook.org/theintercept/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/

[2] ス資料、“Is There a Sustainable Ops Tempo in S2?　How Can Analysts Deal with the Flood of Collection?—An Interview,” *SID today*, 6 April 2011, accessed 4 June 2015, https://www.documentcloud.org/documents/2089125-analytic-modernization.html

[3] ス資料、"Op-de: Leave Bright Pebbles, Not Breadcrumbs, for Those Coming After You,” 24 September 2010,　accessed 4 June 2015, https://www.documentcloud.org/documents/2088974-drowning-in-information.html

[4] ス資料、”The SIGINT Philosopher: Too Many Choices,” 18 January 2011, accessed 4 June 2015, https://www.documentcloud.org/documents/2088983-too-many-choices.html

[5] ス資料、”Dealing With a ‘Tsunami’ of Intercept,” 29 August 2006, accessed　4 June 2015, https://www.documentcloud.org/documents/2088984-tsunami-of-intercept.html

[6] ス資料 *FY2013 Congressional Budget Justification Vol.　I : National Intelligence Program Summary*,　（February 2012）159,　accessed 20 August 2014, http://fas.org/irp/budget/nip-fy2013.pdf

[7] Greenwald, *No Place,* 117, 及び --“NSA’s global interception network,” *Top Level Telecommunications*, 3 December 2013,

本資料では、2012 年時点での NSA の世界の情報ネットワークへのアクセス源として、次の五つの手段が示されている。

① 通信基幹回線

約２０の計画により、世界中の主要ポイントで（関係者に秘匿して、或いは関係者の協力を得て）アクセスできるとしている。

② 外国通信衛星の傍受

主要基地１２箇所と SCS（特別収集サービス）４０箇所で収集しているとする。

③ 特別収集サービス（Special Collection Service: SCS）

NSA と CIA による共同作戦であり、世界の米国大使館や領事館８０箇所以上を収集拠点としている。

④ CNE（コンピュータ・ネットワーク資源開拓）

NSA 内のいわばハッカー技術者集団である TAO による収集であり、2012 年時点では世界中で５万箇所以上のシステムに浸透しているとしている（現在では１０万箇所近くと推定される）。

⑤ サード・パーティ

サード・パーティと呼ぶ協力国約３０カ国を収集拠点としている。（註：セカンド・パーティが記載されていないのは、セカンド・パーティとの協力関係が極めて密接で、実際上 NSA と一体化しているためと考えられる。）

但し、これらの事項には、今や有名になった「プリズム」計画（後述）や米国内電話通信のメタデータの収集手段（後述）は含まれておらず、本資料は、必ずしも NSA のシギント・プラットフォーム全体を網羅して記載したものではない。

（２）NSA 地方本部の資料源分類資料[8]

本資料では、2009 年 12 月時点で、NSA の地方本部の一つ（テキサス州サン・アントニオ所在）が情報化した資料源の収集アクセス別分類資料である。ここでの分類は網羅的であると推定できるが、提示されているアクセス源は、上記（１）と若干異なっている。即ち、②～⑤はほぼ同じ（但し、⑤はセカンド・パーティ/サード・パーティとなっている）であるが、上記①はなく、替りに次の四つが挙げられている。

⑥ SSO（Special Source Operation：特別資料源作戦）

民間企業の協力を得て行うデータ収集。

⑦ 対外諜報監視法 2008 年改正法に基づく収集

---

updated 17 July 2014, accessed 26 September 2014
http://electrospaces.blogspot.jp/2013/12/nsas-global-interception-network.html

[8] “Documents Show N.S.A. Efforts to Spy on Both Enemies and Allies,” *The New York Times,* 2 November 2013, accessed 6 November 2013,
http://www.nytimes.com/interactive/2013/11/03/world/documents-show-nsa-efforts-to-spy-on-both-enemies-and-allies.html?_r=0

電気通信事業者に対する協力命令に基づく収集。

⑧　シギント衛星・機上収集（Overhead）

シギント衛星（国家偵察局 NRO が打上）及びシギント航空機によるデータ収集

⑨　従来型収集（Conventional）

２０世紀にシギントの中心であった主として無線通信の傍受によるデータ収集

（３）推定全体像

上記の内、①と⑥⑦は重複する。即ち、①通信基幹回線からの収集の多くは、同時に民間企業の協力を得た⑥であり、また、その内の米国内での収集は⑥であると同時に⑦の対外諜報監視法による収集でもある。また、「プリズム」計画は、⑥であると同時に⑦でもある。つまり、⑥⑦はむしろ資料源自体というよりも資料源にアクセスするための手段を示したものである。

そこで、全資料源のうち主要なものを推定すると、次の八つが挙げられる。

①　「プリズム」計画
②　通信基幹回線
③　外国通信衛星の傍受
④　特別収集サービス（SCS）
⑤　CNE（コンピュータ・ネットワーク資源開拓）
⑥　セカンド・パーティとサード・パーティの協力国
⑦　シギント衛星・機上収集（Overhead）
⑧　従来型収集（Conventional）

本章では、上記の内、①から⑤について、それぞれ項目を立てて記述したい。

なお、⑦と⑧については、スノーデン資料（として報道されたもの）の中には、現在までのところ殆ど見られない。それは、これら二つがインターネット空間との関連性が相対的に低いためではないかと考えられる。そこで、本稿の分析対象外とする。また、⑥に関しては、前章で既述した通りであり、詳細については別途記述したいと考える。

各項目に移る前に、以下に SSO と対外諜報監視法 2008 年改正法について簡単に説明する。

（４） SSO（特別資料源作戦）[9]

NSA は、その任務中、攻撃（シギント）と防御（情報保証・サイバー防衛）の両面で主要な世界的企業からの協力を得ており、その数は８０社を超える。NSA の内部資料に会社名が挙げられているのは、マイクロソフト、インテル、IBM、オラクル、ベライゾン、ATT、シスコ、モトローラ、ヒューレット・パッカード、その子会社の EDS、クアルコム、キューウエストの１２社である。業種も多彩であり、通信・ネットワーク

[9] Greenwald, *No Place,* 102.

提供事業者、ネットワーク・インフラ事業者、サーバーや端末機器企業、システム運用会社、セキュリティ会社、ソフトウェア企業等多岐に及んでいる。

このような民間企業との協力の内、NSA の攻撃面、即ちシギントの資料収集で協力を得る作業が、特別資料源作戦（Special Source Operation：SSO）と呼ばれており、スノーデンによれば、特別資料源作戦は NSA の「宝冠」(crown jewel)と言えるほど、極めて貴重な情報源であるとされる[10]。

特別資料源作戦も多岐に及び、スノーデン資料によっても現時点ではその全貌が明らかになっている訳ではない。報道された中で、特に注目を集めたのが、後述する「プリズム」計画と基幹通信回線へのアクセスである。

（５） 対外諜報監視法 2008 年改正法等[11]

ア　対外諜報監視法 702 条（対外諜報監視法 2008 年改正法）

前述したように、米国では、対外諜報は本来大統領の行政権限に属し、その実施に関して法律の根拠は要しない。しかしながら、この権限の度重なる濫用の結果、1978 年に対外諜報監視法が制定され、米国内の対象を標的として米国内で行われる対外諜報（電子的監視）に対して一定の制限が掛けられた。ところが、対外諜報監視法は、その後数度の改正によって、米国内で行う対外諜報活動（国外標的を含む）に関して民間事業者に協力義務を課すなど、権限規定の色彩が強まってきており、その典型が 2008 年改正法による 702 条である。

702 条では、司法長官と国家諜報長官は共同して、米国外に所在すると合理的に信じられる非米国人[12]を諜報の標的として認可(authorize)することができるとされているが、本条の主たる適用対象は、米国の電子通信事業者を利用する外国人の通信であり、上記の認可も個別標的毎ではなく包括的認可である。両長官がこの認可をするに当たっては、事前に、対外諜報監視裁判所に、対外諜報情報の収集目的、（米国人に関する情報を極力収集しないようにするための）「標的決定手順」と「最少化手順」[13]を提出し、

10　同上。

11　主な参考文献は次の通り。

--US NSA, *The National Security Agency: Mission, Authorities, Oversight and Partnerships,* 9 September 2013, accessed 28 September 2014, https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf

-- James G. McAdams, Ⅲ, *Foreign Intelligence Surveillance Act (FISA): An Overview,* (2009), accessed 28 September 2014, https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

12　非米国人とは、米国人（即ち、米国民又は米国永住権保有者）でない者と定義されている。50　USC　Sec.1801(i).

13　「標的決定手順」は、米国外に現在すると合理的に信じられる者のみを標的とし、且つ、通

裁判所の承認を得なければならない。その上で、両長官は電子通信事業者に対して協力命令を発することができ、事業者が協力しない場合には、対外諜報監視裁判所に要請して協力の強制命令の発布を受けることができる。他方、事業者は、両長官の協力命令に従った場合には、その協力に関して民事刑事の責任を問われることがない。

ここで注意すべき点は、第１に、これらの「標的決定手順」と「最少化手順」では、当然のことながら米国外にいる非米国人の保護は全く考慮されていないことである。第２に、これらの手順によっても米国人が当事者となる通信の収集は排除されないということである。法律では、「米国内にいる者を意図的に標的にしてはならない」「米国外にいる米国人を意図的に標的としてはならない」「送受信者の全てが米国内にいると知られている通信を意図的に取得してはならない」等[14]としているのみであり、米国外の非米国人を標的として情報収集を行った際、付随して米国人や米国内にいる者が当事者となる通信を収集することは、想定されている。そのために「最少化手順」が存在するのであるが、問題はその運用であり、実際上は、こうして収集される米国人のデータは相当量に及ぶと見られている[15]。

イ　対外諜報監視法 501 条（愛国者法 215 条）

なお、対外諜報監視法 702 条の他に、注目されている条文が同法 501 条（2001 年愛国者法 215 条による改正条文）である。本条文は、元来、国際テロ対策や非米国人に関する対外諜報等の目的ために、FBI が裁判官の令状を得て民間事業者の商業記録（ビジネス・レコード）の提出を求めることができるというものである。（民間事業者にはその提出に関し守秘義務が課せられている。）

後述するように、NSA はこの条文を根拠に FBI の協力を得て、米国内の大手電話事業者三社から米国内の通話メタデータを大量に、即ち三社分全てを入手していたのである。

信当事者が全て米国内に現在すると知られている場合は収集を行わないようにするために、諜報機関が実施すべき手順である。また、「最少化手順」とは、米国人に関する非公開情報の収集保持を最少化し、そしてその配布を禁止する手順である。但し、同手順は、米国人についても、犯罪の証拠となる情報の保持と配布は認めている。50 USC Sec. 1801(h), 1881a(d)(e).

14　50 USC Sec. 1881a(b).

15　上記註にも記載したように、そもそも、「最少化手順」自体が、米国人の犯罪情報の保持を認めるなど、米国人情報の排除の観点からして必ずしも厳格ではない。

２　「プリズム」計画

プリズム計画はNSAの各種情報収集プラットフォームの中でも極めて重要なものである。スノーデンにより、NSAの極秘パワーポイント説明資料(2013年4月付）全41枚が漏洩されており、これらの内約20枚がウェブ上で閲覧可能である。これらの内部資料と内部資料を基にした各種報道を基に分析をしてみると次の姿が浮かび上がる。

（１）プリズム計画の概要[16]

「プリズム計画」とは、NSA の宝冠と言われる「特別資料源作戦（SSO：Special Source Operation)」の一つであり、民間事業者の協力を得て行う作戦である。本計画では、米国のインターネット関連企業９社の協力を得て、これら企業のデータセンターからデータを広汎に収集している。

ア　参加企業

プリズム計画は２００７年当初から開始されたが、これに参加している米系インターネット関連企業の参加時期と企業名は、次の通り。

２００７年　９月　マイクロソフト
２００８年　３月　ヤフー
２００９年　１月　グーグル
２００９年　３月　フェイスブック
２００９年１２月　パルトーク
２０１０年　９月　ユーチューブ（グーグルの子会社）
２０１１年　２月　スカイプ（マイクロソフトの子会社）
２０１１年　３月　ＡＯＬ
２０１２年１０月　アップル

イ　取得可能データ

16　主な資料は、次の通り。
--"NSA slides explain the PRISM data-collection program," *The Washington Post*, 6 June 2013 undated 10 July 2013, accessed 16 July 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
--"What is known about NSA's PRISM program," *Top Level Telecommunications,* 23 April 2014, updated 16 September 2014, accessed 13 October 2014, http://electrospaces.blogspot.jp/2014_04_01_archive.html
--Greenwald, *No Place,* 109-116.
--"What if Google was an intelligence agency?" *Top Level Telecommunications,* 5 August 2014, updated 15 September 2014, accessed 13 October 2014, http://electrospaces.blogspot.jp/2014/08/what-if-google-was-intelligence-agency.html

取得できるデータは、Ｅメール、チャット、ボイスメッセージ、送信ファイル、写真、ビデオ、保管データ等のコンテンツ情報、及びメールアドレス、電話番号、通信時刻、位置等のメタデータである。取得方法は、企業のサーバーに記録されている過去の通信データを取得する方法と、対象を監視するため通信と同時にリアルタイムでデータを取得する方法と、２種類が区分されている。

（註：上記「保管データ」には、当然の事ながら、クラウド・コンピューティングによる保管データを含むと考えられる。従って、マイクロソフト、ヤフー、グーグル等のクラウド・サービスを利用する場合、米国内にデータ保管サーバーがある限り、米国政府により取得可能データとなる。）

ウ　システムと運営方法

プリズム計画では、FBI が NSA と企業のリエゾンを担当しており、FBI のデータ傍受技術ユニット（Data Intercept Technology Unit）が、協力企業のデータセンター内にデータ取得用システムを設置管理する。

プリズム情報へのアクセスを許可された NSA 職員は、世界中どこからでもデータ要求を出すことにより、協力企業の社員が個別に関与すること無しに、施設内データ取得用システムを経由して必要なデータを入手することができる[17]。

プリズムのデータ要求は「セレクター」と呼ばれる情報を提示して行うこととされており、例えばＥメールアドレス、ＩＰアドレスによりデータが要求できる。但し、キーワード検索やテーマによる要求はできないとされている[18]。

データ要求が、データセンターに記録された既存のデータの場合は、分析官がデータ要求を出すと、この要求は先ず NSA 内部の標的決定・任務管理部署によってデータ要求の適正性が審査される。その上で、FBI の電子通信監視ユニット（Electronic Communications Surveillance Unit）に送付され、同ユニットが FBI のデータベースと照合して問題が無いことを確認（標的が米国人と判明した場合には要求は却下）した後に、FBI データ傍受技術ユニットに送信され、同ユニットから各企業のデータセンター内傍受用システムに要求が送信される。データセンターからデータが取得されれば、取得データは、FBI のデータ傍受技術ユニットを経由して、データ要求をした分析官に提供される。

データ要求が、リアルタイムの監視活動の場合には、分析官がデータ要求を出すと、

---

[17] Robert O'Harrow Jr., Ellen Nakashima and Barton Gellman, "U.S., company officials: Internet surveillance does not indiscriminately mine data," *The Washington Post*, 9 June 2013, accessed 10 June 2013, http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/...

[18] 他方、後述する XKeyscore（通信基幹回線等からの収集データを保管）では、キーワード検索などの内容検索が可能である。

既存データの場合と同様に、この要求は先ずNSA内部の標的決定・任務管理部署によって要求の適正性が審査される。その上で、これがFBIデータ傍受技術ユニットに送信され、同ユニットから各企業のデータセンター内傍受用システムに要求が送信される。そして、標的がインターネットにログインしたり、Eメールを送信したり、会話やチャットをしたり、或いはビデオ会議をしたりするのを検知すれば、FBIのデータ傍受技術ユニットを経由して、分析官に対して自動的にリアルタイムで通知が来るシステムとなっている。2013年4月5日現在、プリズムのテロ対策データベースに登録されているリアルタイム監視対象は11万7675件である[19]。

プリズムを通じて入手されたデータは、NSA内のデータ要求者に提供されるだけではなく、FBIやCIAの分析官にも、データ要求に応じて、自動的に送付され共有される。後述するが、プリズム計画は、NSA単独の情報収集計画というよりも、寧ろ、実態はNSA主導で、FBI、CIAが加わった3機関共同プロジェクトに近い者ではないかと推定される。

エ　NSA内でのデータ保管と利用

NSAに送付されたデータに関しては、データの性格に応じて、NSA内の四つのデータベースに保管蓄積され、事後の分析等に活用される。そのデータベースの暗号名と保管蓄積データは次の通り。

マリーナ：　デジタル通信メタデータ
メインウェイ：　電話通信メタデータ
ピンウェイル：　デジタル通信コンテンツ
ニュークレオン：電話通話ボイス・コンテンツ

（2）プリズム計画の成果

プリズム計画の費用は年間2千万ドル程度であるが、その成果は、極めて大きい。

ア　情報成果

NSAのある内部資料によると2012会計年度中の成果は次の通りである[20]。

- プリズムはNSAの最大の資料源であり、情報報告の全体の7分の1以上を占め、その重要度は逐年増している。即ち、2012会計年度中、プリズム由来の情報報告（End Products）は2万4096件（プリズムのみを資料源とするものはその内の74%）であった。これはNSAの情報報告のうち米国を資料源とするもの約16万件中の 15.1%、セカンド・パーティ、サード・パーティ資料源を含む全情報報告約18万件中の13.4%を占める。

---

[19] "NSA slides explain the PRISM data-collection program," *The Washington Post*,

[20] NSA, "PRISM Expands Impact: FY12 Metrics,"19 November 2012, cited in Greenwald, *No Place*, 111.

- また、情報報告で最も重要な大統領デイリー・ブリーフィングについても、プリズムは最も貢献している。2012 年会計年度 1 年間でプリズム資料を使用した大統領報告は 1477 件であり、これはシギント由来の全情報報告約 8200 件の約 18%を占める[21]。大統領が土日を除く毎日報告を受けていると仮定すると、プリズム資料を使用した情報報告が毎日平均 6 件近くもあることになり、これだけでも極めて重要な資料源であることが分かる。
- 更に、諜報コミュニティの主要情報要素（Essential Elements of Information）全体約 1 万 3 千件中、プリズム資料が貢献したのは 4186 件（全体の 32%）であり、更にプリズムだけが資料源であったのは 220 件であった。
- 2012 年 9 月現在の情報要求登録件数は、4 万 5406 件[22]。
- Ｅメールに関してデータ収集の任務付与ができるドメイン数は 2 万 2 千である。

イ　プリズム情報報告の内容

情報報告の内容は、テロ対策初め広汎に及ぶが、その実例として内部資料から伺えるのは次の通り[23]。

- 2012 年ロンドン・オリンピックでは、特別に英国 GCHQ の分析官 100 人にプリズム資料の利用を認め利用について訓練を施したが、GCHQ はオリンピック関連のテロ容疑者・団体の監視活動に活用した。（その後、英国 GCHQ は、NSA に対してプリズムの広汎な利用承認を要望している[24]。）
- 2011 年に国防総省と主要国防企業を標的としたサイバー攻撃を探知した。
- 2012 年 12 月には、某国防企業のネットワークへの浸透を、NSA 脅威作戦センター（NTOC）が探知して FBI に連絡し、FBI が当該企業に警告を発して、発見当日に対処措置を取ることができた。（註：これはプリズムに加えて、後述するインターネット基幹回線からの資料も貢献しているという。）
- 2013 年 2 月中のある 1 週間の情報成果を纏めた資料によれば、次の通り。

21　米国大統領は、毎日、国家諜報長官率いるブリーフィングチームから世界情勢について報告を受けており、これは大統領にとって極めて重要な行事である。情報源は、シギントに限らず、ヒューミント（人的諜報）やイミント（画像諜報）などを網羅する全情報（オールソース・インテリジェンス）報告であるが、その中でプリズム情報が年間 1477 件も使用されているのである。

22　既述したように、2013 年 4 月段階でのテロ対策のリアルタイム監視対象が１１万件以上であるのに対して、2012 年 9 月段階での全情報要求登録件数が 4 万余りであり、1 年足らずの間での増加件数にしては、不可解である。共に NSA の内部資料にある数字であるが、両者で件数の定義が異なる可能性がある。

23 "What is known about NSA's PRISM program," *Top Level Telecommunications.*

24 Ryan Gallagher, "British Spy Secretly Begged to Play in NSA's Data Pools," *The Intercept,* 30 April 2014, accessed 1 May 2014, https://firstlook.org/theintercept/2014/04/30/gchq-prism-nsa-fisa-unsupervised-access-snowden/

情報件数：５８９件
情報内容の例示：メキシコ（薬物、エネルギー、国内治安、政治情勢）
コロンビア（薬物密輸、左翼ゲリラ FARC）
ベネズエラ（兵器取得、石油）
インド（政治情勢、宇宙開発、核開発）
日本（貿易、対イスラエル関係）
（註：本資料では、情報報告の対象国と対象課題の多くは削除されており、ここに示した国名と課題は全体の内の一部である。）

ウ　プリズム計画の成果の背景

プリズム情報の効果が大きい背景を一言で言えば、米国がインターネット通信の中心地であることである。即ち、米国は、インターネット通信が生まれ発展した国であり、依然として優越的地位を占めている。世界のインターネット通信容量の３分の１近くを占め、インターネット世界の郵便局長的機能を有している。インターネット通信は通信コストの安いルートを経由するのであって、必ずしも地理的に近接したルートを経由する訳ではない。従って、米国外の当事者同士の通信であっても容易に米国内を経由する。

また、フリーメール（Ｇメール、ヤフーメール、ホットメール等）やオンライン・ストレージ・サービス（グーグル・ドライブ、ワン・ドライブ、ヤフーボックス等）、更にはソーシャル・ネットワーク・サービス（フェイスブック、パルトーク、スカイプ、グーグルプラス等々）を利用している者は多いが、これら米国系企業のフリーメール、クラウド・コンピューティングのデータセンターの多くは米国内にある（第一次的データセンターが米国外にある場合でも、データのバックアップを米国内のセンターに置く可能性は高い）と考えられるので、多くのデータが自動的に米国内に集積される。そもそも、例えばグーグル１社が保有する情報量それ自体が、諜報機関に匹敵する膨大なものである[25]。こうして、NSA は米国内に居ながらにして、インターネット関連企業のデータセンターを利用して世界の情報にアクセスできるのである。

それ故、米政府に批判的な某ジャーナリストは「フェイスブックは諜報機関への贈り物」と言っているが、フェイスブック愛用者であれば、米諜報機関はその者の行動、嗜好、性格、交友関係などの私的な情報を纏めて容易に入手できるのである[26]。（米国系企業のフリーメールなど広義のクラウド・コンピューティングを利用する者、少なくとも非米国人は、米国内の図書館にデータを預けているのと同じであり、自己の預けたデ

---

[25] “What if Google was an intelligence agency?” *Top Level Telecommunications.*

[26] Andrea Peterson, “Snowden filmmaker Laura Poitras：‘Facebook is a gift to intelligence agencies’,” 23 October 2014, *The Washington Post*, accessed 28 October 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/23/snowden-filmmaker-laura-poitras-facebook-is-a-gift-to-intelligence-agencies/
あるジャーナリストとは、スノーデン氏が最初に接触したローラ・ポイトラス氏である。

ータは何時でもNSAが取得できる状況にあることを覚悟すべきである。）

（３）プリズム計画の法的構造

ア　対外諜報監視法７０２条

プリズム計画で米国内の民間企業からデータを取得する根拠は、2008年に改正された対外諜報監視法 702 条である。これは、米国内において米国外にいる非米国人に対する情報収集を行うために、通信事業者の協力義務を定めたものである。

即ち、702条によれば、司法長官と国家諜報長官は、対外諜報情報を取得するために米国外にいると合理的に信じられる者を標的とすることを共同して認可（authorize）することができ、両長官はこの認可に基づき電子通信サービス事業者に対して情報収集への協力命令を発することができるとされている。

但し、連邦憲法修正第４条令状主義やプライバシー保護の観点から、米国人に関する情報収集は最少限とするべく、同条では、「米国内にいる者を意図的に標的にしてはならない」「米国外にいる米国人を意図的に標的としてはならない」「送受信者の全てが米国内にいると知られている通信を意図的に取得してはならない」「米国内にいると合理的に信じられる特定者の情報を収集する目的で、米国外にいると合理的に信じられる者を意図的に標的にしてはならない」等と禁止事項が定められている（702条（ｂ））。

イ　「標的決定手順」と「最少化手順」

これらの禁止事項を遵守し、米国人に関する情報を極力収集しないようにするため、司法長官は国家諜報長官と協議の上で、「標的決定手順」と「最少化手順」を採択(adopt)することとされている。

「標的決定手順」は、同 702 条（ｄ）によれば、米国外にいると合理的に信じられる者のみを情報収集の標的とし、且つ通信時に送受信者の全てが米国内にいると知られている通信の意図的な取得を防止する手順とされる。但し、実際の手順書[27]においては、米国外にいると合理的に信じられる非米国人か否かの判断は、得られる情報を総合的に勘案して行うものとされ、米国人か否か判然としない時、米国外にいるかどうか判然としない時、居場所自体が知られていない時は、非米国人と推定して良いとするなど、手順は必ずしも厳格ではない。また、米国外の非米国人を標的にして収集した通信であれば、通信当事者に米国内の米国人が含まれても、問題はないこととなる。

また、「最少化手順」は、上記「標的決定手順」によっても現実には米国人に関する情報を入手してしまうため、その米国人に関する情報の収集と保持を最少化し、且つ、その配布を禁止する手順であり、同 101 条（ｈ）などにその内容が規定されている。

---

[27] Glenn Greenwald and James Ball, "The top secret rules that allow NSA to use US data without a warrant," *The Guardian*, 20 June 2013, accessed 24 June 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant

但し、これにも除外事項が認められており、国内情報（米国人に関する情報を含む）であっても、（国際テロや大量破壊兵器拡散対策を含む）対外諜報として価値ある情報、犯罪の証拠であって法執行目的に有用な情報、死亡重傷の結果をもたらす脅威情報は一定の保持と配布が認められている。事実、実際の手順書[28]では、これらの場合、特に前二者の場合は原則として FBI に通報するよう定められている。また、暗号通信は、技術的データベース情報として保管配布できることとしている。更に、これら以外の情報も一定のものは５年間の保管が認められているなど、こちらの手順も必ずしも厳格ではない。

なお、これら「標的決定手順」と「最少化手順」は、NSA 担当官に適用されるだけでなく、FBI や CIA の担当官にも等しく適用される[29]。

ウ　対外諜報監視裁判所

司法長官と国家情報長官は、対外諜報裁判所から、上記の「標的決定手順」「最少化手順」等が法律に適合したものであることを認証する令状（approving order）を取得した上で（緊急時には令状の取得は事後でも可）（同 702 条（ｇ））、電子通信事業者に対して情報提供についての協力命令(directive)を出すことができる（同 702 条（ｈ））こととされている。

エ　米国人の通信傍受

米国政府関係者は、個別の令状なしに、米国人の通信が傍受されることはないという主張をしている。確かに、対外諜報監視法によれば、米国人や純粋な国内通信を情報収集の標的とするには、対外諜報監視裁判所の個別の許可状を必要とする。しかしながら、先に見たように、米国外の非米国人を標的としても、「付随的に(incidentally)」或いは「うっかりと(inadvertently)」米国人の通信或いは国内通信を取得することが可能であり、その量は相当のものになっていると、推定される。

（４）抵抗するヤフー[30]

---

[28] Greenwald and Ball, “The top secret rules…,”

[29] “Classified documents show rules for NSA surveillance without a warrant,” *The Washington Post*, undated, accessed 24 June 2013, http://apps.washingtonpost.com/g/page/politics/classified-documents-show-rules-for-nsa-surveillance-without-a-warrant/248/

本資料を見ると、司法長官が国家情報長官と協議の上「標的決定手順」「最少化手順」を採択するに当たっては、NSA 長官、CIA 長官、FBI 長官の３名から両手順書が法律の要件を充足する旨の宣誓供述書の提出を受けていることが伺われる。

[30] 出典資料は次の通り。

--Center for Democratic and Technology, *Yahoo v. U.S. PRISM documents,* 12 September 2014, accessed 14 October 2014,

プリズム計画が始まった時、協力に抵抗したのがヤフーである。上記イ、エでも述べたように、対外諜報監視法 702 条に基づくデータ提供は相当広範囲に及ぶため、ヤフーはこれを憲法違反であるとして、当初協力を拒否した。

即ち、2007 年 8 月に連邦議会で米国保護法が成立したが、同法には後に改正対外諜報監視法 702 条に継承される規定が含まれていた。同法が成立すると、連邦政府は関係する電子通信事業者にプリズム計画への協力を働き掛けたが、ヤフーが非協力の姿勢を見せた。そこで、11 月司法長官と国家情報長官はヤフーに対してプリズム計画への協力命令を発すると共に、司法長官が対外諜報裁判所に対してヤフーに対する協力の強制命令の発出を求めて提訴した。

ヤフーは、この協力命令は憲法違反であるなどと主張して争ったが、第一審の対外諜報裁判所で 2008 年 4 月に敗訴し協力するよう強制命令を受けた。引き続き、対外諜報控訴裁判所に上訴したものの、ここでも 8 月に敗訴して、米政府の協力命令に関する裁判所の強制命令が確定した。（なお、上訴中の当初、ヤフーは協力命令に従わなかったが、対外諜報裁判所は 5 月、司法省の訴えを受け、命令違反 1 日に付き法廷侮辱罪で 2500 万ドルの課徴金を命じる予告をしたため、ヤフーは命令に従った。）

米国シリコンバレーを拠点とするオンライン・サービス事業者の多くは、比較的政府からの独立を標榜する企業が多く、後述する ATT などの通信事業者と異なり、必ずしもプリズム計画への協力に積極的でなかったとも言われるが、ヤフーの敗訴を見て、他の多くの事業者も協力せざるを得ないという流れができたと言われている。

なお、これら裁判関係資料は機密指定され長らく開示されてこなかったが、ヤフーからの働掛けにより 2014 年 9 月に至り相当部分が開示された[31]。

（5）積極的に協力するマイクロソフト

このようにプリズム計画への協力に関して、ヤフーは抵抗したが、いち早く協力をしたのが、マイクロソフトである。対外諜報監視法 702 条の前身規定（米国保護法）が 2007 年 8 月に成立すると、翌 9 月にはプリズム計画に参加するなど、その協力姿勢は際立っている。その協力の事例の一部は次の通りである[32]。

---

https://cdt.org/insight/yahoo-v-u-s-prism-documents/
--Craig Timberg, "US threatened massive fine to force Yahoo to release data," *The Washington Post,* 11 September 2014, accessed 30 September 2014, http://www.washingtonpost.com/business/technology/us-threatened-massive-fine-to-force-yahoo-to-release-data/2014/09/11/...

[31] Ron Bell (Yahoo's general counsel), *Shedding Light on the Foreign Intelligence Surveillance Court: Court Findings from Our 2007-2008 Case*, 11 September 2014, accessed 7 October 2014, http://yahoopolicy.tumblr.com/post/97238899258/shedding-light-on-the-foreign-intelligence-surveillance

[32] 出典資料は次の通り。

- ウェブチャットの暗号化の回避

  2012 年 7 月マイクロソフトは Outlook. com.（フリーメール）のウェブチャットに SSL 暗号を導入したが、マイクロソフトは、FBI と協働して暗号回避の方法を開発して同年 12 月に導入し、これによりデータ収集上の支障が生じないようにした。

  なお、Hotmail、Live、Outlook. com. email 等のデータに関しては、プリズム計画ではそもそも暗号化前データを取得しているため、データ収集上問題は生じないとしている。

- スカイドライブ（オンライン・ストレージ）のデータ入手の簡略化

  従前はデータ入手のためにスカイドライブ専用の特別手続を必要としていたが、FBI がマイクロソフトと何ヶ月にも亘り調整してきた結果、2013 年 3 月から別個の特別手続が不要となり、迅速完全なデータ収集が可能となった。

- スカイプ（マイクロソフト子会社）蓄積データの収集可能化

  2011 年にスカイプがプリズム計画に参加して以来、リアルタイムの監視活動でのみデータ取得が可能であったが、2013 年３月から、スカイプ・データベースの蓄積データの収集が可能となった。（世界のスカイプ利用者は６億人以上とされており）これにより更に有効な情報入手が期待される。

以上は、マイクロソフトの協力の例であるが、シリコンバレーの企業の中ではマイクロソフトの協力姿勢が際立っているようである。

（６）プリズム計画での FBI と CIA との協力

プリズム計画では、民間事業者とのリエゾンは FBI が務めており、そもそも FBI とは協力関係にあるが、（１）でも述べたように FBI と CIA はデータ利用でも関与しており、NSA 内部資料では、プリズム計画は（NSA, FBI, CIA の）「チーム・スポーツ」であるとまで述べられている[33]。協力の具体例として次の事例が挙げられている。

- 従来、プリズム計画における NSA 任務付与（情報要求）一覧表は、FBI と CIA に対して不完全且つ不正確なものしか提供されていなかったが、2012 年に NSA 内担当部署が、２週間毎に自動的に作成配布するソフトウェアを作成した。これによって、FBI と CIA の担当者は、世界中の NSA 分析官からの任務付与状況（正確且つ最新の状況）を把握して、これら任務付与への対応データ（のコピー）を容易に要求できるようになった。

--Glenn Greenwald, et. al., "Microsoft handed the NSA access to encrypted messages," *The Guardian,* 12 July 2013, accessed 22 October 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.
--Greenwald, No Place, 113-115.

[33] NSA, "Expanding PRISM Sharing with FBA and CIA," 31 August 2012, cited in Greenwald, *No Place*, 116.

○　FBI と CIA の分析官がプリズムを有効活用できるようにする目的で、NSA　の責任者が、プリズム運用に関する週刊ニュースとガイダンスの作成送付を開始した。これは FBI と CIA の担当官から高く評価されている。

私見であるが、これらの事例は、米国の諜報コミュニティが「コミュニティ」と呼ぶに相応しい緊密な協力関係を構築していることを明示している。国家の諜報コミュニティと呼ぶ以上、行政の最高責任者たる大統領の意を受けた情報要求、コミュニティ内での情報及び分析成果の共有、その前提としての統一した秘密保全態勢などのシステムが整備されていることは最低限必要である。ところが、今回のスノーデン資料から、米国の諜報コミュニティはそのレベルを超えて、情報の収集分析においても諸機関が密接な協力関係を有していることが明白であり、正に諜報コミュニィと呼ぶに相応しい実質を備えていることが分かる。

（7）プリズム余話

以上で見たように、プリズム計画は米国にとって極めて有効な情報収集手段である。その背景には、オンライン・サービス事業者のデータセンターには膨大なデータが蓄積されているという事実がある。加えて、米国については同国がインターネット通信の中心地であることが貢献しているが、他方、民主主義国家として国内情報の収集に関しては一定の制約も掛かっている。

それでは、その他の国はどうであろうか。米国以外の諸国においても、インテリジェンスに於いてオンライン・サービス事業者のデータセンターからのデータ取得が極めて有用且つ効率的であることは、電子通信の知識を有する者には自明のことであったろう。そうであれば、米国（及びセカンド・パーティ諸国）以外にも、既にオンライン・サービス事業者のデータセンターからデータを取得している国があっても不思議ではない（それも、法律の制約なしに）[34]。また、仮に、今まで取得していなかったとしても、スノーデン資料によりその有効性が世界中に示された以上、諸国が新たにその取得に取り組むのは自然であろう。事実、スノーデン資料で名指しをされた企業には、他国から同様の協力要請がなされているとの報道もある。

インテリジェンスの世界とはこういう世界である。スノーデンによる告発・漏洩資料によって、我が国民のインテリジェンス理解が進むことが期待される。

---

[34]　次の報道は、ロシアや中国も、同様なことを法律の制限なしに実行している旨述べている。--Associated Press, “Surveillance pervasive around the world, but Silicon Valley gives America the edge,” *The Washington Post*, 2 July 2013, accessed 16 July 2013, http://www.washingtonpost.com/world/middle_east/surveillance-pervasive-around-the-world.../

３　通信基幹回線からの収集[35]

（１） 概要

ア、初めに

NSA は、約２０の計画により、世界のインターネット通信基幹回線の主要ポイントにおいて膨大なデータを収集している。これら約２０の計画には、米国の内と外、収集の法的根拠、民間企業の協力の有無、米国外の場合に他国の諜報機関の関与の有無、具体的な取得データの中身など、様々なものが含まれており、一様ではない。

この通信基幹回線からのデータ収集は、民間企業との協力を得て行う SSO（特別資料源作戦）チームが担当している。SSO のロゴマークは地球を覆う光通信回線を鷲が掴んでいるもの（正に鷲づかみ）であり、ロゴマークが SSO の中心業務を示していると推定できよう。

ところで、この収集と「プリズム」計画との違いは、「プリズム」計画は特定のデータ要求を出して関係企業のデータセンターから関連データを取得するのに対し、本収集は基本的に回線からの大量一括収集であることである。後述する（第２部第３章）が、大量一括収集されたデータは XKeyscore という第一次記憶装置に一定期間記録され、また更に情報価値があると判断されるデータは別のデータベース（「ピンウェイル」「ニュークレオン」等）にも長期間保管される構造となっている。なお、後述する外国通信衛星の傍受や特別収集サービスも、データの大量一括収集であり、これにより収集されたデータは先ず XKeyscore サーバーに記憶されると共に、情報価値があると判断されるデータは別のデータベースにも長期間保管される。

イ、地図上のアクセス点

NSA 内部資料によれば、世界中の通信へのアクセス点として地図上に記載されていた場所は次の１６ヶ所である[36]。

○　米国内：米本土・西海岸４ヶ所、東海岸２ヶ所、
　　ハワイ、グアム各１ヶ所　　（合計８ヶ所）

---

[35] 主要な参考文献は次の通り。
--"NSA's global interception network," *Top Level Telecommunications*, 3 December 2013, updated 17 July 2014, accessed 26 September 2014
http://electrospaces.blogspot.jp/2013/12/nsas-global-interception-network.html
--"Slides about NSA's Upstream collection," *Top Level Telecommunications*, 17 January 2014, updated 20 May 2014, accessed 26 September 2014,
http://electrospaces.blogspot.jp/2014/01/slides-about-nsas-upstream-collection.html
--Greenwald, *No Place,* 103-108, 136-137, 142-144.

[36] ス資料、NSA, Driver 1: Worldwide SIGINT/Defense Cryptologic Platform, (2012) , accessed 23 March 2015,
http://electrospaces.blogspot.jp/2013/12/nsas-global-interception-network.html

- アジア：韓国、シンガポール[37]、カロリン諸島（ミクロネシア）（？）
- 中近東：オマーン、アフガニスタン（？）　　- アフリカ：ジプチ
- 欧州：　英国、フランス（マルセイユ）[38]

これらの地点の多くは世界の光通信の基幹回線の通過地点である。（？）印は地図から判断して他国の可能性もある。

なお、以上の１６ヶ所は例示であって、これ以外にも相当数のアクセス拠点があり、全体で５０～６０ヶ所程度は存在すると推定される。その理由は、後に（第２部第３章）詳述するが、通信基幹回線からの各収集拠点には XKeyscore の第一次記憶装置（サーバー）が設置されているが、そのサーバーの設置拠点数が 50～60 ヶ所程度と推定できる。従って、通信基幹回線へのアクセス地点数も同数程度は存在すると考えられるからである。

ウ、NSA による分類

NSA 内部資料によれば、NSA は 2010 年時点で基幹回線からの収集を大きく次の３種類に分類している[39]。

① 民間企業の協力によるもの

対外諜報監視法又は大統領命令の規定に基づき、主として米国内において米国民間事業者の協力を得て行うもの。主要計画として、「ブラーニー」「フェアビュー」「ストームブリュー」「オークスター」の四つがある。但し、「オークスター」は、米国外の拠点でのデータ収集の小計画を多く含んでいる。

② 外国政府と協力して行うもの

外国政府と正式の協力関係を築いて行うもので、次の２つの計画がある。

○「ウィンドストップ」：セカンド・パーティ諸国と協力して行うもので、協力国は主として英国とされる。

○「ランパート A」：サード・パーティ諸国と協力して行うもので、ドイツが協力国として相当の位置を占めているようである。

③ 単独事業

---

[37] 地図上ではインドネシアのようにも見えるが、次の理由からシンガポールと判定した。①光通信の基幹回線はシンガポールを経由していること、②シンガポールは、SSPAC（太平洋シギント首脳会議）（第２部第１章３の多国間協力枠組参照）にも参加しているなど、東アジアの「サード・パーティ」諸国の中でも主要な位置を占めていると判断できること。

[38] 2013 年 10 月 30 日付けの仏紙ルモンドによれば、仏諜報機関 DGSE と NSA は協力して、2011 年末又は 2012 年初に、通信基幹回線が海底からフランス上陸する地点マルセイユでのデータ収集を開始したとされる。Jacques Follorou, “Surveillance：la DGSE a transmis des données à la NSA américaine,” *Le Monde*, 30 October 2013, accessed 23 March 2015, http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html?xtmc=nsa&xtcr=4

[39] -“NSA’s global interception network,” *Top Level Telecommunications*,

何らかの方法を以て、米国外でNSAが単独で一方的に実施するものであり、５つの計画があるとされているが、これらに関しては情報が極めて不足している。但し、上記のアフガニスタンのデータ収集拠点は、この単独事業である可能性が高い。

エ、法的根拠

上記①の多くは米国内で行われるので、対外諜報監視法により民間事業者に協力義務が課せられていると考えられる。これに対し、②③は米国外で行われるので根拠は大統領命令第12333号であり、民間事業者の協力があるとすれば任意で行っているということになる。

（２） 民間企業の協力によるデータ収集計画

これは、NSAの内部資料では「アップストリーム」といわれるデータ収集であり、多く（以下のア、イ、ウ）は、対外諜報監視法によって米国内の民間事業者に協力命令を発して行っているものである。大統領への情報報告において、貢献度が高いとされている順に見てみる。

なお、これら民間企業の協力によるデータ収集の費用合計（2013会計年度予算Corporate Partner Access）は、（プリズム計画を含めて）2億7813万ドルである[40]。

ア 「ブラーニー」計画[41]

ATT初め幾つかの企業の協力を得て、米国内でデータ収集をしている。

法的根拠は主として1978年制定の対外諜報監視法104条であり、従って本計画は遅くとも1978年から行われていたと考えられる。同条に基づく対外諜報監視裁判所への秘密の令状請求は、司法長官の承認を得て行うこととされている。収集は個別の令状を得て行うことになっているが、この個別の令状がどの程度の特定性を必要とするか（メールアドレス等の特定を必要とするか、或いは大使館名程度の特定で足りるか）は明白ではない。

データ収集の対象は、外交施設、外国政府、テロ活動、経済問題とされている。

2010年時点での標的国には、仏、独、伊、ギリシャ、ＥＵ，イスラエル、ブラジル、

---

40 ス資料 *FY2013 Congressional Budget Justification Vol. I : National Intelligence Program Summary*, February 2012, 159. accessed 20 August 2014, http://fas.org/irp/budget/nip-fy2013.pdf

41 上記註の参考文献の他、
--Siobhan Gorman and Jennifer Valentino-Devries, “New Details Show Broader NSA Surveillance Reach,” *Wall Street Journal*, 20 August 2013, accessed 22 August 2013, http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470?mg=reno64-wsj.

メキシコ、ベネズエラ、日本、韓国、国連が含まれているという[42]・[43]。そして、例えば、EU についてはその電話会議システムの傍受が可能であるとされる[44]。また、2010 年 9 月のエピソードとして、ライス米国連大使からの情報要求を受けて、急遽ガボン、ウガンダ、ナイジェリア、ボスニア 4 カ国の国連代表部と在米大使館を「ブラーニー」の情報収集対象にするべく、「ブラーニー」担当が、FBI の協力を得て、1 日で NSA 長官、国防長官、司法長官の決裁を得て対外諜報監視裁判所に持ち込み、翌々日には令状を得た事例が紹介されている[45]。

なお、2013 会計年度の本計画予算は 6596 万ドルである[46]。本経費は協力企業への支払いを含むものであり、実際それが費用の過半を占めると見られる。

イ　「フェアビュー」計画

これは、国際通信の基幹回線、ルーターやスイッチにアクセスできる米国企業の協力によって、世界の通信を収集するものである。

この企業名は不明であるが、NSA との協力関係は 1985 年にまで遡るという。同企業は米国内で活動するが、米国を通過するデータにアクセスでき、且つ他の通信事業者やインターネット事業者へのアクセスをも提供できる企業関係を有しているとされる。同企業は、NSA が関心を有する通信データが米国内監視装置を通過するように積極的

---

[42] Greenwald, *No Place,* 103.

[43] 「ブラーニー」計画による情報の例として、2013 年 4 月 18 日付の NSA 内部資料によれば、同年春のオバマ米大統領とパン国連事務総長との会談に先立ち、パン事務総長のトーキング・ポインツを入手した事例が上げられている。
--ス資料、NSA, “Blarney: Operational Highlight,” 18 April 2013, accessed 3 July 2015, https://www.documentcloud.org/documents/2153988-un-secretary-general-xks.html#document/p1
-- Morgan Marquis-Boire, Glenn Greenwald and Micah Lee, "XKeyscore: NSA's Google for the World's Private Communications,” *The Intercept,* 1 July 2015, accessed 2 July 2015, https://firstlook.org/theintercept/2015/07/01/nsas-google-worlds-private-communications

[44] Laura Poitras, Marcel Rosenbach and Holger Stark, “How America Spies on Europe and the UN,” *Spiegel Online,* 26 August 2013, accessed 27 August 2013, http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[45] Greenwald, *No Place,* 143－144.
FBI の協力では、より具体的な情報収集の標的決定についても、協力を求めた様である。なお、本件は、国連に於けるイラン制裁問題での関係国の立場に対する情報収集であったが、同年１０月には国連安全保障委員会でイラン制裁決議があり、この際も、フランス、日本、メキシコ、ブラジルを含む８カ国の情報収集を行い、米国連代表部のこれら諸国との事前折衝に貢献した旨が記されている(但し、後者の資料源は「ブラーニー」計画には限定されていない)。

[46] “NSA also has arrangements with foreign internet providers,” *Top Level Telecommunications*, 24 August 2013, updated 25 January 2014, accessed 23 October 2014, http://electrospaces.blogspot.jp/2013/08/nsa-has-also-arrangements-with-foreign.html
以下「民間企業の協力によるデータ収集計画」の費用は、本文献による。

に通信状況を形成しているとされる[47]。

データ収集の主対象は、米国外の当事者同士の通信であり、事例として、パキスタン、北朝鮮、イラン関連の収集力を示す内部資料がスノーデン資料の中に含まれている[48]。

本計画に関与する企業の積極姿勢を見る限り、関与企業は、対外諜報監視法 702 条の規定に基づき協力を開始したというよりは、元々、NSA に積極的に協力してきた企業が、2008 年同法改正後にその協力の根拠を 702 条に置いたものと推定される。

なお、2013 会計年度の本計画予算は 9474 万ドルである。

ウ　「ストームブリュー」計画

これは、国際通信の基幹回線、ルーターやスイッチにアクセスできる米国企業２社（内１社はベライゾンとされる）の協力によって、世界の通信を収集するため、米国内の主要ポイント７ヶ所を通過する通信を収集するものである。

根拠法令は主として対外諜報監視法 702 条であり、これに基づき、司法長官と国家情報長官から、関係企業に協力命令が発出されていると考えられる。詳細は不明であるが、データ収集には FBI も関与している。

なお、2013 会計年度の本計画予算は 4604 万ドルである。

エ「フェアビュー」「ストームブリュー」計画の運用と効果

これら計画の運用は、先ず、企業にインターネット回線からの第一次抽出を依頼する。即ち、企業は、少なくとも一方当事者が外国にある通信データを、情報価値がないと判断されるもの（映画や音楽のダウンロードなど）を除外して、抽出する。この第一次抽出データを、今度は NSA のシステムが、メールアドレス、サーバーアドレス、或いはその他のメタデータ等から判断して情報価値があると考えられるものの第二次抽出を行い、NSA へデータを送付する。また、第一次抽出の対象となっている通信は、米国関係通信の７５％に及び、相当のデータ量を検索対象としていることが伺える。なお、これらの抽出システムの製造には、米国企業のナルス（ボーイング子会社）、シスコ・システムズ、ジュニパー・ネットワークス等の企業が関与していると言われる[49]。

---

[47] Greenwald, *No Place,* 105.及び
--Glenn Greenwald, "The NSA's mass and indiscriminate spying on Brazilians," *The Guardian*, 7 July 2013, accessed 15 August 2013, http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying
--Glenn Greenwald and Jose Roberto Kaz Married, "U.S. spied on millions of e-mails and calls of Brazilians," *O Globo,* 6 July 2013, accessed 15 August 2013, http://translate.google.com.br/translate...oglobo.globo.com...Feua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934&act=url

[48] "Slides about NSA's Upstream collection," *Top Level Telecommunications.*

[49] Gorman and Valentino-Devries, "New Details Show Broader NSA Surveillance Reach," *Wall Street Journal.*

これら二つの計画の効果は高いと考えられる。それは、プリズムでも述べたように、米国がインターネット通信の中心地であるからである。即ち、米国は、今でも、世界の大陸間の通信容量の３分の２を占め、実際の大陸間通信では９０％以上が米国経由であるとも言われる。従って、一方当事者が米国内にいる場合は当然として、米国外の当事者同士の通信であっても容易に米国内を経由する。これらの「アップストリーム」計画はその利点を最大限活用していると見られる。

なお、NSA が取得したデータついては、第一次記憶装置である XKeyscore に記憶されると共に、プリズムでも記述したように、有用なデータはその性格（電話かデジタル通信か、コンテンツかメタデータか）に応じて、NSA 内の４つのデータベース「マリーナ」「メインウェイ」「ピンウェイル」「ニュークレオン」に保管蓄積され、事後の分析等に活用される。

オ　「オークスター」計画

本計画は、情報通信企業の協力を得て通信基幹回線からデータを取得するものであり、少なくとも８つの小計画で構成されている。８つの小計画の多くは大統領命令 12333 号を根拠に米国外で実施されているが、一部米国内での収集もあるとされる。８つの小計画のうち内容の分かるものは次の通り。

なお、2013 会計年度の本計画予算は 941 万ドルである。

○「モンキーロケット」計画：大統領命令に基づく国外収集。主要標的は、中近東、欧州、アジアのテロ活動。（インターネット通信）

○「シフティング・シャドー」計画：大統領命令に基づく国外収集。主要標的は、アフガニスタンの通信。（電話通信）

○「オレンジクラッシュ」計画：大統領命令に基づく国外収集。ポーランド政府の協力も得てポーランド国内で収集。主要標的は、中東、アフガニスタン、アフリカの一部。（インターネット通信と電話通信）。従前は「オレンジブロッサム」という電話通信収集計画があったが、本計画に吸収されたようである[50]。

（註：本計画がサード・パーティとの共同収集に位置付けられていない理由は、運営の主体が NSA であって、ポーランド政府の関与が、共同収集と言えるほど強固ではないためと考えられる。）

○「ヨットショップ」計画：大統領命令に基づく国外収集。標的は、世界のインターネット通信のメタデータ。

○「シルバーゼーファ」計画：米国内における収集。主要標的は、中南米。（インターネット通信と電話通信）。従前は「ブルーゼーファ」という電話通信収集計画があり、本計画に吸収されたようである。ブラジルとコロンビアに協力企業又はその支部が存在するようであり、ブラジル、コロンビアの国内通信の収集も可能として

[50] Greenwald, *No Place,* 106.

いる[51]。

（３） 外国政府（セカンド・パーティ）との共同収集：「ウィンドストップ」

外国政府、中でも UKUSA 協定の参加国（セカンド・パーティ）と協力して行う収集は、「ウィンドストップ」計画と言い、そのなかに４つの小計画がある。収集対象は欧州と中近東の通信である。協力相手国は主として英国であり、小計画の「マスキュラー」と「インセンサー」は英国との事業とされる。他に「トランシャント・サリブル」と名称不明の小計画の２つがある。

なお、2013 会計年度の本計画予算は 1040 万ドルである[52]。

ア 「マスキュラー」計画[53]

2009 年 7 月から運用開始された NSA と GCHQ との共同収集事業であり、英国内において、グーグル、ヤフーなどのインターネット企業の世界のデータセンターを結ぶ通信回線に進入してデータを収集するものである。

例えば、グーグルは現在世界中に１２のデータセンターを置いているが、これらデー

---

[51] 同上。

[52] ス資料、NSA「ウィンドストップ」「ランパートＡ」関係予算資料、accessed 18 July 2014, https://s3.amazonaws.com/s3.documentcloud.org/documents/1200866/foreignpartneraccessbudgetfy2013-redacted.pdf. 後述する「ランパートＡ」の費用も、本資料による。

[53] 「マスキュラー」計画の主要な参考文献は次の通り。

--Barton Gellman and Ashkan Soltani, “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say,” *The Washington Post*, 30 October 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

-- Barton Gellman, Todd Lindeman and Ashkan Soltani, “How the NSA is infiltrating private networks,” *The Washington Post,* 30 October 2013, accessed 5 November 2013, http://apps.washingtonpost.com/g/page/national/the-nsa-is-hacking-private-networks/542/

-- Barton Gellman, Ashkan Soltani and Andrea Peterson, “How we know the NSA had access to internal Google and Yahoo cloud data,” *The Washington Post*, 4 November 2013, accessed 5 November 2013, http://www.washingotnpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/

--“What Yahoo and Google did not think the NSA could see,” *The Washington Post*, accessed 7 November 2013, apps.washingtonpost.com/g/page/world/what-yahoo-and-google-did-not-think-the-nsa-could-see/555/

--Nicole Perlroth and John Markoff, “N.S.A. May Have Hit Internet Companies at a Weak Spot,” *The New York Times,* 25 November 2013, accessed 27 November 2013, http://www.nytimes.com/2013/11/26/technology/a-peephole-for-the-nsa.html?pagewanted=all&_r=0

タセンターは同期して一体的に機能するように構成されていると共に、信頼性と機能性のため同一データを複数のセンターに重複して保管するなどしており、センター間では多くのデータ送信がなされている。この専用回線に侵入して回線上から必要データを取得している。

グーグルのセンターの配置は米国内６ヶ所、欧州３ヶ所（アイルランド、ベルギー、フィンランド）、アジア２ヶ所（台湾、香港）、南米１ヶ所（チリ）であり、欧米が中心である。センター間は専用回線で結ばれているが、米国と欧州のセンター間の専用回線は英国を経由しており、英国での収集が効果的である。これらの事情はヤフーも同様であると見られる。グーグルとヤフーに対する専用回線の提供企業は米国企業「レベル３コミュニケーションズ」であるため、NSA と GCHQ への協力が疑われているが、同社は取材に対して協力について肯定も否定もしていない[54]。

2013 年のスノーデン告発の時点では、データセンター間の専用回線の通信には暗号が施されていなかったが、グーグルは基幹回線への進入を危惧して、その時点で既に暗号化への取組を開始していたとされる。

なお、NSA 内部文書によれば、グーグルとヤフーの他、マイクロソフトのデータセンター間回線にも進入していた可能性が高いとされる[55]。

イ　「インセンサー」計画[56]

「インセンサー」計画も英国と米国との共同事業で、英国において通信基幹回線からデータ収集を行っており、且つその情報成果は「マスキュラー」計画よりも大きいとされる。即ち、英国は大西洋間通信の欧州のハブであり、北米と欧州を結ぶ通信の殆どは英国を経由する。そこで、英国 GCHQ は通信会社７社の協力を得て、大西洋光ファイバー回線の英国経由地でデータ抽出システムを設置して、関心データを抽出しているという。この抽出能力は膨大で、2012 年時点で既に大西洋を通るケーブル 200 本を抽出対象にした上で、同時に４６本以上から抽出処理をしており、且つ抽出能力は増強中であるとされる。

協力企業は、ケーブル＆ワイヤレス（ボーダフォン子会社）、ＢＴ、ベライゾン、グローバルクロシング、レベル３コミュニケーションズ、ヴァイアテル、インタルートの

---

54 Perlroth and Markoff, "N.S.A. May Have Hit Internet Companies at a Weak Spot."

55 "Did the NSA target Microsoft too?" *The Washington Post,* accessed 27 November 2013, http://apps.washingtonpost.com/g/page/world/did-the-nsa-target-microsoft-too/620/

56 主要な参考文献は次の通り。

--Ewen MacAskill, et.al., "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, 21 June 2013, accessed 23 October 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

-- Ewen MacAskill, et.al., "How does GCHQ's internet surveillance work?" *The Guardian*, 21 June 2013, accessed 24 June 2013, http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

７社とされる。特にケーブル＆ワイヤレスが主導的な役割を果たしており、最多の回線へのアクセスを提供して入る他、他社の回線へのアクセスまで提供しているとされる[57]。（なお、英国では 2000 年制定の調査権限規制法により、通信傍受に関する大幅な権限が国務大臣に付与されている。）

この収集能力は膨大であり、英国 GCHQ の 2010 年の内部資料では、GCHQ は NSA 以上にインターネットへのアクセスを持ち、NSA よりもメタデータを収集していると豪語している[58]。

ウ　「トランシャント・サリブル」他２計画

この二つの小計画の内容は全く不明である。

但し、英国の収集拠点は、本土外にもあり、キプロス島内の英国海外領土（デケレア地区）にその収集拠点があると見られる[59]。キプロス島は東地中海の通信基幹回線の一つの拠点であり、英国が海外領土を持ち軍事基地を維持している以上、そこに収集拠点を設定するのは自然なことであろう。また、英国は中東のオマーンのセエブにも収集拠点を構築している。オマーン現国王は 1970 年に英国の支援するクーデタで即位した経緯があり、セエブには英国の衛星通信傍受基地（大きな受信用アンテナ６つ設置）がある。更に、同地が湾岸の海底光回線の経由地でもあるため、2009 年以降英国がインタ

---

[57] James Ball, Luke Harding and Juliette Garside, “BT and Vodafone among telecoms companies passing details to GCHQ,” *The Guardian*, 2 August 2013, accessed 25 October 2013, http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq
--Ryan Gallagher, “Vodafone-Linked Company Aided British Mass Surveillance,” *The Intercept,* 20 November 2014, accessed 21 November 2014, https://firstlook.org/theintercept/2014/11/20/vodafone-surveillance-gchq-snowden/
--Frederik Obermaier, Henrik Moltke, Laura Poitras and Jan Strozyk, “Snowden-Leaks: How Vodafone Subsidiary Cable & Wireless Aided GCHQ’s Spying Efforts,” *Sueddeusche Zeitung International,* 25 November 2014, accessed 26 November 2014, http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsidiary-cable

上記の南ドイツ新聞記事の NSA 内部資料によれば、「ケーブル＆ワイヤレス」は、この事業のために、少なくとも 2008 年 6 月から 2012 年 2 月迄の間 GCHQ との間で「共同事業チーム」の定期的な会合を持ち、また、2009 年 2 月現在 GCHQ 職員が同社内でフルタイムで勤務していた。また、同社が GCHQ にアクセスを提供した他社の回線とは、インドの通信会社「Reliance Globalcom(現在は Global Cloud Xchange)」とされる。

[58] MacAskill, et.al., “GCHQ taps fibre-optic cables….”

[59] “NSA’s global interception network,” *Top Level Telecommunications*, 及び
--Duncan Campbell, et. al., “Exclusive: UK’s secret Mid-East internet surveillance base is revealed in Edward Snowden leaks,” *The Independent*, 23 August 2013, accessed 22 October 2013, http://www.independent.co.uk/news/uk/politics/exclusive-uks-secret-mideast-internet-surveillance-base-is-revealed-in-edward-snowden-leaks-8781082.html

ーネット基幹回線のデータ収集を開始したという[60]。

「トランシャント・サリブル」他２小計画の詳細は全く不明であるが、キプロス島やオマーンでの収集がそれらに当たる可能性がある。

（４） 外国政府（サード・パーティ）との共同収集：「ランパートＡ」[61]

UKUSA 協定諸国以外の所謂サード・パーティ諸国と協力して行う事業が、「ランパートＡ」計画と呼ばれている。2010 年 10 月の NSA 内部資料によれば、本計画は 1992 年に世界の通信基幹回線へのアクセスを求めて開始したものである。協力国は、基幹回線へのアクセスと機器の設置を受け持ち、米国 NSA はデータ抽出・処理・分析のための機器を提供する。両当事国は共同してデータ収集を行い、収集データはサード・パーティの分析官が分析をすると共に NSA にも送信される。なお、この共同収集ではお互いを収集標的にはしないこととしているが、NSA はこの点にはついては例外はあるとしている。

協力国は、2010 年の段階では、協力国が５ヶ国、協力的関係を有する国[62]が２ヶ国、更に、協力関係について調整中の国が２ヶ国とされている。この時点で協力国として名前が判明しているのは、ドイツとデンマークである。また、スウェーデンが 2011 年から協力を開始した。

ドイツとは相当緊密な関係があるようであり、同国との間では複数の小計画が運用されているとされる[63]。また、デンマークでの収集対象は、ロシア及び北欧、スウェーデ

---

[60] Duncan Campbell, "Revealed: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base, *The Register,* 3 July 2014, accessed 4 November 2014, http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base?page=2

[61] 主要な参考文献は次の通り。

--Ryan Gallagher, "How Secret Partners Expand NSA's Surveillance Dragnet," *The Intercept,* 18 June 2014, accessed 18 July 2014, https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

--ス資料 NSA, *RAMPART-A: Project Overview*, 1 October 2010, accessed 18 July 2014, https://s3.amazonaws.com/s3.documentcloud.org/documents/1200864/tssinframpartaoverview-v1-0-redacted-information.pdf

--ス資料 NSA「ウィンドストップ」「ランパートＡ」関係予算資料、accessed 18 July 2014, https://s3.amazonaws.com/s3.documentcloud.org/documents/1200866/foreignpartneraccessbudgetfy2013-redacted.pdf

[62] 「協力的関係を有する国」とは如何なるものか不明である。明確なのは通常のサード・パーティとの協力関係とは異なり、諸々の制約のため、データ収集や情報共有などの点において、NSA が望ましいと考える水準の協力関係に至っていないものであろう。

[63] "The German operation Eikonal as part of NSA's RAMPART-A program," *Top Level Telecommunications,* 15 October 2014, updated 22 October 2014, accessed 23 October 2014, http://electrospaces.blogspot.jp/2014/10/the-german-operation-eikonal-as-part-of.htm

ンでの対象はロシアである。

なお、2013 年時点では、「ランバートＡ」計画による収集拠点は１３ヶ所あり、その内９ヶ所が運用中。その中の上位３つの拠点では、合わせて７０のケーブル或いはネットワークからデータを抽出処理しているとされる[64]。なお、収集拠点の多くは、冷戦時代に建設された衛星通信傍受ための受信基地が利用されている例が多い(事業秘匿のため）とされる。

本計画は、世界中を対象としていることから判断すると、上記（１）概要で NSA 内部資料が図示する収集拠点を紹介したが、その内、韓国やフランス収集拠点は、本計画のサード・パーティとの共同収集として設定している可能性が高いと推定できる。

なお、2013 会計年度の本計画予算は 4619 万ドルである。

（５） 単独（一方的）事業

米国外で NSA が単独に（相手国との共同事業ではなく一方的に）実施するものであり、５つの計画がある。その内３つの計画名が「ランパート I/X」「ランバート T（CLANSIG)」「ミスティック」であることは判明しているが、残り２つの計画名は不明である。

ア 「ミスティック」計画[65]

これまで記述してきた収集計画とは少し毛色が異なる興味深い計画である。

「ミスティック」は、2009 年に開始。外国政府に対して、表向きは通信事業会社の合法的な商業サービスの提供という形を採りながら、その裏で NSA が必要とするシギントデータを収集するものであり、外国政府との関係は麻薬取締局 DEA、CIA や豪信号局が仲介をしている。2013 年時点では５つの小計画が動いており、対象国はメキシコ（CIA)、ケニア（CIA)、フィリピン（豪信号局)、バハマ（DEA)、不明国の５つで、それぞれ括弧内記載の機関が関与している。

５カ国全てで、携帯電話メタデータを収集しているが、バハマと不明国では更にその国での全通話の内容も記録しており３０日間保存できるシステム（「ソマルゲット」）を構築している。このため、NSA の分析官はメタデータ分析の結果必要性を感じた場合

--Anton Geist, et.al., “NSA ‘third party’partners tap the Internet backbone in global surveillance program,” *Dagbladet Information,* 19 June 2014, accessed 23 October 2014, http://www.information.dk/print/501280.

[64] Gallagher, “How Secret Partners Expand NSA’s Surveillance Dragnet.”

[65] Ryan Devereaux., Glenn Greenwald and Laura Poitras, “Data Pirates of the Caribbean: the NSA is Recording Every Cell Phone Call in the Bahamas,” *The Intercept*, 20 May 2014, accessed 19 November 2014, https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

は、即座に関心ある通話内容を遡って確認できるので大きな成果が上がっているとされる。

バハマでの傍受設備の設置は DEA が仲介しているもので、バハマ政府が国際犯罪捜査のために設備を設置しているが、そのために契約した米国系民間通信会社が秘密裡に DEA と NSA と協力していると考えられる。

このような収集が可能となったのは、先ず、DEA の存在がある。DEA は国際的な薬物取締を任務とするため世界中に８０以上の海外事務所を展開し、諸外国の薬物取締機関と協力関係を築いている。他方、DEA は薬物取締機関であると同時に、大統領命令第 12333 号によって対外諜報の任務も有しており、当然一般インテリジェンスも収集している。次に、米国では 1994 年に「法執行のための通信支援法」が制定され、米国の通信会社は、法執行諸機関のために、効率的で且つ中央で管理する通信傍受能力を構築することが義務付けられた。これに続いて、多くの国が類似の法制度を整備したため、薬物犯罪その他国際的犯罪対策のために通信情報を収集し易くするシステムの構築が世界標準となってきたという。ところで、そのシステムを構築するには、技術力のある民間会社と傍受設備の設置維持を契約する必要があるが、契約企業が NSA の協力企業であれば秘密裡に当該国が契約していない特殊機能を構築してしまうことが可能ということであろう。

なお、「ミスティック」計画が運用されている５ヵ国中の不明国１ヶ国については、アフガニスタンと推定する分析がある[66]。アフガニスタンにおいては、携帯電話を資料源とするタリバン幹部の割出と（無人攻撃機や武装ヘリによる）攻撃によりタリバン側に大きな損害が発生しており、そのため、タリバン兵士には携帯電話を使用しないよう指示が出されていると報道されている。仮に、上記不明国がアフガニスタンであって、その携帯電話通信が全て記録されているとすれば、他のデータに加えてそのデータを使用した分析は相当効果的な筈であるから、納得のいく話である[67]。

イ　「ランバート I/X」「ランパート T」他の４計画

これら計画の内容については、資料が極めて不足しており、不分明である。

但し、４計画の内の一つが「ダンシングオアシス」計画と考えられる[68]。同計画は

---

[66] "Toward the identity of "Country X" in MTSTIC," *Cryptome* , May 2014, accessed 27 November 2014, http://cryptome.org/2014/05/nsa-mystic-identity.pdf

[67] Jacob Appelbaum, et. al., "A dubious History of Targeted Killings in Afghanistan," *Spiegel Online,* 28 December 2014, accessed 5 January 2015, http://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html

[68] "NSA's largest cable tapping program: DANCINGOASIS," *Top level Telecommunications,* 24 May 2014, updated 12 July 2014, accessed 20 October 2014, http://electrospaces.blogspot.jp/2014/05/nsas-largest-cable-tapping-program.html

2011 年に開始されたもので、西欧と極東を結ぶ基幹回線を対象としており、主たる標的はアフガニスタン、パキスタン、イラン、ヨルダンと推定されている。相当な量のデータを取得しているが、NSA はこれを回線を管理する企業の協力を得ずに行っているとされる。「ダンシングオアシス」の収集拠点は、上記（１）概要で紹介した収集拠点図示の内、アフガニスタンである可能性が高いと言えよう。

他の計画は一切不明であるが、地図の内、ジプチの収集拠点は、この単独事業である可能性がある。

なお、後述するように、アフガニスタンや中東では、米軍や CIA がドローン（無人航空機）による「テロリスト」攻撃作戦を実行しているが、それには NSA による「テロリスト」の特定と位置評定が不可欠であり、そのためにも同地域での情報収集力の強化が求められていると言えよう。

（６）まとめ

通信基幹回線からのデータ収集は、以上に述べたように、世界中からの収集であり、その内容は極めて多岐に及ぶ。

２０世紀後半の世界の通信経路の主体は、海底電線やマイクロ波通信、衛星通信であったが、２１世紀になるとインターネットの利用が急速に増大し主たる通信手段となると共に、光通信回線が通信経路の中心を占めるようにった。NSA にとって正にここがデータ収集の主戦場であり、今後も NSA は光通信基幹回線からのデータ収集能力の拡大の取組を止めることはないであろう[69]。

---

[69] “NSA also has arrangements with foreign internet providers,” *Top Level Telecommunications*.

４　愛国者法２１５条に基づくメタデータ収集

愛国者法 215 条に基づくメタデータ収集は、必ずしも主要プラットフォームとまでは言えないが、スノーデン資料に基づく告発報道の第１弾（2013 年 6 月 5 日）となるほど注目を集めたものであったので、その意味背景をここで触れておきたい。

（１） メタデータとは何か

先ず、メタデータとは何かであるが、メタデータとは、通信内容を除く通信に付随する情報の全てと定義されている。

具体的には、携帯電話通話であれば、通話当事者の電話番号、携帯端末識別番号（International Mobile Equipment Identity(IMEI) number）、利用者識別番号（International Mobile Subscriber Identity(IMSI) number シムカードに記載）、回線識別符号、通話日・時刻、通話時間、テレホンカード番号、携帯端末位置データ等である。また、インターネット通信であれば、当事者のメールアドレス、IP アドレス、通信日・時刻、通信時間、SNS 通信の通信内容以外のデータ、ネットワークに於ける活動履歴（訪問ウェブサイト、ログイン時刻、地図検索履歴等）、その他各種のデータが該当する。

メタデータの分析利用方法については後述（第 2 部第 3 章 1 メタデータ）するが、これには通信内容自体は含まれないものの、通信内容と同様に、或いは（関係者の交友関係の究明など）場合によっては通信内容以上に有用な情報資料である。それ故、NSA はメタデータ専用のデータベース（電話メタデータには「メインウェイ」、インターネット・メタデータには「マリーナ」）を構築するなど、メタデータを重視している。

（２） 愛国者法 215 条に基づく収集の意味

このようなメタデータの収集において、愛国者法 215 条が主要プラットフォームとまでは言えないという意味は、メタデータの入手経路は多様であり、愛国者 215 条はその一部に過ぎないということである。即ち、メタデータは重要であるが故に、「プリズム」計画、基幹通信回線からの収集、外国通信衛星傍受、SCS（特別収集サービス）その他、NSA の有する全てのプラットフォームにおいて収集しているのである。

他方、告発記事の第一弾となるほど注目を集めたのは、米国内で米国人を含む電話通話についてのメタデータを包括的に収集していたからである。それも、愛国者法 215 条という一見無関係とも見える条文を根拠にしていたのである。

即ち、愛国者法は 2001 年の 9/1 1 の後に対策法として急遽制定されたものであるが、愛国者法 215 条（対外諜報監視法 501 条）の趣旨は、対外諜報情報入手、或いはテロ対策と防諜のため、FBI 長官は、ビジネス記録（業務記録）がある調査(an authorized investigation)に関係する（relevant）と信じる合理的な根拠がある場合には、対外諜

報監視裁判所の令状を得て当該ビジネス記録の提出を受けることができるというものである。

この規定に基づき、FBI はテロ対策調査のため米国関連の全ての電話通話のメタデータが必要であるとして、対外諜報監視裁判所の令状を得て、電話通信事業者上位３社（ベライゾン、ATT,、スプリント三社）から、３社が保有する電話メタデータ全ての提供を（業務記録であるとの解釈で）受け、これを NSA に提供してテロ対策の分析のためのデータベースとしていたのである。

さすがの米国人もそのデータ量の膨大さと包括性には驚いて、プライバシーの侵害ではないかと注目を集めたものである。

他方、この愛国者法 215 条に基づくメタデータ収集の経緯を見ると、米国諜報機関のデータ収集にかける只ならぬ執念を感じる[70]。

（３） 愛国者法 215 条に基づく収集の経緯[71]

９/１１後、当時の NSA 長官マイケル・ヘイデンは、ブッシュ大統領からテロ対策のため情報収集の強化を命ぜられたが、その際、対策の一つに通信メタデータの利用を提案した。即ち、米国関連の電話やインターネット通信のメタデータを収集してこれを分析することにより未知のテロリストを発見しようとするものである。この提案は、大統領の承認を得て、2001 年 10 月から開始された。このために必要なデータは、従来からの国外でのシギント収集（主として SCS と衛星通信傍受）に加え、米国内の通信事業者３社の任意の協力を得て取得することとなった。

この通信事業者の協力は極めて有効であり、米国内の地域電話サービス及び携帯電話サービスの顧客は上記３社で２億人もいる。更にこの３社は長距離電話サービスでは圧倒的な占有率をもっている。スノーデン資料によれば、2003 年時点で、この３社の協力で、米国関与国際通話（通話時間）の 81%が捕捉可能であったという。一方、世界の国際電話の 20%が米国発又は米国着で、13%が米国経由、合計 33%が米国関与であったという。米国関与 33%の 81%を捕捉可能ということは、即ち、世界の国際電話の 27%が米国の民間事業者３社の協力で、捕捉できたということになる。

---

[70] 愛国者法 215 条は時限立法であり、有効期間は 2015 年 5 月末までであったが、ミュラー前 FBI 長官は、2015 年 2 月 24 日全米法律家協会の朝食会で、有効期間の延長の必要性について力説したとされる。例証として、2013 年 4 月のボストンマラソン爆弾テロ事件でも、兄弟犯人の他の共犯者の有無の解明などに効果を発揮したと述べた。
--Jana Winter, “Former FBI Director Defends Metadata Collection,” *The Intercept*, 24 February 2015, accessed 25 February 2015,
https://firstlook.org/theintercept/2015/02/24/former-fbi-director-defends-metadata-collection/

[71] これらの経緯については、次の資料が詳しい。
--ス資料 NSA, Office of the Inspector General, *ST-09-0002 Working Draft*, 24 March 2009、accessed 6 November 2014,
https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf

ところが、2005 年 12 月にニューヨークタイムズ紙が、大統領の秘密命令による情報収集の存在を暴露報道し、更に 2006 年 5 月には「USA Today」紙が、ATT、ベライゾン、ベルサウス（当時）の 3 社が電話通話メタデータを政府に提供していると暴露記事を掲載した[72]。斯かる情勢下で 3 社の任意の協力が得難くなり、米政府は新たな方法を検討し、考え出したのが愛国者法 215 条のビジネス記録としての提供命令である。米国政府の憲法解釈では、メタデータには通信内容が含まれず、通信事業者が業務の為に収集した情報であるため、そこには保護されるべきプライバシーの期待が生ぜず、従って、その収集に憲法修正第 4 条の令状主義は適用されない。そこで、収集すべき個別のメタデータを特定することなく、愛国者法 215 条の業務記録の提出として包括的に収集できるとするものである[73]。

---

[72] James Risen and Eric Lichtbblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times,* 16 December 2013, accessed 7 November 2014, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0
--Leslie Cauley, "NSA has massive database of American' phone calls," *USA TODAY,* 10 May 2013, updated 11 May 2006, accessed 7 November 2014, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

[73] US, *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act,* 9 August 2013, accessed 11 November 2014, http://big.assets.huffingtonpost.com/Section215.pdf
—公開情報 *DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents,* 31 July 2013, accessed 11 November 2014, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents.

上記文書にも記載されているように、米国の憲法修正第 4 条の適用範囲は限定されている。上記白書で政府は次のように主張している。「連邦最高裁判所の諸判決によれば、電話通話者は電話番号を通信事業者に任意に提供している。そして、電話メタデータは、通信事業者が料金徴収その他の業務目的で通常保管している情報である。そして、このように通信事業者に顧客が任意に提供した情報については、これを政府機関に提供する際に、憲法修正第 4 条の令状主義の対象には当たらない。通信事業者のデータ保管場所まで、個人のプライバシーの期待権は及ばない。」*Administration White Paper*、19-21.

また、米政府は、「愛国者法 215 条に基づくメタデータ収集は、テロ対策という限定された目的で、位置情報を除くメタデータという限定された情報を、限定された手続きで分析している。これにより仮に個人のプライバシーに最小限の影響があったとしても、テロ対策という国家安全保障上の利益と比較すれば、問題はない。」と主張している。なお、ここで言う限定された手続きとは、収集したメタデータを自由に分析しているのではなく、米国内のテロ企図者を発見するため所謂「接触連鎖分析」（contact chaining analysis）に限定して使用しているということである。即ち、既に把握しているテロリストとテロ容疑者約 300 人が、米国内の誰と連絡を取っているか、そして、米国内の連絡相手は更に誰と連絡を取り合っているかを解明するため、約 300 人の連絡先を 3 つ先（連絡先の更にその連絡先の更にその連絡先）迄に限定して、その人物たちの社会的ネットワークを把握分析するものであるという。

但し、3 つ先迄の連絡先を取れば、実は相当広範囲に及び得るのである。また、これらの制約は、愛国者法 215 条に基づくメタデータ収集に適用されるだけであり、実は、メタデータ収集はこれ以外の法的位置付けによる収集が多くあることを忘れるべきではない。

2006 年以降、この解釈に従い、愛国者法 215 条を根拠に、対外諜報監視裁判所の令状を得て、通信３社（ベルサウスは ATT に吸収され、現在は、ATT、ベライゾン、スプリント３社と言われる）から電話メタデータを収集していた。収集しているデータは、メタデータの全てではなく、位置情報は取得していないとしている[74・75]。

なお、電話メタデータの他、嘗ては、対外諜報監視法 402 条の規定に基づき、インターネット・メタデータも収集していたが、2011 年に停止されている。その理由は、継続するだけの価値がないということであるが、インターネット・メタデータ分析自体の価値は、NSA がそのための特別のデータベースを構築している程であるので、疑いがないところである。従って、この停止は、他の方法（「プリズム」計画、基幹通信回線からの収集その他）によるインターネット・メタデータの収集と対比して、相対的な価値が低下したということであろう[76]。

（４）連邦控訴裁判所による違法判決

ところで、愛国者法 215 条のビジネス記録（業務記録）の提出の解釈としても、テロ対策上の「ある調査(an authorized investigation)に関係する」として米国内の全て

74　上記註の *Metadata Collection Documents* によれば、収集対象データは、通話当事者の電話番号、携帯端末識別番号（IMEI）、利用者識別番号（IMSI）、回線識別符号、通話日・時刻、通話時間、テレホンカード番号他である。2005 年時点では位置情報（cell site location data）も含んでいたが、上記の公開文書 *Administration White Paper* では位置情報の取得を否定している。アレキサンダーNSA 長官（当時）は、2013 年 7 月 25 日には「位置情報を入手していない」と発言（過去については言及せず）。また、同年 9 月には「愛国者法に基づいては位置情報を入手していない」と発言している。位置情報の重要性に鑑みれば、憲法解釈上の問題から、愛国者法 215 条に基づく位置情報収集は中止したが、大統領命令 12333 号その他の権限に基づく位置情報収集は中止していないということである。

75 愛国者法 215 条による電話メタデータ収集で、実際に米国関連通話のどれだけを収集しているかは、明確ではない。2014 年 2 月 8 日付ワシントンポスト記事によれば、2006 年当時は米国通話のほぼ 100%のメタデータを収集できていたが、2013 年夏の時点では 30%以下に落ちており、政府はその回復に努めているという。収集比率の低下の理由は明確ではないが、インターネット回線利用通話の増加、データ処理等収集技術の問題、スノーデン告発による担当者の多忙などが考えられるとしている。

--Ellen Nakashima, “NSA is collecting less than 30 percent of U.S. call data, officials say,” *The Washington Post*, 8 February 2014, accessed 10 February 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.

76　Office of DNI, “Newly Declassified Documents Regarding the Now-Discontinued NSA Bulk Electronic Communications Metadata Pursuant to Section 402 of the Foreign Intelligence Surveillance Act,” 11 August 2014, accessed 6 September 2014, http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1099-newly-declassified-documents-regarding-the-now-discontinued-nsa-bulk-electronic-communications-metadata-pursuant-to-section-401-of-the-foreign-intelligence-surveillance-act

の電話メタデータの提供を求めるのは、余りにも広汎である。そのため、愛国者法の主たる提案者であった下院議員のセンセンブレンナー議員ですら、スノーデン告発でその存在を知って、想像もしていなかった運用であると驚いた程であった。

そのため、NGO 団体のアメリカ市民自由連合（American Civil Liberties Union）がその停止を求めて提訴した。連邦第二巡回控訴裁判所は、2015 年 5 月 7 日判決を下し、憲法判断までは至らなかったが、本件のような包括的収集は調査（又は捜査）との関係性が不十分で、愛国者法 215 条で許された範囲を超える違法収集であると判断して、審理を地区裁判所に差し戻した[77]。

（5）愛国者法 215 条の改正（2015 年 6 月）[78]

愛国者法 215 条は 2015 年 5 月末までの時限法であったが、2015 年 6 月 2 日米国自由法が制定されて、有効期間が延長されると共に、その内容が改正された。

それによれば、愛国者法 215 条では、FBI が米国で電話メタデータやインターネット・メタデータを包括的に収集することは禁止された。これに代えて、FBI 長官はテロ対策においては対象者を特定して、対外諜報監視裁判所の令状を得て、この者と二つ先の連絡者（連絡先の更に連絡先まで）の間の電話メタデータを取得できることとされた。令状は 1 回最長 180 日間有効であり、この間通信事業者は令状に係る電話メタデータを毎日提供する義務を負う（米国自由法 101 条）。対象となる電話メタデータには、通話当事者の電話番号、携帯端末識別番号、利用者識別番号、通話日・時刻、通話時間、テレホンカード番号が含まれるが、携帯端末位置データは含まれない。なお、緊急時には、司法長官は裁判所の令状を得るまで 7 日間に限りビジネス記録の提供を要求することもできることとされた（同法 102 条）。

本改正案は、諜報機関、自由主義運動家や通信事業者も関与して作成され、オバマ大統領も賛成しているものであり、NSA のデータ収集能力全体に大きな変更をもたらすものではない。実際、元 NSA 長官のマイケル・ヘイデン氏は、本改革について、2015 年 6 月ウォールストリート・ジャーナル誌主催の会合で、愛国者法 215 条による収集は小さなもの（that little 215 program）で、この改革は問題ない（Cool!）と

---

[77] Dan Froomkin, “NSA’s Bulk Collection of Phone Records is Illegal, Appeals Court Says,” *The Intercept,* 7 May 2015, accessed 18 May 2015, https://firstlook.org/theintercept/2015/05/07/appellate-court-rules-nsas-bulk-collection-phone-records-illegal/
--AP, “5 Things to Know About the NSA Court Ruling,” *The New York Times*, 8 May 2015, accessed 18 May 2015, http://www.nwitimes.com/news/national/things-to-know-about-the-nsa-court-ruling/article_29b110b2-b8b7-5044-88af-fcaf60c7782f.html

[78] USA Freedom Act（Summary and Text）, accessed 3 June 2015, https://www.congress.gov/bill/113th-congress/house-bill/3361
--Mike DeBonis, "Congress turns away from post-9/11 law, retooling U.S. surveillance powers,” *The Washington Post*, 2 June 2015, accessed 3 June 2015, http://www.washingtonpost.com/politics/senate-moves-ahead-with-retooling-of-us-surveillance-powers/2015/06/02/28f5e1ce-092d-11e5-a7ad-b430fc1d3f5c_story.html

述べている[79]。

[79] Michael Hayden, "Former NSA Chief Michael Hayden on Edward Snowden's leaking of classified information," *WST Video News*, June 2015, accessed 19 June 2015, https://screen.yahoo.com/former-nsa-head-hayden-snowdens-020710743.html

５　外国衛星通信の傍受[80]

衛星通信の傍受は、海底電線やマイクロ波の傍受と並んで、２０世紀からシギント情報の主要な収集プラットフォームであったが、２１世紀のインターネット時代にあっても依然として主要プラットフォームの地位を維持している。NSA の収集拠点は、大規模な傍受施設で収集する主要傍受施設、及び後述する秘密の特別収集サービス（SCS）拠点の二つの類型がある。

なお、「外国」衛星通信の傍受とは、「外国通信」（少なくとも一方当事者が国外）の傍受を示すものであり、必ずしも「外国衛星」の通信傍受を意味するものではないと考える。

（１） 主要傍受施設　約１２ヶ所

2012 年の NSA 内部資料によれば、主要な傍受施設は１２あるとしている。但し、図示されている拠点は６ヶ所、コード名が示されているのは１０ヶ所しかない。当該資料を合理的に解釈すると、１２ヶ所の傍受施設の国名とコード名は次の通り。

米本土	ヴァージニア州シュガー・グローブ	「ティンバーリン」
	ワシントン州ヤキマ	「ジャックナイフ」
欧州	英国メンウィズ・ヒル	「ムーンペニー」
	英国バッド	「カーボーイ」
	デンマーク　Skibsbylejren	「コード名不明」
中東	キプロス（英国海外領土）アイオス・ニコラオス	「サウンダー」
	オマーン	「スニック」
アジア	日本・三沢	「レディーラブ」
	フィリピン	「コード名不明」
	タイ・コンケン	「インドラ」
大洋州	豪州・ジェラルドトン	「ステラー」
	ニュージーランド・ワイホパイ	「アイロンサンド」

これらの施設は、NSA が単独で運営しているか、セカンド・パーティ諸国に所在する拠点の場合は共同で運用している施設もあると推定される。

なお、2012 年の資料を 2002 年の内部資料と対比すると、４つの施設が欠落している。それは、先ず、プエルトリコ・サベナシーとケニア・ナイロビの２つである。これ

80　主要参考文献は次の通り。
--Greenwald, *No Place,* 117.
--“NSA’s global interception network,” *Top Level Telecommunications*,.
--“The National Security Agency in 2002,” *Top Level Telecommunications*, 3 July 2014, accessed 26 September 2014, http://electrospaces.blogspot.jp/2014/07/the-national-security-agency-in-2002.html

らは閉鎖された可能性が高いとされる。次に、ドイツ・ミュンヘン市南東のバードアイブリングの施設である。これは 2004 年に NSA の施設としては閉鎖されたが、ドイツに引き渡された。従って、現在 NSA の施設としては位置付けられていないが、ドイツ当局 BND による収集データはサード・パーティ情報として相当部分が NSA に提供されていると考えられる。最後に、オーストラリアのダーウィンの施設（コード名「ショアルベイ」）がある。これは現在も運用されていると見られるが、2012 年資料では記述がない。可能性としては、ドイツの施設と同様、その運営が完全にオーストラリアに移管されたか、或いは単純に記載をしなかったか、何れかと考えられるが、後者の可能性が高い。従って、NSA の衛星通信の主要傍受施設には、世界中に１２ヶ所ではなく、１３ヶ所あることになる[81]。

なお、これら収集に掛かる費用は、2013 会計年度予算 FORNSAT では 8133 万ドルである[82]。

（２） 特別収集サービス（SCS）　約４０ヶ所

NSA は CIA との共同作戦として、世界中の米国大使館や領事館８０ヶ所以上にシギントの収集拠点を置いている。それらの８０ヶ所以上の収集拠点のうち、約４０ヶ所には衛星通信の傍受設備を秘密裡に設置しているという。

なお、2002 年の内部資料で SCS であって外国衛星通信の傍受拠点として具体名が示されているのは、インドのニューデリーとブラジルのブラジリアの２ヶ所であった。

ここで設置しているアンテナは、秘匿して設置する都合上、先に述べた（１）主要傍受施設のアンテナと比較して相当小型のものを開発していると考えられる。

81　NSA とセカンド・パーティ諸国との密接な協力関係から考えると、オーストラリアのダーウィンの拠点が完全にオーストラリアの運営に委ねられたと考えるのは、若干の無理があると考える。

なお、オーストラリアには他にパインギャップに衛星通信用の基地があり、これは基本的には米国が保有するシギント「衛星」の運用基地とされている。

--Duncan Campbell, “Australia first to admit ‘we’re part of a global surveillance system,” *Heise Online,* 28 May 1999, accessed 13 February 2015, http://www.heise.de/tp/artikel/2/2889/1.html

82　ス資料 *FY2013 Congressional Budget Justification Vol. I : National Intelligence Program Summary*, February 2012, 159. accessed 20 August 2014, http://fas.org/irp/budget/nip-fy2013.pdf

６　特別収集サービス（SCS）

（１） 概要[83]

特別収集サービス（SCS）は、NSA と CIA の共同事業で３０年以上の歴史がある。SCS 発足以前は、一方で NSA は大使館を拠点に独自のシギント活動を行い、他方 CIA も大使館を拠点に盗聴器を使用するなどして技術的情報収集を行っていた。しかし、これでは生産的でないとして、1970 年代末に両者の機能を統合して、SCS を設置したという[84]。

現在、SCS 本部はメリーランド州ベルツビルにある。世界中の米国大使館、領事館、利益代表部等の外交施設８０ヶ所以上に、「ステートルーム（特別室）」という暗号名の拠点を設置している。拠点では、建物の屋上や上層階に（電波透過率の高い）ポリエチレンやセラミックで作った偽装工作物を設置して、その中に各種の高性能アンテナを秘匿設置すると共に、建物内にはデータ処理や分析のための部屋を確保している。但し、このステートルームの活動は極秘事項であり、大使館等の他の大多数の職員に対しては秘匿されている。

アクセスしている電波は、マイクロ波、WiFi や WiMAX などの無線 LAN、GSM, CDMA などの携帯電話通信、衛星通信など多様である。

メリーランド州の本部には、大使館を模した建物が設置されており、訓練施設を兼ねていると推定できる。また、「ステートルーム」の技術支援施設が、英国クロフトンの米空軍基地内とタイ国バンコックにある施設に置かれており、世界中の拠点に対する技術支援の前線拠点となっている。SCS のトップは、NSA と CIA が交代で出しているという。

なお、2013 会計年度の SCS 予算は、NSA2 億 4909 万ドル、CIA1 億 576 万ドル、合計 3 億 5485 万ドルである。

SCS は、単に NSA と CIA の共同事業というだけではなく、他の多様な機関と戦略

83　主要参考文献は次の通り。
--Von Konrad Lischka and Matthias Kremp, “So functionieren die Abhoeranlagen in US-Botschaften,” *Spiegel Online*, 28 October 2013, accessed 12 November 2013, http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehskandal-so-funktionieren-die-abhoeranlagen-in-us-botschaften-a-930392.html
--ス資料 *Special Collection Service: Pacific SIGDEV Conference March 2011,* accessed 5 November 2014, http://www.spiegel.de/media/media-34100.pdf
--Greenwald, *No Place,* 117.
--“NSA’s global interception network,” *Top Level Telecommunications*,.

84 Jason Vest and Wayne Madsen,　”CIA/NSA Special Collection Service,” *CRYPTOME*, 13 May 2002, accessed 31 October 2014, http://cryptome.org/eyeball/scs/scs-eyeball.htm
但し、「８の秘匿シギント(CLANSIG)」で述べるが、この SCS に統合されていない NSA と CIA のそれぞれの秘匿シギント活動が依然として存在すると見られる。

的協力関係にあるとされており、協力の詳細は不明であるが、その予算額の多さとも相俟って、米国諜報コミュニティにおいて相当重要な位置付けをされているのではないかと、推定される。協力関係にある機関は、国務省、FBI、シークレットサービス、国家偵察局 NRO、国防諜報庁 DIA、更には、NSA 内の SSO、TAO、CLANSIG、それにセカンド・パーティ諸国等である。

セカンド・パーティ諸国（英国、カナダ、豪州、ニュージーランド）との協力においては、これら４カ国も大使館等に収集拠点を設置しており、これらの拠点も「ステートルーム」と呼ばれる。実際は、５カ国の大使館、領事館などがそれぞれの地の利を生かして共同して活動していると考えられる。後述するが、ベルリンでも英米両国の大使館はデータ収集の適地に位置しており、その屋上に設置された工作物の形状から判断しても、共同していたことが伺われる。

（２） SCS の特性と利点

NSA の 2011 年 3 月付の内部資料[85]によれば、SCS 活動は次のような利点を有する極めて独特なシギントのプラットフォームであるとしている。

- 地理的利点：他国という敵対的な空間でありながら、米外交施設というホームフィールドで活動できる。また、顧客に近いところで活動できる。
- 信号アクセスの利点：マイクロ波、衛星通信、携帯電話通信、無線 LAN など多様な信号にアクセスして、受動的（passive）なデータ収集の他、積極的(active)なシステムへの浸透とデータ取得が可能。
- 分析の利点：通信インフラやシステム構成などの把握、標的設定や標的の行動の把握が容易なこと。
- 情報成果の利点：国家的需要と共に地域的な需要に応えることができる。現地に対する背景知識、現地情勢や状況変化を踏まえた情報成果を提供できる。

これらの記述から推定できるのは、大使館等に駐在して任国情勢を熟知した分析官が、シギント資料を得てより実態に迫る正確な情勢分析を行い、米本国の大統領以下の国家的情報需要に応えると共に、駐在大使への情勢報告にも活用されている姿である。また、内部資料には、「シギントを進めるヒューミント、ヒューミントを進めるシギント」という標語も掲げられている。これは、一方で、例えば外交官や CIA 要員が傍受すべき携帯電話番号を収集するなどして、シギントの資料源開拓にヒューミントが貢献し、他方、シギントで得た情報を利用してヒューミント(例えば協力者獲得工作)を行うなど、シギントとヒューミントの密接な協力関係の存在を伺わせるものである。

（３） 特別収集サービスの収集拠点名

2012 年の NSA 内部資料には、拠点名８８ヶ所（支援施設を含む）と地図上の印が

[85] ス資料 *Special Collection Service: Pacific SIGDEV Conference March 2011.*

多数示されているが、拠点名は４６ヶ所が黒塗りにされており判読できない[86]。

これに対して、2010 年 8 月時点の NSA 内部資料によれば、その時点で、人員配置のある拠点７４ヶ所、遠隔操作で人員配置の無い拠点１４ヶ所、休止中３ヶ所、技術支援拠点２ヶ所が示されている[87]。一部判読出来ない部分もあるが、2012 年資料とも対比して検討すると、2010 年から 2012 年に運用中の収集拠点（遠隔操作を含む）は、概ね次の通りと推定できる。

ア　欧州　　２３ヶ所（内４ヶ所は遠隔収集）

独（ベルリン、フランクフルト）、仏（パリ）、伊（ローマ、ミラノ；後者は遠隔収集）、スペイン（マドリッド）、スイス（ジュネーブ）、オーストリア（ウィーン、別館；後者は遠隔）、チェコ（プラハ）、ハンガリー（ブダペスト）、ブルガリア（ソフィア）、

露（モスクワ、別館；後者は遠隔）、ウクライナ（キエフ）、アゼルバイジャン（バクー）、ジョージア（トビリシ）

クロアチア（ザグレブ）、ボスニア・ヘルツェゴビナ（サラエボ）、コソボ（プリシュティナ）、ギリシャ（アテネ、別館；後者は遠隔）、アルバニア（ティラナ；2010 年は休止中で 2012 年には活動再開）

イ　中東　　１９ヶ所（内３ヶ所は遠隔収集）

トルコ（アンカラ、イスタンブール）、イラク（バグダッド、スレイマニア、キルクーク、アマーラ、バスラ；後三者は遠隔収集）、シリア（ダマスカス）、ヨルダン（アンマン）、レバノン（ベイルート）、サウジアラビア（リヤド、ジェッダ）、クウェート（クウェートシティ）、UAE（アブダビ）、バハレーン（マナーマ）、イエメン（サナア）　他３ヶ所

ウ　アフリカ　　１０ヶ所（内１ヶ所は遠隔収集）

エジプト（カイロ）、リビア（トリポリ）、アルジェリア（アルジェ）、スーダン（ハルツーム）、エチオピア（アディスアベバ）、ケニア（ナイロビ）、ザンビア（ルサカ）、コンゴ（キンサシャ）、ナイジェリア（アブジャ、ラゴス；後者は遠隔）、他に２０１２年に休止中２ヶ所リベリア（モンロビア）とアンゴラ（ルアンダ）

エ　南アジア　　８ヶ所（内１箇所は遠隔収集）

パキスタン（イスラマバード、カラチ、ラホール、ペシャワール）、インド（ニューデリー）、アフガニスタン（カブール、カブール別館、ヘラート；カブール別館は遠隔）

オ　東アジア　　１２ヶ所（内１ヶ所は遠隔収集）

---

86 Greenwald, *No Place,* 117.

87 “Special Collection Service slides,” *Duncan Campbell.Org*, (undated), accessed 27 October 2014, http://www.duncancampbell.org/content/special-collection-service-slides

中国（北京、上海、成都）、香港、台湾（台北）、フィリピン（マニラ）、インドネシア（ジャカルタ）、マレーシア（クアラルンプール）、タイ（バンコック、チェンマイ（後者は遠隔））、カンボジア（プノンペン）、ミャンマー（ラングーン）

カ　中南米　　１６ヶ所（内４ヶ所は遠隔収集）

メキシコ（メキシコシティー、グアダラハラ、モントレー、メリダ、エルモシージョ；後四者は遠隔収集）、グアテマラ（グアテマラシティー）、ホンジュラス（テグシガルパ）、ニカラグア（マナグア）、コスタリカ（サンホセ）、パナマ（パナマシティー）、キューバ（ハバナ）

ベネズエラ（カラカス）、コロンビア（ボゴタ）、エクアドル（キト）、ボリビア（ラパス）、ブラジル（ブラジリア）

○　注目点

これらのSCS収集拠点を見ると、概ね米国の情報関心が高い諸国と目されるが、注目されるのは日本にSCS収集拠点がないことである。日本に収集標的にする価値がないとは到底考えられないのであるから、理由として考えられるのは次の二つであろう。第１に、在東京の米国大使館が収集拠点として好ましくない可能性が考えられる。米国大使館の周囲には、現在、高層民間ビルが相当数建てられており、ベルリンの米国大使館などと比較すると収集拠点として適地でないことは明らかである。第２の理由は、米国大使館にわざわざSCS収集拠点を構えなくても、他に（他のUKUSA諸国による収集も含めて）十分なシギント情報入手手段が確保されている可能性が考えられる。この二つの要因が相俟って、大使館内にSCS収集拠点を設置していないのではないだろうか[88]。

（４）米独関係への波紋

SCSについては、2013年秋にドイツ誌のシュピーゲルがメルケル首相の携帯電話の傍受を取り上げて大々的に報道したため、これに対するメルケル首相の対応が注目された。

そもそも、メルケル氏は「携帯首相」と渾名される程、携帯電話を多用する政治家であり、所属政党支給の携帯電話と政府支給の両者を使用している。政党支給の携帯電話には暗号機能がなく、他方、政府支給の携帯電話は2009年には暗号付携帯電話を採用。

88　蛇足ながら、我が国では、例えばマスメディアの政治部が有力政治家の担当（番記者）を決め、各社の番記者は共同して有力政治家の一日の言動をまとめていると承知しているが、この「まとめ」は通常の国家であれば機密情報にも相当するものが含まれていると思われる。これらの情報が外部（況して外国の政府職員）に漏洩しないように確実なデータ管理がなされているのであろうか。筆者が、嘗て某政治部記者に聞いた限りでは、そのような厳密な管理はなされていないということであった。

更に2013年3月にはこれを更新し、閣僚や高級官僚5000人以上に配布したとされる[89]。

ところが、独誌シュピーゲルが、NSA 内部資料を分析して、メルケル女史の携帯電話番号が収集標的として記載され、且つ、その任務が SCS に付与されているのを発見。同誌は2013年10月10日これを首相府に通告。独政府は、諜報機関による調査を行い、これを真実であると判断した。独首相府は米ホワイトハウスと遣り取りをしたが、必ずしも満足いく結果を得られなかったという。そこで、メルケル首相は 10 月 23 日にオバマ大統領に直接電話をし、信頼関係の大きな侵害であると抗議し、且つ、諸諜報機関の活動と協力関係について明確な相互取決を定めるよう要求した。これに対し、オバマ大統領は、「メルケル氏の携帯電話傍受は知らなかった。知っていればさせなかった。現在、メルケル氏の電話は傍受されていないし、将来も傍受することはない。」旨応えたと報道されている[90、91]。

---

[89] Jacob Appelbaum, et. al., "Did US Tap Chancellor Merkel's Mobile Phone?" *Spiegel Online,* 23 October 2013, accessed 24 October 2013,
http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html 及び
--Philip Oltermann, "Merkel spying claims: the 'mobile chancellor'," *The Guardian,* 23 October 2013, accessed 24 October 2013,
http://www.theguardian.com/world/2013/oct/23/merkel-phone-mobile-chancellor.及び
--"How secure is the Merkel-Phone," *Top Level Telecommunications*, 25 October 2013, updated 28 October 2013, accessed 7 November 2014,
http://electrospaces.blogspot.jp/2013_10_01_archive.html
メルケル氏が使用する政党支給の携帯電話はボーダフォン製でこの傍受は通信内容を含めて容易であるとされる。他方、2009 年に導入した政府携帯電話はノキア製でドイツ企業 Secusmart 社の暗号チップを挿入（但し 2010 年迄は暗号は音声通話のみ）。2013 年に導入した携帯電話は、ブラックベリー社の携帯電話に同じく Secusmart 社の暗号チップを挿入したものという。この暗号の強度はそれ程高くない(暗号鍵は 128 ビット)と言われているが、NSA がこの暗号まで解読していたか否かは明らかではない。
--Ian Traynor, Philip Oltermann and Paul Lewis, "Angela Merkel's call to Obama: are you bugging my mobile phone?" *The Guardian*, 24 October 2013, accessed 24 October 2013,
http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german
[90] "NSA-Überwachung: Merkels Handy steht seit 2002 auf US-Abhörliste," *Spiegel Online*, 26 October 2013, accessed 27 October 2013,
http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html
--"The NSA's Secret Spy Hub in Berlin," *Spiegel Online,* 27 October 2013, accessed 28 October 2013,
http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html
[91] なお、元 NSA 長官のマイケル・ヘイデン氏は、シュピーゲル誌のインタヴューに答えて、オバマ大統領はメルケル氏の携帯電話傍受を知っていた事を示唆する発言をしている。
--Michael Hayden, interview by Marc Hujer and Holger Stark, *Spiegel Online,* 24 March 2014, accessed 31 March 2014,

なお、ベルリンの米英両大使館はベルリン官庁街に位置して連邦首相府や連邦議会は指呼の間にあり、且つ公園を挟んで見通せる空間環境にある。通信傍受には最適な位置である。そして、その屋上には受信装置を格納していると推定される構造物が設置されているのが明確に識別できる。本件が大きく報道されて後（2013 年 11 月頃の時点）、米大使館屋上の構造物の表面温度が大幅に低下しており、構造物内部での活動が停止されたのではないかと報道されている[92]。また、英国大使館屋上の構造物は、2014 年 7 月までに撤去されたと報道されている[93]。

（５）補足

SCS のように外交施設に於いてシギント活動を行うのは、そのために無線電波を発信していれば外交関係に関するジュネーブ条約に違反し、そうでなくても国際礼譲に反すると考えられるが、実際は、このような活動は広く行われてきたようである。過去に報道されたところでは、例えば、米ソ冷戦時代の 1971 年には、米英両国が協力して在

---

http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389.html

ヘイデン氏は次のように述べている。「我が政府が大統領は知らなかったと明確にしている。また、大統領が知らなかったと言っている以上、大統領は知らなかったのだと私は言おう。しかし、ホワイトハウスが知らなかったというのは、本当とは思えない。国家安全保障会議が知らなかったというのも、本当とは思えない。しかし、大統領が知らなかったというのは大統領の個人的な意思決定ではない。」

そもそも、既述したように、オバマ大統領は「諜報機関というものはすべて、・・・各国の首都で何が起きているかを理解しようとしている。それをしないようであれば、諜報機関としての価値はない。」と述べている。また、2007 年のシギント「戦略的任務リスト」には、主要任務として外交政策の標的国としてドイツが中国、ロシア、フランスに次ぐ４番目に位置付けられているが、ドイツの外交政策の主宰者は当然のことながらメルケル首相である。そして、米大統領は毎朝世界の情勢報告を受けており、その中にはドイツとメルケル首相の外交政策に関する「ディープ」な情報が含まれていた筈である。そして、その「ディープ」な情報の信頼性を評価するためにも、概ねの情報源を理解していた筈である。とすれば、オバマ大統領がメルケル首相の携帯電話の傍受を知らなかったと述べるのは、諜報機関の責任者からすれば、単なる言い逃れにしか聞こえないであろう。筆者には、上記ヘイデン元 NSA 長官の発言は（元政府高官の発言として許されるギリギリの）オバマ大統領とそのスタッフに対する抗議のように聞こえるが、如何であろうか。

なお、後述するが（第３部第２章３（４）オ及び第３章２（２）ウ）、政府高官用の「世界シギント・ハイライト」（Global SIGINT Highlights）幹部版（Executive Edition）には、情報内容から判断して明らかに資料源がドイツ首相やフランス大統領の電話会話と推定できる情報も掲載されていた。

[92] Duncan Campbell, “British embassy spying,” *Duncan Campbell. Org,* undated, accessed 27 October 2014, http://www.duncancampbell.org/british-embassy-spying

[93] Melanie Amann, et. al., “Keeping Spies Out: German Ratchets Up Counterintelligence Measures,” *Spiegel Online*, 22 July 2014, accessed 23 July 2014, http://www.spiegel.de/international/world/germany-increases-counterintelligence-in-response-to-us-spying-a-982135.html

モスクワ大使館からソ連指導者の公用リムジン車からの無線通信を傍受していたことが暴露され、ソ連当局は対抗措置として両大使館に対して強力な妨害電波を照射したとされる[94]。

他方、米国の首都ワシントン初め米国各地でも、ソ連と他の共産圏諸国は大使館や領事館から通信電波の収集に努めていたとされる。NSA の公式「60 年史」によれば、ソ連及びその衛星諸国は、大使館や領事館を拠点にして米国内のマイクロ波通信を傍受していたため、1970 年代後半に、秘匿すべき政府通信は、マイクロ波通信を地上回線に移行させ、或は、マイクロ波回線の使用を継続する場合には回線全体に暗号を掛けて対抗したという[95]。なお、現在でも、例えばベルリンでは、ロシア大使館の屋上には秘密の電波受信装置と目される構造物が見られるといわれる[96]。

---

[94] Duncan Campbell, et. al., "Revealed: Britain's 'secret listening post in the heart of Berlin'," *The Independent,* 5 November 2013, accessed 5 November 2014, http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html

[95] US NSA, *NSA 60 Years of Defending Our Nation*, 3, accessed 1 September 2014, https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf.

[96] Joerg Diehl, "Berlin Makes Easy Target for Spies," *Spiegel Online*, 21 November 2013, accessed 20 December 2013, http://www.spiegel.de/international/germany/spying-believed-to-rampant-in-the-german-capital-a-934759.html

7 CNE（コンピュータ・ネットワーク開拓（システムやデータ資源開拓））

コンピュータ・ネットワーク資源開拓(Computer Network Exploitation)とは、一言でいえばハッキングによってコンピュータ・ネットワークに侵入し、システム資源やデータ資源を開拓することである[97]。手法としては、遠隔地からインターネット網を介して行う侵入(remote access)と近くからの直接的な侵入(close access)の二つの手法がある。その担い手は、NSA の中の TAO グループであるが、必要に応じて CIA や FBI その他の機関の協力を得るという。また、米国内外の企業とも協力しているとされる。

（1）TAO（Tailored Access Operation）とその成果[98]

TAO は 1997 年発足で、NSA の本部フォート・ミードの他、NSA の四つの地方本部（ハワイ州ワヒアワ、テキサス州サンアントニオ、ジョージア州フォート・ゴードン、コロラド州バックリー）に支部を置く。その他、ドイツ・フランクフルト近郊グリースハイムの欧州シギント・センター(European Security Center)にも事務所を置いている。人員は急速に増加しており、2013 年度会計予算では 1870 人である[99]。

TAO の内部構成は、作戦に必要なソフトウェアやハードウェアの開発部門（ANT、DNT、TNT）、作戦の実施部門（ROC、AT&O）、作戦の企画調整を行う部門（R&T）、

---

[97] 厳密に言えば、コンピュータ・ネットワーク開拓 CNE は、次の二つの類型の活動に分類される。①標的とするコンピュータ・システムから情報データを取得する活動（collection activities）、②標的とするコンピュータ・システムへのアクセスを獲得し促進する活動（enabling activities）である。②は①のための前提作業である場合の他、コンピュータ・ネットワーク攻撃 CNA の前提作業である場合も含まれる。本節では②についての記述が中心となる。
--ス資料、NSA, Office of General Counsel, “CNO Legal Authorities,” circa 2010, p.8, accessed 8 June 2015,
https://www.documentcloud.org/documents/2092794-document-cyber-surveillance-documents.html#document/p9 参照。

[98] 主な資料は次の通り。
---Jacob Appelbaum, et. al., “Documents Reveal Top NSA Hacking Unit,” *Spiegel Online*, 29 December 2013, accessed 20 January 2014,
http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
---Barton Gellman and Ellen Nakashima, “U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show,” *The Washington Post,* 31 August 2013, accessed 18 November 2013,
http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

[99] ス資料 ”Excerpt from the secret NSA budget on computer network operations / Code word GENIE,” *Spiegel Online*, 17 January 2015, accessed 19 January 2015,
http://www.spiegel.de/media/media-35660.pdf

そして作戦を支えるネットワーク・インフラ部門（MIT）の４部門からなっている[100]。

その技術は極めて高いとされ、NSA 内部資料の中でも TAO のメンバーが、「デフコン」や「ブラックハット」などハッカーが集まる会合に参加しても技術的に得る所はないと豪語している[101]。

予算は「ジェニー」というコード名で計上されており、2013 会計年度予算は 6 億 5200 万ドルと巨額に上っている。（また、マルウェア等は後述するように基本的には NSA で内製しているが、それでも、補足的に主として西欧の闇市場からウィルスやシステム侵入プログラムを購入する予算が 2510 万ドル程ある。）

成果としては、各種システムに対する NSA の操作可能なマルウェアの累計注入件数(implants)が、2008 年では 2 万 1252 件、2011 年では 6 万 8975 件であるが、それを運用する人員不足で実際に運用できているのは 2011 年で 8448 件に過ぎないという。マルウェアの累計注入件数は 2013 年度会計年度中には 8 万 5 千から 9 万 6 千件に及ぶ見込み（その内運用予定は 9 千件から 1 万件）であり、操作員不要の自動運用システムを開発中であるという[102]。

運用の効率化の一例としては、2013 会計年度は、侵入したネットワークの通信の中から、特定者の音声を検知して自動的に抽出して送信するソフトウェアを開発中であったとされる。

なお、TAO は単にデータ収集を担当するだけではなく、サイバー防衛、サイバー攻撃にも関与している。2011 年には攻撃的工作を 231 件実施したが、その内 4 分の 3 は優先目標であるイラン、ロシア、中国、北朝鮮等に対するものであったという。攻撃的工作の多くは、システムを破壊するというよりは、システム上のデータやシステムの機能に悪影響を与えるものであったという[103]。

但し、アレクサンダー前 NSA 長官は、2013 年秋のインタビューで、８年に及ぶ任期中に実施した攻撃作戦は、数える程（only a handful of times）しかないと述べてい

---

[100] ス資料　“Interview with an employee of NSA's department for Tailored Access Operations about his field of work,” *Spiegel Online,* 17 January 2015, accessed 19 January 2015,　http://www.spiegel.de/media/media-35655.pdf
-- ス資料　*NIOC Maryland Advanced Computer Network Operations Course,*　undated, accessed 19 January 2015,　http://www.spiegel.de/media/media-35657.pd

[101] Ryan Gallagher and Peter Maass, “Inside the NSA’s Secret Efforts to Hunt and Hack System Administrators,” *The Intercept,* 20 March 2014, accessed 1 December 2014, https://firstlook.org/theintercept/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

[102] ス資料 ”Excerpt from the secret NSA budget on computer network operations / Code word GENIE,” *Spiegel Online.*

[103] 攻撃的作戦とは、コンピュータやコンピュータ・ネットワーク自体、或はそれらに存在するデータを操作し、妨害し、破壊する等の作戦であり、2010 年には 279 件を実施したという

る[104]。同元長官の言う数える程の攻撃作戦とは、作戦の内でも「破壊的な」攻撃に限定していると推定される。

（２）遠隔侵入(remote subversion, remote access)

遠隔進入は、ネット侵入(On-net)、ソフトウェア注入(software implant)等とも呼ばれる。担当は、遠隔作戦センター（ROC：Remote Operations Center）である。ROCのモットーは、「君らのデータは我らのデータ、君らの機器は我らの機器。何時でも、何処でも、どんな手を使っても。」（Your data is our data, your equipment is our equipment – anytime, any place, by any legal means.）[105]であり、正にその任務を象徴している。

嘗ては、NSA もマルウェアを仕込んだスパムメールの送付を主軸としていたようであるが、その成功の確率が極めて低くなり、今や成功率は１％にも満たないとされる。そのため、現在では、コード名「クオンタム」計画という「側面者攻撃」(man on the side attack)が中心であり、その他「中間者攻撃」(man in the middle attack)他の侵入方法もとっている。そこで、次に①「クオンタム」計画、②その成功例、更に③その他の侵入方法に分けて記述したい。

なお、NSA 内部資料によれば、「基本は、何らかのウェブブラウザーによって標的に我々（NSA の偽装サイト）を訪問させること。これが出来れば、標的を支配することが出来るのであり、問題はどうやって誘い込むかである」としている[106]。

ア「クオンタム」計画[107]

---

[104] David E Sanger, “Syria War Stirs New U.S. Debate on Cyberattacks,” The New York Times, 24 February 2014, accessed 25 November 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0
--David E Sanger and Thom Shanker, “N.S.A. Director Firmly Defends Surveillance Efforts,” The New York Times, 12 October 2013, accessed 9 February 2015, http://www.nytimes.com/2013/10/13/us/nsa-director-gives-firm-and-broad-defense-of-surveillance-efforts.html?pagewanted=all

[105] ス資料、NSA, ROC, *The ROC: NSA’s Epicenter for Computer Network Operations* (6 September 2006), accessed 20 February 2015, http://www.spiegel.de/media/media-35654.pdf

[106] “NSA Phishing Tactics and the Man in the Middle Attacks,” *The Intercept,* 12 March 2014, accessed 1 December 2014, https://firstlook.org/theintercept/document/2014/03/12/nsa-phishing-tactics-man-middle-attacks/

[107] 主な資料は次の通り。これらは全てスノーデン資料である。
--“NSA Phishing Tactics and the Man in the Middle Attacks,” *The Intercept*。
--“Quantum Insert Diagrams,” *The Intercept,* 12 March 2014, accessed 1 December 2014, https://firstlook.org/theintercept/document/2014/03/12/quantum-insert-diagrams/

この計画は 2005 年から開始されたものである。「クオンタム」計画でも一番初めに開始されたのが「クオンタム・インサート」であり、極めて成功しているという。そこでそれを例に説明したい。

そのシステムの基本構造は、①データ取得制御器、②「ターモイル」、③「タービン」、④「フォックス・アシッド」サーバーの四つのシステムから構成されている。

先ず④の「フォックス・アシッド」サーバーを説明すると、TAO グループがインターネットに接続して設置しているマルウェア注入用サーバーであり、そこには実在の多くの各種サイト、例えば、ヤフーやフェイスブックの他、ＩＴ関係者に人気のあるウェブサイトである LinkedIn や Slashdot.org についても全く同じ偽装サイトが設置してある[108]。

これに対し、①～③はこの「フォックス・アシッド」サーバーに誘い込む仕掛けである。

①のデータ取得制御器（Switch Contoroller）は、通信基幹回線や外国衛星通信の傍受拠点に設置されているデータ取得のための制御装置である。

②の「ターモイル」システムは、データ取得制御器から送られてきたデータに対するセンサー装置であり、ＩＰアドレスデータ等から、一定の通信を選択して抽出する装置である。「クオンタム」計画に使用する「ターモイル」システムは、世界各地に設置してあり、2010 年時点の NSA 内部資料では、設置場所として、SSO「インセンサー」計画による英国内基幹回線からのデータ抽出拠点、英国メンウィズ・ヒル（NSA 基地）、日本・三沢米軍基地、NIPRNet（国防総省の秘密指定無し情報用の通信網）とインターネット網との接続点（10 ヶ所）[109]の４種類が挙げられているが、更に別の場所への設置計画もある。

③の「タービン」システムは、NSA 本部にのみあり、②の「ターモイル」システムが、クオンタム・インサート発動に適した通信であると判断して送信してきたデータに対して、一定の加工を加えて、「フォックス・アシッド」サーバーに誘い込むための信

--"The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics ," *The Intercept,* 12 March 2014, accessed 1 December 2014, https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/

--"There Is More Than One Way to Quantum," *The Intercept,* 12 March 2014, accessed 1 December 2014, https://firstlook.org/theintercept/document/2014/03/12/one-way-quantum

[108] 偽装サイトとして設定されているのが、NSA では 22 件、これに加えて英 GCHQ が設定しているのが２２件ある。

--ス資料、NSA, *Tailored Access Operation,* undated、accessed 29 January 2014, http://www.spiegel.de/fotostrecke/nsa-dokumente-die-abteilung-tao-der-nsa-fotostrecke-105355.html

[109] NSA 内部資料によれば、インターネット網との接続点は、米国領土内に７ヶ所、ドイツに２ヶ所、日本に１ヶ所存在する。（出典）ス資料、NSA, NTOC, *TUTELAGE*, circa 2011, accessed 28 April 2015, http://www.spiegel.de/media/media-35685.pdf.

号を送信するシステムである。

そこで、具体例を挙げると、NSA が標的としている対象者が LinkedIn サイトに接続しようとして自分の端末を操作すると、そのデータはインターネット回線を通って同サイトのサーバーに向かうが、これが回線途中に設置してある①データ取得制御器でコピーされると、②「ターモイル」システムに送られる。「ターモイル」システムが発信端末を標的端末と認識すると、それが③「タービン」システムに送信される。「タービン」システムは、「フォックス・アシッド」サーバーに誘導するために必要なデータを付加したデータを標的端末に向け送信する。標的端末がこれを受信するとそれに誘導されて④「フォックス・アシッド」サーバーに接続してしまうというものである。ここで重要なのは、標的端末に、真の LinkedIn サイトからの返信よりも早く「タービン」システムからのデータが到達することであり、正に速度の競争であるという。

この速度競争に、NSA のシステムが勝って、一旦「フォックス・アシッド」サーバーに接続させてしまえば、後は事前に分析してある対象者端末の脆弱性を狙ってマルウェアを送り込むだけであり、LinkedIn 偽装サイトでは注入成功率は５０％を超えるとされる。

（課題は速度競争である。「ターモイル」は世界主要地点に設置してあるものの、「タービン」システムは米国 NSA 本部にしかない。この間は高速回線で結んでいるが、通信に 0.1 秒程かかってしまい、速度競争には不利である。そこで、2011 年現在開発中の QFIRE というシステムでは、「タービン」機能を「ターモイル」所在地に統合する予定と見られている[110]。）

「クオンタム」計画で不可欠なのは、インターネット基幹回線等へのデータ取得制御器と「ターモイル」システム等の設置である。NSA はこれらのシステムを世界中に相当数設置しているが、UKUSA 諸国以外のシギント機関ではこれと同様の機材を広域に且つ数多く設置するのはなかなか難しいとされ、これが NSA の強みとなっている。

イ「クオンタム」諸計画

「クオンタム」計画には、上記の「クオンタム・インサート」の他にも下記の各種の侵入手法があり、この他にも各種の手法が開発中であるとされる。

- 「クオンタム・ボット」（2007 年 8 月開始）（IRC botnet 乗取り）
- 「クオンタム・ビスケット」（2007 年 12 月開始）
- 「クオンタム・DNS」（2008 年 12 月開始）（DNS 注入）
- 「クオンタム・ハンド」（2010 年 10 月開始）（フェイスブック偽装サイトに特化）

---

[110] Robert Sesek, “Unraveling NSA’s TURBULENCE Programs,” *IC off the Records*, 15 September 2014, updated 26 January 2015, accessed 3 February 2015, https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html

○　「クオンタム・ファントム」（2010 年 10 月試験中）[111]

ウ「クオンタム」計画の成功例

インターネット基幹回線へのアクセスでは､既述のように英国が大きな役割を果たしている。この事実からも推測できるように、この「クオンタム」計画でも、英 GCHQ が大きな役割を果たしているようであり、成果も挙げている。そこで、先ず、英 GCHQ による携帯電話会社に対する取組を取り上げ、次に NSA 固有の「クオンタム」計画の成功例を記述したい。

① 英 GCHQ による携帯電話に関する取組[112]

GCHQ は 2011 年「何時でも何処でも如何なる携帯電話でも」をビジョンに掲げ、このため､「電話番号さえ分かれば､遠隔からマルウェアを注入し得る作戦能力の向上」（即ち､電話番号だけで､その携帯を情報収集用或は監視用機材として使用できる能力）を掲げた。その為には、世界の携帯電話通信網の実態把握が必要であり、先ず標的とされたのが携帯電話通信網の運営に関して重要な役割を果たす通信会社である。なお、NSA・TAO に対応する英 GCHQ のハッキング組織は、「マイノック」(MyNOC: My Network Operation Centre)と呼ばれる。

○「ソーシャリスト作戦」（対ベルガコム）

ベルガコムは、それ自体が EU 諸国に多くの顧客を持つベルギーの通信会社であり、同社のシステムへの浸透はそれら顧客の情報入手、通信傍受にも繋がるが、本作戦の主目的は、GRX ルーターシステム（Global Roaming Exchange 携帯電話の国際接続に不可欠のシステム）への侵入である。即ち、その子会社 BICS(Belgacom International Carrier Services)は世界で 25 社程しかない GRX ルーターシステムの運用会社であり、且つその中でも巨大３社の内の１社（米国外で唯一）であり、世界の 400 社以上の移動体通信事業者に接続サービスを提供しているという。そのシステムを支配できれば、これら世界中の 400 社以上の携帯電話・スマートフォンに対する侵入攻撃「中間者攻撃」(man in the middle attack)

---

111 これらの各種手法については、次のスノーデン資料が詳しい。
--“The NSA and GCHQ’s QUANTUMTHEORY Hacking Tactics ,” *The Intercept.*
--“There Is More Than One Way to Quantum,” *The Intercept.*

112 Laura Poitras et.al., “GCHQ Used Fake LinkedIn Pages to Target Engineers,” *Spiegel Online*, 11 November 2014, accessed 20 January 2014,
http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html
--“Britain’s GCHQ Hacked Belgian Telecoms Firm,” *Spiegel Online,* 20 September 2014, accessed 22 October 2014,
http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

が容易になるとされる。

ベルガコム侵入のため、英マイノックは「クオンタム・インサート」の技術を使用した。先ず、2011 年初までに同社のシステム管理担当者の男性３人を割り出して標的に決定し、彼らが業務用端末から LinkedIn（世界最大のビジネス特化型 SNS）のサイトにアクセスするのを狙って「クオンタム・インサート」により端末にマルウェアを注入した。その後、それを足掛かりにベルガコムのネットワークに侵入し、同年末迄にはシステム中枢への侵入にも成功。携帯電話の国際接続を統制するデータリンク（GPRS プロトコールを使用）やベルガコムと他の 400 社以上の移動体通信会社間の業務用 VPNs にも浸透したという。更に、2013 年夏には国際通信ネットワークの中枢をなす複数の巨大 GRX ルーター（シスコ社製）からもマルウェアが発見されたという[113・114]。

---

113 ベルガコム攻撃では、GCHQ は攻撃対象として最も効果的なシステム管理者を見つけ出すことに労力を使ったようであるが、その過程でカナダのシギント機関 CSE の協力を得たという。即ち、システム管理者の割出には、世界中のＩＰアドレス情報を集めたデータベースとグーグルやヤフーのクッキー情報から構成したメタデータのデータベースを分析に使用したが、加 CSE と英 GCHQ のデータベース構築方法が異なる（加は国別、英は事業会社別）ので、両者を結合分析することで成果が出たとされる。

また、「クオンタム・インサート」攻撃では「レギン Regin」と呼ばれるマルウエア（マイクロソフトの技術者が名付親）が使用されたというが、これは、Stuxnet や Flame のマルウエアと比べても更に高度なものであるとされている。

なお、ベルガコムは 2013 年夏メールサーバの機能不全のため、コンピュータ・セキュリティ企業と契約して徹底的に調査した結果、メールサーバその他から多数のマルウエアが発見されたという。その後、８月末にはマルウエアの幾つかは外部から（多分 GCHQ によって）除去されたが、ベルガコムが情報開示に積極的でなく、また、当該セキュリティ企業も契約を中断されたので、その後の対処状況は不明であるという。

--Huib Modderkolk, “Lees hier hoe de Britse geheime dienst GCHQ Belgacom aanviel,” *NRS Handelsblad*, 13 December 2014, accessed 16 December 2014, http://www.nrc.nl/nieuws/2014/12/13/verantwoording-en-documenten/

--Ryan Gallagher, “Operation Socialist: The Inside Story of How British Spies Hacked Belgium’s Largest Telco,” *The Intercept*, 13 December 2014, accessed 15 December 2014, https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/

--Kim Zetter, “Researchers Uncover Government Spy Too Used to Hack Telecoms and Belgian Cryptographer,” *WIRED,* 24 November 2014, accessed 1 December 2014, http://www.wired.com/2014/11/mysteries-of-the-malware-regin/

114 Regin というマルウエアについては、2014 年秋にコンピュータ・セキュリティ会社のカスパルスキー（ロシア）とシマンテック（米国）が初めて公表したが、カスパルスキー社の分析よると、そのソース・コードは NSA 内部資料にあるマルウエアのサンプル QWERTY と酷似しているという。また、ベルガコムの他に Regin が発見されたところとして、欧州委員会と国際原子力委員会のシステム、メルケル独首相のスタッフの個人用パソコンが挙げられている。そして他に、カスパルスキー社だけでも、２７の国際企業、政府、個人のコンピュータから Regin を発見しており、Regin の発見は更に増えるであろうとしている。

--Marcel Rosenbach, Hilmar Schmundt and Christian Stoecker, “Experts Unmask ‘Regin’

正に、世界中の携帯電話への侵入のための作戦が粛々と進んでいたということである。

○「ワイルキー作戦」

（対「スターホーム・マッハ」等の国際携帯電話料金清算会社）

次に GCHQ の標的とされたのが、国際携帯電話料金清算会社「マッハ」である。同社は、上記の GRX ルーターシステム運用会社よりも更に数が少ない料金清算のための世界の寡占企業であり、この侵入成功は更に大きな資料源を入手することになるという。

英マイノックは、「マッハ」侵入作戦に当り、先ず、LinkedIn の SNS サイト等を活用して、標的となり得るネットワーク技術者（3 人）を選定し調査した。その際、対象者に関して、人定の他、業務用と私用のコンピュータ端末情報、スカイプ利用状況、Gメール利用状況、SNS 掲載情報、私用や業務用で良く訪問する IP アドレス等々、対象者のデジタル生活の全てを調査把握した上で、対象者それぞれのコンピュータ端末に合わせた 6 つのマルウェアを作成して、「クオンタム・インサート」作戦を実行したとされる。

そして、同社関連の秘匿通信や携帯の通信ネットワークに関して、成果を挙げたとしている。

② NSA の固有の作戦

NSA 自体も多くの作戦を実行しているが、報道された中から興味深いものを幾つか紹介すると次の通り。（なお、最初の 2 作戦は「クオンタム」計画を使用したという明確な記載はないが、同計画を使用したものと推定した。）

○「ショットジャイアント作戦」（対・華為）[115]

TAO は 2007 年には華為（ファーウェイ：中国の巨大な通信インフラ・製品メーカー）に対する作戦を開始していたが、2009 年から「ショットジャイアント作戦」としてその努力を抜本的に強化したようである。

Trojan as NSA Tool," Spiegel Online, 27 January 2015, accessed 28 January 2015, http://www.spiegel.de/international/world/regin-malware-unmasked-as-nsa-tool-after-spiegel-publishes-source-code-a-1015255.html

[115] "NSA Spied on Chinese Government and Networking Firm," *Spiegel Online*, 22 March 2014, accessed 26 March 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html

--David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times,* 22 March 2014, accessed 26 March 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=0

その成果として、華為の広東省深圳市にある本社のシステムへの侵入に成功し、1400 の顧客リストを入手したほか、Ｅメールの保管サーバーへのアクセスに成功（2009 年 1 月からメール取得可能）、更に華為の各種製品のソース・コードまで入手したという。

民間企業である華為への侵入の理由としては、華為は今や世界でも有数な巨大通信インフラ・製品会社であり、第１に、華為の広汎なインフラは中国政府にシギント能力を提供し得るところであり、華為が中国政府のためにシギント活動をしているか否かを解明する必要があること、第 2 に、NSA が標的とする諸外国の多くが華為のネットワークや製品を使用しているため、それら標的に対する諜報のために華為ネットワークや製品に関する情報を入手する必要があること、を挙げている。

○「ホワイトタマーレ作戦」（対メキシコ）[116]

作戦対象は、メキシコにおける国内治安の総括組織である公安局（警察、テロ対策、刑務所、国境警備に責任を持つ 2 万人の組織、2013 年に国家安全保障委員会に改組）であり、この情報システムに浸透することにより、米国として関心の高い薬物取引、人の密輸、国境警備等に関する情報を収集することができる。

TAO は、2009 年に公安局の情報システムの管理者を狙い、先ずこれら職員のＥメールアカウントに侵入し、これを土台に全体のネットワークに侵入したという。

○対オペック作戦[117]

2008 年 1 月には、ウィーンにある OPEC 本部のシステムへの浸透に成功し、OPEC の秘密資料へのアクセスが可能となった。その成果は、CIA や国務省に加えて、エネルギー省から高く評価されたとされる。

エ　その他の攻撃方法等[118]

ここでは「クオンタム」以外の攻撃方法と、その他の攻撃手法について幾つかの興味深いエピソードを紹介したい。

①　「ウィロウ・ヴィクスン」

標的にメールを送付し、メール中のリンク（これ自体は真正のサイトへのリンクと見られる）をクリックすると、それを送信途中で「ウィロウ・ヴィクスン」サーバーが検知して、NSA の構築した偽装サイトに誘導する方式。

---

116 Appelbaum, et. al., “Documents Reveal Top NSA Hacking Unit,” *Spiegel Online*.

117 “How the NSA and GCHQ Spied on OPEC,” *Spiegel Online,* 11 November 2013, accessed 12 November 2013, http://www.spiegel.de/international/world/how-the-nsa-and-gchq-spied-on-opec-a-932777.html

118 “NSA Phishing Tactics and the Man in the Middle Attacks,” *The Intercept.*

② 「セコンドデート」

「中間者攻撃」(man in the middle attack)の一種。

対象者とサーバー間の通信にリアルタイムで影響を与え、「フォックス・アシッド」サーバーとの接続に移行させる手法。ネットワークの結節点を通過する通信を大量に捕捉することができるが、特定の個別の対象を標的にすることもできるという。

③ マイクロソフト社の「クラッシュ報告」の活用

これは攻撃方法そのものではなく、標的端末の弱点情報の収集手段である。

即ち、マイクロソフトではコンピュータの機能に不具合があると自動的にクラッシュ報告を送るように促すメッセージが表示されるが、ＩＰアドレスなどで標的端末を特定して NSA 内データベースに登録しておくと、標的端末に関するクラッシュ報告を自動的に収集することができるという。これは標的端末が発信するメッセージを受動的に捕捉しているだけであるが、これにより標的端末ソフトウェアの抱える脆弱性が判明し、セキュリティ・ホールに関する弱点情報が得られるという。このように「クラッシュ報告」を収集できるのは、後述する「XKeyscore」システムの威力であるとされる[119]。

④ システム管理者を狙う[120]

2012 年の NSA 内部資料では、CNE の遠隔侵入では標的ネットワークのシステム管理者を狙うことが提唱されている。それは、システム管理者は既にシステムの「鍵」を持っており、同人の端末からはネットワーク構成図、顧客リストやシステム関連の業務連絡を取得でき、システム侵入作戦の効率性が高いためである。

そして、NSA の内部資料の作成者は、世界中のネットワークのシステム管理者リストを予め作成しておくことを提唱している。即ち、特定のネットワークに対する諜報需要が生じてから当該システム管理者を探索するよりも、予め管理者リストを保持していれば、必要が生じた場合に直ぐに「クオンタム」攻撃を仕掛けることができるためである。

そこで、世界中のシステムの管理者リストを作成する方法として、システム管理者が良く使う SSH 通信や Telnet 通信に着目し、NSA データベースの中から一定の形態の SSH 通信や Telnet 通信をするＩＰアドレスを抽出し、且つ、これらの使用するウェブメールやフェイスブック・アカウントを解明しておくことによって、世界中のシステム管理者リストが可能であると提唱している。

驚くべきは、先ず、世界中のネットワークのシステム管理者リストを予め作成保持

---

[119] Appelbaum, et. al., "Documents Reveal Top NSA Hacking Unit," *Spiegel Online.*

[120] Gallagher and Maass, "Inside the NSA's Secret Efforts to Hunt and Hack System Administrators," *The Intercept.*

しようと提唱するほどの潜在的諜報需要が存在する(少なくともそう認識する職員がいる）という事実であり、また、既存のデータベースから（完全ではないにしても）そのような管理者リストの作成が可能であるという事実(既にそれ程のデータを保持しているという事実）である。

（３）物理的侵入（physical subversion、close access）

TAO によるシステム侵入の手法としては、先に述べた遠隔侵入の他に、物理的侵入、近接侵入、或はネット外侵入(Off-net)と呼ぶ手法もある。担当は、AT&O（Access Technologies & Operations）である。

これは、先ず、サプライ・チェーン工作などにより対象機器に物理的に接近して、マルウェア注入やハードウェア装入を行う、この物理的侵入では、FBI や CIA の支援を受けるとされ、必要な場合には、TAO の技術者を迅速に必要な地点に移動させるため、FBI 所有ジェット機を使った要員移送支援さえも受けているとされる[121]。マルウェア注入或はハードウェア装入に成功した後は、一般的には前述した遠隔作戦センター ROC による遠隔収集に移行すると見られるが、他にそのまま AT&O が近接地点から収集（short-rage collection）をする場合もある。

この物理的侵入は更に秘匿度が高いと見られ、関係資料や報道が少ないが、判明している内で興味深いものは次の通り。

（註：本稿では、ソフトウェアとしてのマルウェアを仕込む行為を「注入」、単なるソフトウェア工作に止まらずハードウェアの改変設置を伴ってマルウェアを仕込む行為を「装入」と記載している。）

ア　サプライ・チェーン（配送経路）介入

世界中の標的組織が、サーバーやルーター等のコンピュータ・ネットワーク関連製品を発注した場合、その製品を配送途中で一旦確保して、これにマルウェアを注入し或はマルウェア入りハードウェアを装入した上で、配送経路に戻して発注先に届ける方法である。2010 年 6 月の NSA 内部資料[122]によれば、シリア通信事業機構（Syrian Telecommunications Establishment）のインターネット基幹部分に使用する製品に対してサプライ・チェーン介入を実施した結果、シリアのインターネット通信の基幹部分に侵入できたが、同基幹部分は携帯電話通信にも使用されているため、極めて大きな情

---

[121] Appelbaum, et. al., “Documents Reveal Top NSA Hacking Unit,” *Spiegel Online*. --ス資料、*Computer Network Exploitation(CNE) Classification Guide/2-59*, 1 March 2010, accessed 1 December 2014, http://www.documentcloud.org/documents/1312012-cne-declass-guide.html#document/p1

[122] ス資料、NSA, “Stealthy Techniques Can Crack Some of SIGINT’s Hardest Targets,” *SID Today,* June 2010,　accessed 1 Mary 2015, http://www.spiegel.de/media/media-35669.pdf

報成果を挙げているという。これは、最も生産性の高い作戦であるとされる[123]。

製品への注入・装入工作は、TAO グループ内のアクセス作戦専門部門 AO（Access Operations ; S326）が秘密の場所で行うが、これは FBI 等の諜報コミュニティのメンバーの支援を受けて行うという。

イ　在米大使館、国連代表部からのデータ収集[124]

2010 年 9 月現在の NSA 資料によれば、TAO は様々な手法を用いて各国の在米大使館や在ニューヨークの国連代表部からデータを収集している。

収集対象公館は３８とされており、その内、判明している対象公館は次の２５公館である（国連代表部は国連と記載）。また、判明していない公館の中には、中国、ロシア初め当然対象となっている筈のものが含まれているであろう。

＜欧州＞EU（大使館、国連）、仏（大使館、国連）、伊（大使館）、ギリシャ（大使館、国連）、スロバキア（大使館）、ブルガリア（大使館）、ジョージア（大使館）
＜中南米＞メキシコ（国連）、ブラジル（大使館、国連）、コロンビア（通商部）、ベネズエラ（大使館、国連）、
＜アジア＞韓国（国連）、日本（国連）、台湾（国連）、ベトナム（大使館、国連）、インド（大使館、別館、国連）
＜アフリカ＞南アフリカ（国連）

収集手法としては、10 種類以上の様々な手法があり、各公館に対して複数の手法が使われているが、日本の国連代表部を例にとると、次の 4 つの手法が使われているという。即ち、

- 「ミネラリズ」～LAN にインプラントを設置してデータ取得
- 「ハイランズ」～端末或はシステムに何らかのインプラントを設置してデータ取得
- 「マグネチック」～漏洩電磁波を収集してデータ取得
- 「バグラント」～コンピュータ・スクリーンのデータ読取収集

---

[123] マルウェアを仕込む対象としては、発注されたコンピュータ関連製品の他に、会議参加者に事後に送付されてくる会議記録 CD も指摘されている。2009 年、米国ヒューストンで科学者の国際会議が開催され、参加者には通例に従い会議後に会議記録 CD（議事次第、資料、写真集等を含む）が送付されて来たが、一部参加者の CD にはマルウェアが仕込まれていたという。
--Kaspersky Lab. *Equation Group: Questions and Answers* (February 2015), 15, accessed 18 February 2015,
http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf
--Dan Goodin, "How 'omnipotent' hackers tied to NSA hid for 14 years—and were found at last," *Ars Technica*, 17 February 2015, accessed 18 February 2015,
http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

[124] Greenwald, *No Place*, 145-147.

（註：「インプラント」は、システムに注入されたマルウェア、或はマルウェアを仕込んだハードウェアを指している。）

何れにしろ、昔から、大使館等の公館は各国の政治外交活動の拠点であり諜報活動の拠点でもあるため、当然、米国も含めて普通の国は、駐在大使館等を諜報活動、防諜活動の対象とするということである。筆者個人としては、対象公館数が意外と少ないという印象である。米国としては、手間暇のかかる各国公館のシギント収集はこの程度の収集で十分（その他の国に対しては他のシギント手法によって十分な情報を得ている）という判断であろうか。

（４）高度ネットワーク技術(ANT: Advanced Network Technologies)

ANT は TAO 内部の技術部門の一つであり、ネットワークに侵入したり、携帯電話やコンピュータからデータを収集したりするためのマルウェアや機材を開発している。その ANT が開発した機材カタログ（2008 年時点のもの）の一部がシュピーゲル誌のウェブサイトで紹介されている[125]。紹介されている機材は、全体の一部であり、且つ、現時点から見れば旧式のものが多い（最新型は紹介されていない）。しかし、それでもなお、NSA がデータ収集に於いてどのような機材と手法を使用しているか、また、NSA がどれだけの努力を傾注しているかが分かる資料であり、その一部を紹介したい。

なお、マルウェアは、基本的に、バイオス BIOS（コンピュータのマザーボードにあるソフトウェア）内に注入或は装入するよう求められおり、これによって、ハードドライブを消去してオペレーティングシステムなどのソフトウェアを全て消去しても、生き残るように工夫をしている。また、ウエスタン・デジタル、シーゲート、マックストアやサムスンなどが製作したハードドライブ内のファームウェアに工作して探知されないように埋め込まれたマルウェアもある[126]。

また、ANT の製品には、遠隔侵入でも注入可能なものが多いそうであるが、紹介されている製品は、近接しての物理的侵入で使うものが多くを占めるようである。

① ファイアウォール用インプラント（「シスコ」「ジュニパー」「華為」）

- 「ジェットプロー」～シスコの PIX、ASA シリーズのファイアウォール用インプラント。システムのバイオスに注入。注入後は NSA・TAO の遠隔作戦センター(ROC)からインターネット回線を通じて操作。幅広く使用されているとされる。

---

[125] "Interactive Graphic," *Spiegel Online*, 30 December 2013, accessed 9 December 2014, http://www.spiegel.de/international/world/a-941262.html

[126] Jacob Appelbaum, et. al., "NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need," *Spiegel Online*, 30 December 2013, accessed 20 January 2014, http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

② ルーター用インプラント（「ジュニパー」「華為」）

- 「ヘッドウォーター」～華為ルーター用インプラント。システムのバイオスに注入。遠隔注入も可能とされる。注入後は NSA・TAO の遠隔作戦センター（ROC）から操作。
  （なお、「ターボパンダ」プロジェクト（華為ネットワーク機器を標的とした NSA と CIA の共同事業であるが、詳細不明）で使用できる様に作られている。）
- 「スクールモンタナ」「シエラモンタナ」「スッコモンタナ」～ジュニパー用。

③ サーバー用インプラント（「デル」「ヒューレットパッカード」他）

- 「アイロンシェフ」（料理の鉄人）～ヒューレットパッカード用インプラント。物理的侵入によるハードウェアとソフトウェアの装入が必要。クローズドな（インターネット回線に接続されていない）システムからのデータ収集用。装入後は、標的クローズド・システムから、無線で秘匿の中継用システム（プリンター、サーバーやコンピュータ等を利用）を経由して、更に無線で NSA・TAO の遠隔作戦センター（ROC）から操作する。

④ 各種コンピュータ端末（種々）

- 「ギンス」～ウィンドウズ・ビスタ搭載の全ての端末に対応。物理的侵入によるハードウェアとソフトウェアの装入が必要。無線により遠隔操作。
- 「アイレイトモンク」（怒れる修道士）～物理的侵入でも遠隔侵入でも、注入可能なインプラント。インターネット回線を通じて操作。

⑤ 偽装 USB コネクター無線送受信機。遠隔操作可能。

- 「コットンマウスⅠ」～短距離の無線通信可能。50 個約 100 万ドル。
- 「コットンマウスⅡ、Ⅲ」～他のインプラント装入のパソコン端末等を経由して無線通信の可能距離を延伸。

⑥ モニター画面情報発信器

- 「レイジマスター」～モニター画面用コードに仕込んだ微小発信機。1 個 30 ドル。「レイジマスター」に遠距離から「CTX4000」という装置を使って特殊なレーダー波を照射すると、モニター画面用コード内を通る信号内容を反映してレーダー波を変調する。この変調レーダー波を受信して、増幅復調するとモニター画面が再現できる。

日本の国連代表部に対する情報収集手法「バグラント」の構成要素

⑦ キーボード情報発信器

- 「サーリー・スパーン」～キーボードに仕込んだ微小発信機により、キーボードの打鍵状況を電波（方形波）で発信。1 個 30 ドル。遠距離からこれに「CTX4000」という装置を使ってレーダー波を照射して捕捉し、増幅復調して打鍵情報を取得する。先のモニター画面情報発信器と同類。この発信電波の探知は極めて難しいと見られる。

⑧ 微量電波受信装置「CTX4000」～レーザープリンター等は、発信機を仕掛けなくても、本器材で受信復調可能とされる。

EU の国連代表部のレーザープリンターからの情報収集手法「ドロップマイヤー」は、この受信装置を使用していたとされる。

⑨ 無線ＬＡＮ侵入通信用装置

- 「スパローⅢ」～無線 LAN の存在を探知するシステム
- 「ナイトスタンド」～無線 LAN に侵入して任意の端末にマルウェアを注入可能。理想的な環境では 8 マイルの遠距離からも注入に成功。

両者共に、ドローン（無人飛行機）に搭載可能。

⑩ 携帯電話用各種装置

- 「ドロップアウトジープ」（2008 年現在開発中）～アイフォン用インプラント。標的アイフォンから、ファイルデータの取得と挿入、ショートメールサービス記録、通信した相手、ボイスメール、位置情報の取得ができ、更にマイクとカメラを勝手に起動できるというものである。一言で言えば、アイフォンをその使用者に対する監視器材に転換するソフトウェアである。

  当面（2008 年）は近接侵入用が提供され、遠隔侵入用は将来開発予定。

- 特殊加工の携帯電話（2008 年時点ではサムスン、東方通信用）～監視・情報収集用にインプラントなど特殊加工をした携帯電話。サムスン等の本物そっくりであり、標的者の携帯と摩り替えるか、協力者やエージェントに所持させて、遠隔地から自由に情報を収集することができる。
- 「キャンディグラム」～電話通信塔機能を有し、本機材を設置すると、標的携帯端末が通信エリア内に入ると、その事実を自動的に遠隔地の司令部まで通報するシステム。

ここで紹介したのは、シュピーゲル誌がウェブサイトで紹介しているもの（それ自体も ANT カタログの一部であろう）の一部であり、NSA は諜報活動に有用と考えられるものは凡そ何でも開発していると推定される。

（５）CNE 対策（Counter – CNE）

ところで、コンピュータ・ネットワーク資源開拓（Computer Network Exploitation : CNE）は、その能力規模に違いはあれ、世界中の諸シギント機関が行っていることである。米国に対しては、中国、ロシアその他の諸機関が積極的に CNE 作戦を実行している。そこで、これら他国機関による CNE 作戦から自国を守る CNE 対策（Counter—CNE）が必要になるが、その第一歩は当該他国機関の CNE 作戦の実態を解明することである。ここでは、中国からの CNE 作戦に対抗する NSA の CNE 対策を、その内部資料[127]を基に見てみたい。

NSA は、中国による CNE 作戦全体に対して「ビザンチン・ヘデス（Byzantine Hades）」とのコード名を付けてその解明と対策に当たっている。中国による CNE 作戦は種々あり、作戦グループ毎に使用する機器や手法が異なるようであり、少なくとも１２の作戦グループが存在すると見られる。それら作戦グループに NSA が付けたコード名には、「ビザンチン・カンダー」「ビザンチン・ラプター」など「ビザンチン」を冠したものが７つ、他に「マベリック・チャーチ」「ディーゼル・ラトル」などの名称に関連性の伺われないものが５つある。各作戦グループの標的は、主として米国であるが、「ディーゼル・ラトル」グループは日本も標的にしている。

これらの各グループの活動について、NSA は少なくともその一部を解明しているが、一例として「ビザンチン・カンダー」の解明を NSA 内部資料[128]によって見ると、解明の経緯は次の通りである。即ち 2009 年に、国防省のネットワークに対して何者かが侵入しているのが探知され、NTOC（脅威作戦センター）からの依頼を受けた TAO グループがその解明に乗り出した。侵入者は、多くの作戦中継機（hop points）を経由して侵入している上、更に発信端末自体の IP アドレスも変更されるため、発信端末を特定するのは困難を極めたとされるが、遂に、中国人民解放軍総参謀部第三部が使用するユーザー・アカウントを特定することが出来たという。そしてそのユーザー・アカウントの関与するインターネット事業者のネットワークに侵入して、所謂「中間者攻撃」を掛けて、2009 年 10 月には「ビザンチン・カンダー」グループの５つのコンピュータ端末への侵入に成功した。侵入に成功した端末には CNE 作戦の責任者のものも含まれるという。これにより同グループの構成員情報、技術概要、取得データ、将来の攻撃目標（米国や外国政府職員の個人情報等）などに関するデータを入手することが出来たという。

NSA は、これらの CNE 対策によって、「ビザンチン・ヘデス」即ち、中国からの

---

[127] ス資料、NSA, NTOC, *Byzantine Hades: An Evolution of Collection*, June 2010, accessed 19 January 2015, http://www.spiegel.de/media/media-35686.pdf

[128] ス資料、NSA, TAO, *Byzantine Candor: A TAO Success Story*, June 2010, accessed 19 January 2015, http://www.spiegel.de/media/media-35686.pdf

CNE 作戦全体によって米国が受けた被害を見積もっているが、その被害は NSA 内部資料[129]によれば次の通りである。

国防総省のシステムに対する侵入事案は、少なくとも３万件以上、重大な侵入事案が 500 件以上。1600 台以上のネットワーク端末が侵入されている。これらの侵入によるネットワークの損害の見積り・修復のために１億ドル以上の費用を要している。

窃取されたデータは、３万人以上の空軍軍人の個人情報、３０万件以上の海軍のユーザーID とパスワード、原子力潜水艦や海軍防空ミサイルのデザイン情報、国防企業から B2 爆撃機、F22 ステルス戦闘機、F35 戦闘機等に関する機密情報であり、貴重な情報が大量に窃取されたと見られる。

実際、中国の J20 戦闘機や J31 戦闘機のデザインは、以前から F３５戦闘機に似ていると指摘されており、この内部資料によって中国によるスパイ行為が裏書された形である[130]。

なお、このようにして敵対者の CNE の実態解明が出来れば、これにより敵対者からのシステムへの侵入を阻止するコンピュータ・ネットワーク防禦（CND）が実施し易くなる。

（６）「第四者（フォース・パーティ）収集」

ア　「第四者（フォース・パーティ）収集」とその類型

CNE 対策によって敵対者の CNE 作戦の解明ができれば、それによって自国のネットワーク防禦に役立てるだけではなく、当該機関（サード・パーティ第三者）の CNE 作戦そのものを利用して更に他の国（フォース・パーティ第四者）の情報を収集することも可能となる。

そこで、TAO グループは、第四者収集という分野を開設して、その標語の一つに「彼らの道具、技術、標的、そして成果を盗め」（steel their tools, tradecraft, targets and take.）と定めて取り組んでいる[131]。

因みに、NSA の内部資料[132]では、第四者収集の類型について、次の４類型が示されている。即ち、

①　消極収集（第三者による第四者からの収集データを回線の中間で盗取する方法）

---

129 ス資料、“Chinese Exfiltrate Sensitive Military Technology,” circa 2010, accessed 19 January 2015, http://www.spiegel.de/media/media-35687.pdf

130 Philip Dorling, “China stole plans for a new fighter plane, spy documents have revealed,” *The Sydney Morning Herald*, 18 January 2015, accessed 19 January 2015, http://www.smh.com.au/national/china-stole-plans-for-a-new-fighter-plane-spy-documents-have-revealed-20150118-12sp1o.html

131 ス資料、NSA, NTOC, *Case Studies of Integrated Cyber Operation Techniques,* undated, accessed 19 January 2015, http://www.spiegel.de/media/media-35658.pdf

132 ス資料 *Fourth Party Opportunities*, undated, accessed 19 January 2015, http://www.spiegel.de/media/media-35684.pdf

② 積極収集（第三者の端末に浸透して、これを操作して第四者に対する収集を行う方法）
③ 乗取り（第三者が第四者に注入したマルウェアを利用して、これに換えて自己のマルウェアを注入する方法）
④ 再利用（第三者による CNE 作戦から得た情報を利用して、第四者に対する自らの CNE 作戦の効率化迅速化を図る方法）

このような内部資料が存在するということ自体が、世界諸国に於ける CNE 作戦の蔓延と、更にそれに対抗し且つ利用する NSA の実態を示唆していると言えよう。

イ 具体例～中国の CNE の利用

NSA 内部資料[133]により具体例を挙げると、2009 年 7 月米国システムに対する CNE 作戦を解明していたところ、中国の CNE グループ「ビザンチン・ラプター」の指令端末に辿りついたという。そこでこの指令端末を監視していると、同グループが国連（第四者）のコンピュータをハッキングして継続的に有益なデータを入手しているのを発見した。そこで、NSA はそのデータをそのまま入手したという。これは、上記収集類型では①の消極収集に該当する例であろう。

ウ 具体例～韓国の CNE の利用

別の例では、NSA が北朝鮮のネットワークに対する情報収集を開始した当初の 2010 年頃、NSA は殆どアクセスできていなかった。他方で韓国（第三者）は必死に北朝鮮に対する収集をしてきたので、資料源開拓の一環として韓国の CNE に侵入したところ、韓国が北朝鮮（第四者）の端末（複数）にマルウェア注入していたのを発見した。そこで、これらを北朝鮮のネットワーク対するデータ収集態勢構築に利用したという。因みに、北朝鮮の端末の幾つかは北朝鮮自体の CNE 作戦に使用されていたものであるという。詰まり、北朝鮮の CNE 作戦の解明にも役立った訳である。

収集類型としては、これは上記の③の乗取り或は④の再利用に該当するであろう。

なお、この当時は、NSA としては韓国の CNE 作戦自体にはそれ程関心が無かったが、その後韓国が米国を標的とした収集を強化しているので、韓国自体にも関心が強まっているとしている[134]。

エ 具体例～正体不明ハッカーの利用

---

[133] ス資料、NSA, NTOC Hawaii, *NSA's Offensive and Defensive Missions: The Twain Have Met,* 26 April 2011, accessed 19 January 2015, http://www.spiegel.de/media/media-35681.pdf

[134] ス資料、NSA, *Is there "fifth party " collection?* circa 2011, accessed 19 January 2015, http://www.spiegel.de/media/media-35679.pdf

2010 年 5 月（2012 年 11 月補正）の NSA 内部文書[135]によれば、正体不明のハッカー集団が E メール窃取システムによりデータを窃取しているのを NSA と加 CSE が発見し、そのシステムを INTOLERANT と名付けた。ところが、その窃取データには NSA 自体も関心を持っている有益なものが多かったので、そのままデータを入手しているという。

INTOLERANT は高度なシステムで、標的アドレスのメールをばらばらに細切れにした上で衛星通信を経由し複数の異なる IP アドレス宛に送信しているという。細切れにしてデータ量を小さくしているので、発見され難い。但し、ハッキングしているメールアドレスは分類整理されているので、一旦収集に成功すれば NSA としても情報価値が高いという。

ハッキングの対象となっているメールアドレス分類の中で、NSA としても関心があるものとして、次の 7 分類を上げている。即ち、①インド外交・海軍、②中央アジア諸国外交、③中国人権活動家、④チベット民主運動家、⑤ウイグル活動家、⑥欧州アフガニスタン特別代表とインド写真ジャーナリスト、⑦チベット亡命政府である。ハッカー達の技術レベルと収集対象から見て、国家主体或は国家支援の活動と推定されるが、2012 年 11 月段階でも特定に至っていないとしている。

常識的に考えて、このハッカー集団は、中国のシギント組織或はその支援を受けた集団であろう。但し、既述した「ビザンチン・ヘデス」の各作戦グループとは異なるグループということであろう。何れにしろ、中国によるシギントへの取組と更にその上前を刎ねようとする NSA の取組と、正に国益を賭けて、中国、米国が鎬を削っている様が伺われ、興味深いものがある[136・137]。

---

135 ス資料、NSA, "Who Else Is Targeting Your Target? Collecting Data Stolen by Hackers," *SID Today,* 6 May 2010, modified 10 November 2012, accessed 5 February 2015, https://firstlook.org/theintercept/document/2015/02/04/intolerant-else-targeting-target-collecting-data-stolen-hackers/
--Glenn Greenwald, "Western Spy Agencies Secretly Rely on Hackers for Intel and Expertise," *The Intercept*, 4 February 2015, accessed 5 February 2015, https://firstlook.org/theintercept/2015/02/04/demonize-prosecute-hackers-nsa-gchq-rely-intel-expertise/

136 個人の民間ハッカーは、ブログやチャットルームで、自らのハッキングの技術を誇示したり、窃取したデータを公開したりしており、その中にはシギント機関にとっても貴重な情報が含まれるという。ところが、シギント機関の分析官がこれらをマンパワーでフォローするのは効率が悪い。そこで、英 GCHQ の 2012 年頃の内部資料によれば、GCHQ はハッカーの議論を自動的にフォローするため、LOVELY HORSE というプログラムを作成している。これは、各種のブログやツイッターなどソーシャルメディアに現れるハッカーによる議論の中から、分析官が関心あるものを自動的に検索して分類して提供するシステムである。有益なデータであれば、ハッカーをも収集対象にするのがシギント機関である。
--ス資料、GCHQWiKi, *Lovely Horse*, circa 2012, accessed 5 February 2015, https://firstlook.org/theintercept/document/2015/02/04/lovely-horse-gchq-wiki-overview/

137 本文（5）（6）の記載からは、米中両国はそれぞれ CNE で鎬を削っているものの、全体

的な印象では米国が上手を取っているかの様にも見えるが、中国もなかなか負けてはいないことを示す事件が、最近表面化した。それは、米国連邦政府職員の機微な個人情報の大量漏洩である。

即ち、米国人事管理局（Office of Personnel Management）は、2015 年 6 月 4 日、人事管理局の情報システムが侵入を受け 400 万人に及ぶ連邦職員のデータが窃取された可能性がある旨公表した。更に 7 月 9 日には、これに加えて個人背景調査（background investigation）記録から 2150 万人分の個人情報が窃取された旨公表した。

人事管理局の公表と報道を総合すると、次の 2 種類の個人データが窃取されたことが分かる。

① 連邦職員の人事管理用データベースから、現職及び退職した連邦職員 420 万人（内現職は 210 万人）分の個人情報。情報には、氏名、生年月日、住所、社会保険番号、勤務歴、人事評価が含まれる。（2014 年 10 月から 2015 年 4 月の間に窃取。）

② 連邦職員の個人背景調査（background investigation）記録のデータベースから、現在、過去、そして将来の連邦職員又は契約職員 2150 万人分の個人情報。2150 万人中、1970 万人は個人背景調査の申請者本人のものであり、180 万人は申請者の配偶者や同居人のものである。また、背景調査によるインタビュー記録の一部や指紋データ 110 万人分も盗まれたという。（2014 年後半から 2015 年 1 月の間に窃取。）

そして、①と②の両方で重複してデータを盗まれた者は 360 万人いるとされる。

ところで、個人背景調査とは連邦職員に採用され特定の職務に就くために必要な適格性を有するか否かを判断するための背景調査であり、全ての連邦職員とその候補者が受ける必要がある。そして、その前提として申請者は調査に必要な個人情報の提供を求められるが、それは職務の種類により、様式 86、様式 85、様式 85C の三つに分かれる。（インテリジェンス関連を含む）高度なセキュリティ・クリアランスを必要とする国家安全保障関連職務（national security positions）に就くには、様式 86 に従い詳細な個人情報を提供しそれに基づく調査を受ける必要がある。様式 86 に含まれる情報は実に詳細であり、過去の各居住地とそこでの隣人、通った各学校とそこでの友人、各職歴とそこでの上司、結婚歴、家族親族関係、交友のある外国人、国外での経済活動、外国企業との関係、外国政府との関係、外国への渡航歴、健康状態、犯罪歴その他の警察記録などの多くの情報が含まれる。

匿名の米国当局者は、このデータ窃取は中国によりなされたと語っている。これらの情報は、諜報機関にとって極めて有用な情報であり、米国政府職員と友人知人関係にある中国人を脅迫し、協力者とし、或は処罰するための資料にも使えるし、また、米国諜報機関職員に対してスパイ工作を仕掛けるための最高の基礎資料としても使えるものである。「これは職員情報の宝の山である」とコーメイ FBI 長官は 7 月 9 日に語っている。

諜報関係者によれば、過去１、２年間に中国は、サイバー諜報活動によって米国人の個人情報の大量データベースを構築中と見られており、人事管理局の他、個人背景調査を受託している民間事業者、国土安全保障省、民間医療保険会社などのデータベースへの侵入を図っているという。

実に、中国も積極果敢に闘いを仕掛けているのである。

-- Office of Personnel Management, “OPM to Notify Employees of Cybersecurity Incident,” and “OPM Responds to Cyberattack,” 4 June 2015, accessed 15 June 2015, http://www.opm.gov/news/latest-news/announcements/

-- Office of Personnel Management, “Information About the Recent Cybersecurity Incident,” 15 June 2015, accessed 16 June 2015, http://www.opm.gov/news/latest-news/announcements/

-- Office of Personnel Management, “OPM Steps to Protect Federal Workers and Others From Cyber Threats,” 9 July 2015, accessed 17 July 2015, https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-worker

s-and-others-from-cyber-threats/
-- Office of Personnel Management, "Information About OPM Cybersecurity Incidents," (undated), updated 9 July 2015, accessed 17 July 2015, https://www.opm.gov/cybersecurity/
--AP, "Officials Say Deeply Personal Information in Hackers' Hands," *The New York Times,* 13 June 2015, accessed 15 June 2015, http://www.nytimes.com/aponline/2015/6/03/ap-us-government-hacked .html.
--REUTERS, "China-Kinked Hackers Get Sensitive U.S. Defense and Intelligence Data-Report," *The New York Times,* 13 June 2015, accessed 15 June 2015, http://www.nytimes.com/reuters/2015/06/13/world/asia/13reuters-cybersecurity-usa-china.html
--Ellen Nakashima, "Chinese hack of federal personnel files included security-clearance database," *The Washington Post*, 12 June 2015, accessed 14 July 2015, https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/
--Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *The Washington Post*, 9 July 2015, accessed 14 July 2015, http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

８　CLANSIG（秘匿シギント活動）

CLANSIG（clandestine sigint：秘匿シギント活動）は、機密度が極めて高く、現在まで報道されたスノーデン資料を見てもその内容は殆ど不明である（唯一、通信基幹回線からのデータ収集事業の中の「ランパートＴ」計画（内容不明）が CLANSIG であることが判明しているのみ）[138]。しかし、CLANSIG はその予算額を見ても、極めて重要な活動と考えられる。即ち、スノーデン資料の中の 2013 会計年度・国家諜報計画予算案では、NSA 予算中に 3 億 4820 万ドル、CIA 予算中に 4 億 6463 万ドル、合計 8 億 1282 万ドル･邦貨で 800 億円以上という巨額な CLANSIG 予算が計上されており、これは SCS（特別収集サービス、NSA と CIA の共同事業）の予算額の 2 倍以上である[139]。また、予算の記載場所が SCS との並びであることから判断して、基本的に米国外、多分に危険な地域(hostile territory)における活動と推定できる。

そこで､スノーデン資料等の中からこれらに合致すると推定できるものを探索すると、NSA の活動として TAREX 計画、CIA の活動として国家秘匿サービス(National Clandestine Service: NCS)中のシギント関連活動が挙げられる。現時点では TAREX 計画が予算上の CLANSIG であるとの確証はないが、この二つについて紹介したい。

（１）NSA の TAREX(Target Exploitation)計画

2012 年 2 月付の内部資料[140]によると、TAREX 計画は、世界中で行う秘匿シギント活動のための①標的ネットワークへの物理的侵入と②公然非公然のヒューミント作戦であるという。作戦は、NSA と陸軍ヒューミント機関（INSCOM：陸軍諜報・安全保障司令部）の重複する権限の下に実施されるが、作戦全体は、NSA の要求に基づき、NSA の指揮・費用負担により行われ、作戦の執行は、ヒューミント・コミュニティが責任を負うとされる。内部資料の記載から判断して、この秘匿シギント活動では、TAREX 要員への身分偽変支援等のヒューミント部分は INSCOM が支援提供し、個別作戦では必要に応じて CIA、INSCOM、FBI 等の諜報コミュニティ・ヒューミント部門の最適部署と密接に協力しているということではないかと考えられる。

また、TAREX 部門は、ヒューミント及び（シギント関連の）技術的諜報についての

---

138 ス資料、*Special Source Operations,* Page 2, undated, accessed 9 February 2015, https://www.documentcloud.org/documents/1200860-odd-s3-overviewnov2011-v1-0-redacted-information.html

139 ス資料 *FY2013 Congressional Budget Justification Vol. Ⅰ：National Intelligence Program Summary*, February 2012, 159,162,　accessed 20 August 2014, http://fas.org/irp/budget/nip-fy2013.pdf

140 ス資料　NSA/CSS, *Classification Guide for the NSA/CSS Target Exploitation (TAREX) Program,* 6 February 2012, revised through 25 April 2012, accessed 11 October 2014, https://firstlook.org/theintercept/document/2014/10/10/target-exploitation-classification-guide/

諜報コミュニティとのNSAの窓口であり、また、CIA、DIA国防諜報庁、FBIの（シギント関連の）ヒューミント作戦ではTAREX要員がそれら機関の担当部署に配置されることがあるとされる。

標的ネットワークに対する物理的侵入の記載は、TAOの物理的侵入と同様であり、物理的侵入の他、近接侵入、或はネット外侵入(Off-net)とも呼び、また、サプライ・チェーン工作やハードウェア装入などの手法が含まれるとされる。なお、公然非公然のヒューミントが、この物理的侵入と重複する範囲内のものであるのか、或は、更に身分を秘匿してのシギント資料（例えば暗号資料）収集、或は、「本論第１章１（３）宝島」の註記で述べたように中国、ロシア等に於ける秘匿サーバーの設置等の活動を含んでいるのか、資料からは明確でないが、TAREX部門にはNSA自体のヒューミント要員がいる旨の記載もあり[141]、含まれると考えられる。つまり、TAREXでは、例えば身分を偽変してIT企業で働き暗号情報を入手するなどの活動も行っていると考えられる。

TAREX計画による活動は、欧州、中近東他の広汎な地域で行われており、そのため、前進基地が次の諸地点に置かれている。即ち、米国内ハワイ、テキサス、ジョージア各州のNSA地方本部、在ドイツのNSAシギント・センター、韓国、中国・北京、特定の米大使館、特定の海外拠点とされている。この中でも、ドイツ、韓国、中国・北京が特記されているのは注目に値する。これら三国は何れも電気通信製品の巨大企業の所在地であり、それとの関連も疑われる[142]。

（なお、TAREXの活動分野については、前節で記述したTAOによるコンピュータ・ネットワーク作戦中の物理的侵入と重複しており、当該部分を特にTAREX計画と呼称している可能性もある。但し、TAOに関するスノーデン資料にはTAREX或はINSCOMに関する言及が見られないことから判断して、現時点では別物と推定した。）

（２）CIAによるCLANSIG・NCS

国家秘匿サービス(NCS: National Clandestine Service)は、CIAの非公然・秘密工作を担う組織であるが、それまでの作戦局（Directorate of Operations）が2005年に改組されて出来たものである。任務としては、秘密工作など特殊なヒューミント活動の他に、秘匿の技術的収集も担当しており、その中にシギントとマシントが含まれている。

---

141 ス資料　NSA/CSS and JFCC-NW, *National Initiative Protection Program—Sentry Eagle(Draft),* undated but derived from a document dated 23 November 2004, accessed 11 October 2014,
https://firstlook.org/theintercept/document/2014/10/10/national-initiative-protection-program-sentry-eagle/

142 Peter Maass and Laura Poitras, “Core Secrets: NSA Saboteurs in China and Germany,” *The Intercept,* 10 October 2014, accessed 11 October 2014,
https://firstlook.org/theintercept/2014/10/10/core-secrets/

報道[143]によれば、CIA による秘匿シギント活動は 2001 年の 9/1 1 事件後に強化されたが、特に、2007 年から 2013 年まで国家秘匿サービス長を務めたスリック氏が、外国通信やコンピュータに対するヒューミントを最優先事項の一つとして強化したという。その結果、現在国家秘匿サービスには、NSA のためにこれらシステムへの侵入を専門とする技術作戦要員(Technical Operations Officers)が数百人(several hundreds)もおり、その内数十人(several dozens)はNSA本部で勤務しているとされる。

彼らの活動例としては、例えば、スカンジナビア半島某国のテロ対策担当官によれば、自国内でイスラム過激派の居宅を監視していたところ、居住者が金曜礼拝でモスクに出掛けての留守中に、CIA 要員 2 名が居宅に侵入して過激派のパソコン端末にマルウェアを注入して素早く撤収するのを目撃したという。また、最近の事例では、西欧の某国でシリア過激派「アルヌスラ戦線」戦闘員の勧誘者の居宅に、CIA 要員が侵入してパソコン端末にマルウェアを注入し、そのパソコンの全てのＥメールとスカイプによる会話を収集可能としたこともあるという。また、その他、外国政府や軍の通信・コンピュータシステムへの侵入事例も多々あるとされる。

以上、現時点では、CLANSIG の内容については良く分からない点が多いが、今後スノーデン資料が更に報道されれば、その内容や TAO との関係などが判明する可能性がある。

---

143 Matthew M. Aid, "The Role of CIA Covert Ops in Penetrating Foreign Computers and Communication Networks," *Atlantic Council*, 17 July 2013, accessed 26 August 2014, http://www.atlanticcouncil.org/blogs/natosource/the-role-of-cia-covert-ops-in-penetrating-foreign-computers-and-communication-networks

９　その他

（１）旅客機上の携帯電話収集[144]

2012 年時点の内部資料によれば、GCHQ と NSA は、旅客機上での携帯電話使用に対する収集力の構築中であり、既に一部収集可能となっている。

即ち、旅客機輸送では、長距離ビジネスクラスを中心に機上での携帯電話利用サービスを提供する会社が増加しつつある。例えば、英国航空は、音声通話は認めていないが、データ通信や SMS（ショート・メッセージ・サービス）のサービスを提供している。

そこで、機上での携帯電話を収集対象とするのであるが、対象の通信端末は、GSM（第２世代通信）と GPRS（第２.５世代通信）である。GPRS でも、ブラックベリー携帯電話については、一定の収集能力を開発したとしている。

これによって、ニア・リアル・タイムで特定の携帯電話端末が特定の旅客機内にあることを確認できるようになるという。特定の旅客機では２分毎に位置確認ができる。その結果、端末を所持する者の監視が可能になり、必要な場合には対象者の身柄拘束チームを（空港などに）事前配置することが可能となる。また、対象者が携帯電話による通信を行えば、Ｅメールアドレス、フェイスブックＩＤ，スカイプ・アドレス等を取得できるとされる。

（２）無人飛行機による収集

「７　CNE（コンピュータ・ネットワーク開拓)」や「第３章１メタデータ分析」の記述から分かるように、無人機によるデータ収集が行われている。しかし、現時点では、その規模等に関する資料は報道されていない。

---

144 Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014), 164-166.

第３章　収集分析その他の活動の実態

前章では、NSA のシギント・データの収集態勢について述べたが、本章では、その収集態勢を使って NSA が実際に何を収集しどのように分析しているかについて、主としてスノーデン資料に拠って述べてみたい。但し、NSA は超巨大産業であり、その収集分析その他の活動の全貌を記述することは到底不可能であるので、報道された中から重要であると考えられるもの、興味深いものを選んで言及する。

１　メタデータ分析

メタデータ分析は、聞き慣れない用語であるが、NSA の分析手法の中では極めて重要な手法であり、ここにその概要を述べたい。

（１） メタデータとデータベース「メインウェイ」「マリーナ」

メタデータとは、既述（第２章の４）したように、通信内容を除く通信に付随する情報の全てであると定義されている。

具体的には、携帯電話通話であれば、通話当事者の電話番号、携帯端末識別番号（International Mobile Equipment Identity(IMEI) number）、利用者識別番号（International Mobile Subscriber Identity(IMSI) number シムカードに記載）、回線識別符号、通話日・時刻、通話時間、テレホンカード番号、携帯端末位置情報等である。

また、インターネット通信であれば、E メール活動の内メールの内容以外の全て、即ち、当事者のメールアドレス、IP アドレス、通信日・時刻等、SNS 活動の通信内容以外の情報、その他ネットワーク上の活動（ウェブサイト訪問履歴、ログイン時刻、地図検索履歴等）情報が該当する。

これらのメタデータを保管し分析するために、NSA は二つのデータベースを構築している。電話通話メタデータ用の「メインウェイ」とインターネット通信メタデータ用の「マリーナ」である。これらのデータベースには、第２章で既述した全ての収集プラットフォーム、即ち、「プリズム」、通信基幹回線、外国通信衛星、特別収集サービス等で収集したメタデータが全て保管されているという。

そのデータ量は膨大であり、例えば、電話「メインウェイ」データベースは、2011 年は米国内で毎日７億件の通話メタデータを収集していたが、同年８月には某通信会社から毎日１１億件の携帯電話メタデータが増加したという。そこで、2013 会計年度予算では、メタデータ保管のために、毎日 200 億件のメタデータを受入れ可能で、且つ受入れ後６０分以内に分析可能とするメタデータ保管システム構築が計上されている[1]。

---

[1] James Risen and Laura Poitras, “N.S.A. Gathers Data on Social Connections of U.S. Citizens,” *The New York Times,* 28 September 2013, accessed 22 October 2013,

メタデータには通信内容が含まれないのであるから、通信内容よりも価値が低いと誤解する者もいるかも知れないが、通信内容そのものの価値と比べても価値が低いとは言えない。先ず、通信内容は千差万別であり、定型的・システム的な情報処理に適していないが、メタデータは定型的な自動分析が可能であり、膨大なデータからのデータ抽出が通信内容よりも容易である。また、通信内容は必ずしもそれが事実とは限らないが、メタデータは実在した通信活動に関するデータであり、そこには嘘が入る余地がない。後述する各種のメタデータ分析手法も、このメタデータの特性を利用したものである。

（２） 接触連鎖分析[2]

メタデータの最初の大々的な活用は、2001 年９/１１以後のテロ対策での接触連鎖分析（contact chaining analysis）である。即ち、既に把握しているテロリスト及びテロ容疑者と直接或いは間接に連絡を取っているテロ企図者を割り出すため、元ロシア担当の通信状況分析官（トラッフィク・アナリスト）で通話接触の分析経験を有する者を多数参加させたと言う[3]。これに FBI や CIA がテロリスト或いはテロ容疑者として把握していた者の電話番号を提供しメタデータの分析を開始した[4]。

即ち、把握しているテロリストとテロ容疑者が、米国内の誰と連絡を取っているか、そして、米国内の連絡相手は更に誰と連絡を取り合っているかを解明するため、元のテロリスト乃至テロ容疑者の連絡先を３つ先（連絡先の更にその連絡先の更にその連絡先）まで、その人物たちの社会的ネットワークを把握分析するものである。

2004 年までにはこの分析チームに FBI や CIA の分析官も参加したという。

その後、電話メタデータのデータベース「メインウェイ」に自動分析機能が付加され、

---

http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all&_r=0

[2] この経緯は次の資料に詳しい。

--ス資料 NSA, Office of the Inspector General, *ST-09-0002 Working Draft*, 24 March 2009, 11-14, accessed 6 November 2014, https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf

[3] 通信状況分析については、既に、第１部第１章国家安全保障庁概観で述べたとおりであるが、所謂コミントの中では暗号解読と並ぶ重要な分析手法である。通信内容が全く不明であっても、外形的な通信状況を詳細に分析することにより、情報を抽出する手法であり、具体的には、敵軍の戦力組成（組織）、軍部隊の移動状況等の把握が可能である。具体例については次の資料が詳しい。この通信状況分析を電話通話やインターネット通信に適用したのが、正にメタデータ分析と言えよう。

--公開資料 Donald A. Borrmann, et. al., *The History of Traffic Analysis: WW I -Vietnam,* Center for Cryptologic History, (NSA, 2013), accessed 10 October 2014, https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/traffic_analysis.pdf

[4] 2002 年３月にパキスタンでアルカイダ幹部を捕捉。その際に CIA はコンピュータや携帯電話、電話番号表を入手して、これにより接触連鎖分析が進展したと言われる。

接触連鎖分析のため自動的に相関図を作成することが出来るようになった。更に、特定者と電話接触があった場合には自動的に警報が発せられるように改良が加えられた。警報が発せされた際には必要に応じて、FBI や CIA に連絡することとなっている。

NSA による接触連鎖分析の成果として、2012 年中には分析の結果、テロ企図の容疑者ついて 500 件の情報が FBI に提供されたという。（FBI は、その後、FBI のデータベース或いは公開情報等を元に調査を遂行することとなる。[5]）

（３） 人物分析[6]

特定人物がインターネットを相当利用しているならば(現代ではそれが普通であろうが)、インターネット通信メタデータを分析することにより、その人物像、生活習慣や生活実態を浮彫りにして把握することができる。

即ち、誰と何時どの程度の E メールの遣取りをしているか、どの程度の SNS の遣取りをしているか、如何なるウェブサイトに何時どれ位アクセスしているか、スマートフォンの現在位置は何処か等々を分析することにより、友人知人の関係、どのような（宗教団体や政治団体その他の）組織団体と関係を持っているか、居場所と移動の状況、生活習慣、行動履歴が分かる。また、それだけでなく、何に関心を持っているか、行動の意図は何か等々、その人物を浮彫りにする情報を入手することができる。

更に、それ以外の情報を付加して分析するならば、当該人物の全体像を知ることができよう。付加的情報としては、銀行口座情報、保険情報、フェイスブックプロファイル、旅客名簿、選挙人名簿登録、財産情報、税務情報等々、政府機関（特に FBI など米国の政府機関）であれば、容易に入手できる情報であろう。

かくして、ある人は、メタデータ分析により、日記を読むがごとく頭の中を見ることができると言い、ある人は、メタデータ分析はデジタル時代の行動監視であるという[7]。

（４） 位置情報データベース（FASCIA）と同伴者分析等

---

[5] Dana Priest, “Piercing the confusion around NSA’s phone surveillance program,” *The Washington Post,* 9 August 2013, accessed 22 October 2013, http://www.washingtonpost.com/world/national-security/piercing-the-confusion-around-nsas-phone-surveillance-program/2013/08/08/bdece566-fbc4-11e2-9bde-7ddaa186b751_story.html

[6] Glenn Greenwald and Spencer Ackerman, “NSA collected US email records in bulk for more than two years under Obama,” *The Guardian,* 27 June 2013, accessed 12 July 2013, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.
-- Risen and Poitras, “N.S.A. Gathers Data on Social Connections of U.S. Citizens,” The New York Times.

[7] 前者はケイトー研究所のジュリアン・サンチェス氏、後者はジョージワシントン大学のオリン・カー博士。何れも上記註 Greenwald and Ackerman, “NSA collected US email records in bulk …,” *The Guardian* が出典。

ア　位置情報データの収集とデータベースの構築[8]

メタデータの中でも注目されるのが、携帯電話の位置情報を活用する分析手法である。

NSA は、スマートフォンを含む世界中の携帯電話の位置情報を、毎日５０億件近くも収集して、それを FASCIA という位置情報データベースに蓄積しているという。同一の携帯電話から毎日複数の位置情報を入手することとなるので、携帯電話５０億台の位置情報を収集している訳ではないが、億単位の携帯電話に関する情報を収集していると見られている。

収集する位置情報は、DNR(Dialed Number Recognition)データと DNI(Digital Network Intelligence)データ の２種類である。DNR データとは、電話通信網自体から収集されるデータである。即ち、通話を可能とするためには携帯電話端末に関する情報を、現在どの通信塔と通信接続可能であるかを含めて、システム上登録しておく必要がある。そのシステムは現在 SS7（Signaling System No7、No7 共通線通信方式）という、世界の公衆交換電話網で使われている電話接続管理の通信プロトコールによって管理されている。これにより、電源を入れて携帯電話をネットワークに接続する際、或は通信圏（塔）を移動する際には、その情報がシステム上登録されるが、そのデータを収集しているという。この収集は、既に収集プラットフォームで述べた通信基幹回線等から行っている。例えば、「ストームブリュー」という計画では、米国通信会社同士の電話回線接続点(OPC/DPC pairs)２７ヶ所からデータを収集しているという。通信回線構成の技術的特徴から、少数の通信会社の協力を得るだけで、他社の契約者の携帯電話情報にもアクセスできるという。

DNI データは、デジタル通信網から位置情報を取得するものである。スマートフォンでは、その現在地に対応して最寄りのレストランや公共施設を案内するなど、現在地に対応した各種の情報サービスが提供されているが、そのため端末のＩＰアドレスと位置情報がグーグル初めインターネット関連事業者に送信されている。端末の位置情報は端末搭載の GPS により取得されることが多いと考えられるが、GPS 情報が無くても、WiFi データ或は複数の通信塔からの三角測量により算出されている。ＩＰアドレスと位置情報を自動収集するシステムは、「ハッピーフット」計画と呼ばれている。

---

[8] Barton Gellman and Ashkan Soltani, “NSA tracking cellphone locations worldwide, Snowden documents show,” *The Washington Post,* 5 December 2013, accessed 6 December 21014,
http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
--Ashkan Soltani and Barton Gellman, “New documents show how the NSA infers relationships based on mobile location data,” *The Washington Post,* 10 December 2013, accessed 12 December 2013,
http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/

更に、データ収集の方法としては、携帯電話から発せられる電波自体を捕捉する方法もあり、具体的には海外の米国外交施設でアンテナを設置して収集するやり方（SCS特別収集サービス）や、航空機からの機上収集もあるとされる。機上収集は、滞空時間の長い無人飛行機を活用していると推定できる[9]。

イ　各種分析手法、特に同伴者分析（Co-Travel Analytics）

位置情報を含むメタデータの分析手法は多岐に亘る。

○　先ず、簡単なものとしては、テロ容疑者やスパイ容疑者など監視対象者の行動把握に使用する。監視対象の保持する携帯電話が特定できていれば、その者の行動を居場所を含めて把握することが可能である。

○　また、不審人物の割出しにも使える。即ち、携帯端末に関する「通信保全活動」（自分の携帯端末に対する監視を警戒して行なう行動）それ自体を自動的に捕捉し抽出する。通話時だけ電源を入れる者（逆に言えば、頻繁に電源を切る者）、幾つかの携帯電話を使い分ける者（一つの携帯電話の電源を切り、近くで別の携帯電話の電源を入れる行動）、会合地点近くで電源を切る行為（近くで複数の携帯電話の電源が相前後して切られる）、使い捨て携帯電話の使用、これらの行為を自動的に検索するシステムがあると言われる。

○　或は、特定船舶の乗員の割出しの例もある（特定船舶の寄港地毎に寄港時間中の携帯電話を割出す）。

この他、同伴者分析という分析技法と自動システムがあり、これについては2012年10月付のNSA内部資料「同伴者分析の概要」[10]が詳しい。これは、位置情報データベース（FASCIA）を活用して、既把握のテロ容疑者や諜報対象者から未把握のテロ容疑者や諜報対象者を割り出すプログラムであるが、その時点で使用中或は開発中の分析アルゴリズム１２個の概要をまとめて紹介した資料である。なお、各種技法の開発は、主としてNSAによってなされているが、米国家地理空間諜報庁NGAや豪信号局ASD

9　最近の報道によれば、米国司法省は、2007年以来、犯罪人の逮捕やインテリジェンス目的で、米国内でセスナ機を使用して上空から携帯電話の位置情報を収集している。そのため全米で少なくとも５つの飛行場からセスナ機を飛ばしており、人口の大部分をカバーできるという。そのシステムは携帯電話の位置を１０フィート以内の精度で特定し、且つ、必要であれば携帯端末から記録文章や写真を取得することが可能であるという。
--Gail Sullivan, “Report: Secret government program uses aircraft for mass cellphone surveillance,” *The Washington Post,* 14 November 2014, accessed 18 November 2014, http://www.washingtonpost.com/news/morning-mix/wp/2014/11/14/report-secret-government-program-uses-aircraft-for-mass-cellphone-surveillance/

10 ス資料　NSA, S215, *Summary of DNR and DNI Co-Travel Analytics*, 1 October 2012, accessed 12 December 2013, http://www.documentcloud.org/documents/888734-cotraveler-tracking-redacted.html#document/p1

の他、民間企業も協力しているとされる[11]。１２個の分析アルゴリズムの中から幾つかを紹介すると次の通り。

① 「チョークファン」分析

一定期間中に既把握対象者と類似の行動を取る者（位置情報が一致する者）を割り出すプログラム。位置情報の一致度合いをどれ程に設定するかは、分析者の裁量が可能。

② 豪 ASD 開発の同伴者分析

既把握対象者の移動を地図上の道路等へ投影して、経路分析を加えて、未把握の対象者を把握しようとする分析手法。更に不審な通信保全行動を加味した分析手法も開発中。

③ 国家地理空間諜報庁 NGA による分析

二人の当事者がどこかで会合した可能性があるか否かを検証するプログラム。

④ 海外エージェントが監視下に置かれていないかを点検するプログラム

CIA など諜報機関の海外駐在員が監視されていないかを点検するため、当人から実際の行動の詳細情報の提供を受け、これを尾行するような行動を取る者がいるかどうかどうか分析するもので、追跡者（Fast-Follower）分析と呼ばれている。

⑤ スラーヤ携帯電話対応の同伴者分析

中近東ではスラーヤ携帯電話（衛星通信と地上波通信を併用）の利用が増大しており、これに対応して NSA と NGA が共同で開発したもの。対象とするスラーヤ携帯電話と類似する移動を行うスラーヤ携帯電話を割り出すプログラム。

以上、同伴者分析の一部を記載したが、一部を見ただけでも、位置情報データが広汎に活用されているのが分かる。

（５）「ＩＣリーチ」プログラム[12]

---

[11] Gellman and Soltani, “NSA tracking cellphone locations worldwide・・・” *The Washington Post.*

[12] 主要な資料は次の通り。

--Ryan Gallagher, “The Surveillance Engine: How the NSA Built Its Own Secret Google,” *The Intercept,* 25 August 2014, accessed 5 September 2014, https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

--ス資料 NSA、*Sharing Communications Metadata Across the U.S. Intelligence Community—ICREACH*, 15 May 2007, accessed 5 September 2014, https://firstlook.org/theintercept/document/2014/08/25/sharing-communications-metadata-across-u-s-intelligence-community

--ス資料 NSA、*CRISSCROSS/PROTON Point Paper,* 22 February 2006, accessed 5 September 2014, https://firstlook.org/theintercept/document/2014/08/25/crisscross-proton-point-paper

--ス資料 NSA、*Memorandum for the DNI-- Sharing Communications Metadata Across the U.S. Intelligence Community,* undated, accessed 5 September 2014,

ア　「ＩＣリーチ」の概要

「ＩＣリーチ」とは、NSA が責任部署として管理運営する諜報コミュニティ全体のための通信メタデータの分析システムである。中核組織は、NSA、CIA、FBI、DIA、DEA（麻薬取締局）の５機関であるが、2010 年現在、利用できる分析官は米国政府 23 機関で 1000 人以上に及ぶとされる[13]。

メタデータ提供の中心は NSA であり、運用を開始した 2007 年現在、NSA が世界各地から様々な手法（５０以上という）で収集した通信メタデータ数兆件の中から、8500 億件のデータが分析利用可能であり、更に、毎日１０億から２０億件のデータが利用可能データに追加されているという。また、メタデータ収集の対象は、Ｅメール、通話、ファクス送信、インターネット・チャト等であり、データ項目は３３個で携帯電話や衛星電話については位置情報も含まれている。

使用方法は、容易であり、特定の電話番号やＥメールアドレスを入力すれば、指定期間内にその特定者と通信した者の一覧表が提示されるとされる。また、このシステムにより、対象者の生活パターンの分析が可能であり、通話通信の相手方、訪問先、生活習慣や将来の行動予測もできるとされている。利用法が簡便で効果が高いためか、2010 年 7 月に CIA の犯罪・薬物対策センター(CNC)の分析官にシステムの教育をしたところ、大好評であり、同年９月には CIA の大講堂で 100 人の分析官に再度教育を行ったという[14]。

「ＩＣリーチ」システムの必要費用は、毎年 250 万から 450 万ドルとされる。

なお、この「ＩＣリーチ」システムは、既存の「グローバルリーチ」システムに必要な修正を加えたものである。「グローバルリーチ」とは、NSA が UKUSA 協定諸国５カ国用に構築したメタデータの分析システムであり、英国 GCHQ、豪州 ASD 等の諸機関が使用を認められている。

イ　「ＩＣリーチ」前史

諜報コミュニティのためのメタデータ分析システムとしては、「クリスクロス」[15]と

---

https://firstlook.org/theintercept/document/2014/08/25/decision-memorandum-dni-icreach

[13]　分析官の数が多く、また多くの機関に跨っているためか、「ＩＣリーチ」利用のための通信回線は、シギント専用の通信システムである NSANet ではなく、国防総省の JWICS 通信網を使用している。この点からも、同じトップ・シークレットでもシギント情報の秘匿度の程度が高く設定されているのが理解できる。

[14] ス資料 NSA, *CIA Colleagues Enthusiastically Welcome NSA Training,* 21 September 2010, accessed 5 September 2014,
https://firstlook.org/theintercept/document/2014/08/25/cia-colleagues-enthusiastically-welcome-nsa-training

[15] DEA によるメタデータ収集については、最近、裁判記録と関係者の匿名取材に基づいて詳細な報道がなされた。それによれば、DEA は、1980 年代コロンビアの麻薬カルテル対策で、協力者や潜入捜査官による捜査（ヒューミント）では成果が上がらないため、米国とコロンビア

いうものがあった。これは、1990 年に CIA が DEA（麻薬取締局）と協力して構築したもので、電話料金請求のための通話記録を収集してデータベース化したものである。データとしては、通話日、通話時刻、通話時間、発信電話番号、受信電話番号の５項目のみであったが、中南米の麻薬密輸事件捜査に極めて有効であったという。

そこで、1999 年までには、NSA、FBI、DIA がメンバーに加わり、データ提供・システム利用の両面で参加した。そして、「クリスクロス」には「プロトン」という機能が追加され、上記の５項目の情報の他に、携帯電話や衛星電話に固有のデータ項目や CIA による分析レポートの抜粋情報も追加されたという。これにより、「クリスクロス/プロトン」システムは、中南米の麻薬密輸対策だけでなく、一般的な対外諜報、テロ対策、防諜の各方面で活用されるようになり、海外所在テロ容疑者の CIA による秘密の誘拐連行作戦にも貢献するなど、重要なシステムであった。

2005 年頃には、この「クリスクロス/プロトン」の拡張増強が課題となっていたようであるが、NSA は既に大量のメタデータ分析のためのシステムと高度な能力を保有しており、アレクサンダーNSA 長官（当時）が、NSA 主導での新システム構築を提案したとされる。2007 年時点では、「クリスクロス/プロトン」システムのメタデータの保有件数が 1490 億件（内 NSA 提供データが約 500 億件）であるが、「IC リーチ」では発足時からして NSA の提供データ件数が 8500 億件以上であるので、NSA 主導になるのは自然なことであろう。

（６）「ドローン」攻撃と NSA[16]

等関係国間の国際電話のメタデータ分析を開始した。その有効性が確認されたため、収集データの拡大を始め、1992 年には米国と特定国間の国際電話の全通話のメタデータの収集を開始した。収集は国際電話事業者に対して DEA から行政令状を発出して行うもので、裁判所は関与していない。収集対象は、徐々に拡大し、最盛期には 116 ヶ国、中南米カリブ海の殆どの国、カナダ、西アフリカ諸国、欧州（イタリアを含む）、アジア（アフガニスタン、パキスタン、イランを含む）に及んだという。ところが、2013 年 6 月のスノーデン告発後、同年 9 月に司法長官の指示でプログラムは停止された。現在は、容疑電話番号（１千件程度）との通話に限定してメタデータを収集しているが、効率性は低下したとされる。

なお、「クリスクロス/プロトン」データベースは、「ＩＣリーチ」システムに統合された訳ではなく、少なくとも 2013 年 9 月までは存続している。

--Brad Heath, “U.S. secretly tracked billions of call for decades,” *USA Today,* 8 April 2015, accessed 10 April 2015,
http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

--Kevin Johnson, “Feds kept separate phone recored database on U.S. calls,” *USA Today*, 16 January 2015, accessed 20 April,
http://www.usatoday.com/story/news/nation/2015/01/16/phone-database-justice/21868063/

[16] Jeremy Scahill and Glenn Greenwald, “The NSA’s Secret Role in the U.S. Assassination Program,” *The Intercept*, 10 February 2014, accessed 20 October 2014,
https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/

ドローン（無人航空機）による攻撃自体は、米軍或は CIA の任務であり、NSA の任務ではない。しかし、実際上は NSA が深く関与している。スノーデンの NSA 幻滅の一因でもあるので、その関与の実態について述べる。

ア　米軍には、合同特別作戦司令部（Joint Special Operations Command）指揮下のドローン攻撃部隊があり、他に CIA もドローン攻撃部隊をもっている。これらは、アフガニスタンやイエメン、ソマリア、パキスタン等で「テロリスト」に対して空からのドローン攻撃を行っている。そして、ドローン攻撃は、NSA の参加無しにはなし得ない程 NSA が深く関与している。

イ　標的決定

先ず、標的決定は各種情報を総合して行われているとされるが、アフガニスタンの様に現地に米軍の基地が置かれ、一定のヒューミントが可能な所は別として、米軍の地上での拠点が無いところ、即ち、イエメン、ソマリア、パキスタン等では専らシギントに依存することとなり、シギントでもメタデータ分析の比重が高いとされる。必ずしも全ての標的決定において通信内容から確証を得て「テロリスト」との判定が下されている訳ではないとされる[17]。

ウ　標的の位置評定

次に実際にドローン攻撃をするには、先ず標的を特定する必要がある。そのため NSA には位置評定室（Geolocation　Cell）が設置され、攻撃の際には標的の位置評定を担

--Dana Priest, "NSA growth fueled by need to target terrorists," *The Washington Post,* 21 July 2013, accessed 21 October 2014,
http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

本文に記載した他、前者の記事によれば、CIA のドローンには「シェナンギガンス」というシステムが搭載されおり、これを使用すれば、6000 メートル離れた上空から地上の WiFi 通信などの無線 LAN 通信を全て傍受できるという。2012 年 3 月から始まった「ヴィクトリーダンス」という CIA・NSA 共同の任務では、オマーンの基地を拠点にイエメン内の主要な町全ての WiFi 通信の地図を作成したとされる。

また、後者の記事によれば、NSA は 2004 年 9 月に電源を切ってある携帯電話についても発見する技法を開発したとされる。但し、その詳細は不明である。

[17] 2012 年 10 月ドローンによるグル（当時アルカイダの軍事部門責任者）殺害は、（単なるメタデータ分析ではなく）、シギントの総合的運用により当人を特定し殺害し、且つそれを確認した例として報道されている。
--Greg Miller, Julie Tate and Barton Gellman, "Documents reveal NSA's extensive involvement in targeted killing program," *The Washington Post*, 16 October 2013, accessed 21 January 2015,
http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/....story.html

当している。位置評定室の NSA 職員は、標的の持っている携帯電話のシムカードその他端末を特定する情報を与えられると、ドローンに搭載されている「ギルガメシュ」システムを使用してその電波を捕捉し受信して誤差１０メートル以内で位置を評定（Find）、更に、（位置評定室に派遣された）地理情報の専門家である NGA（国家地理空間諜報庁）職員が実際の地理上で標的を決定（Fix）、それに従い、ドローン操作員が爆撃をする（Finish）という。

エ　「テロリスト」による対抗措置と誤爆

ところが、「テロリスト」もドローン攻撃の手法を知るようになり、対抗措置を採るようになったという。某タリバン指導者は、仲間が会合するとその場で各人の携帯電話のシムカードを供出してランダムに交換するなどして、米側の分析の混乱を図っているという。逆に、米国のドローン攻撃の仕組みを知らずに、自己の携帯電話を友人や家族に貸したりすることもある。これらのため、携帯電話で標的を特定しているドローン攻撃では、本来の意図した標的ではない、一般住民を誤爆してしまう可能性があり、これは相当数に及んでいるとも言われる。（なお、パキスタンの一部は米国により「戦闘地域」と指定されており、同地域では、他に「シグニチャー攻撃」というより簡便な標的決定手法が許されているため、更に誤爆が多くなっていると言われる[18]。）

このように NSA は、単に情報を収集する諜報機関ではなく、作戦支援も行う組織であり、その一つの現われが、「ドローン攻撃」への参画である。その運用の適否、道徳的価値判断は別として、米国の軍事力を支える諜報機関、特に NSA の存在の大きさを示す一例である。

18　「シグニチャー攻撃」とは、「テロリスト」の特徴を示す一定の行動類型を取る者を「テロリスト」と看做して攻撃を認めるものである。問題はテロリストの特徴を示す行動類型の定義であり、20～40 才の武装した男で一定の行動を取ればテロリストと認定するようである。
--Arianna Huffington, "'Signature Strikes' and the President's Empty Rhetoric on Drones," *Huffington Post*, 10 July 2013, updated 9 September 2013, accessed 20 November 2014, http://www.huffingtonpost.com/arianna-huffington/signature-strikes-and-the_b_3575351.html

2　分析ツール

分析ツールとしては、数年前に開発配備された XKeyscore というシステムが極めて重要であるので、これについて述べる。また、Boundless Informant というシステムは 2013 年 6 月に大きく報道されたので、その実態について述べる。

（1）XKeyscore

ア　XKeyscore とは何か

XKeyscore とは、NSA が様々な方法によって大量に取得するデータの一次記憶装置であり、また、この一次記憶装置から必要なデータを検索抽出し分析するための分析システムである。このシステム概要について、2008 年 2 月付 NSA 内部資料と内部資料を分析した報道を元に説明する[19]。

イ　システム概要

XKeyscore の一次記憶装置は、世界中の約 150 ヶ所の拠点に配置されたサーバー700 以上で構成される。サーバーの主な配置場所は、内部資料では特別資料源作戦（SSO）の拠点、外国衛星通信の傍受拠点、特別収集サービス（SCS）の三種類が挙げられている。

第 2 部第 2 章の収集態勢で説明したが、NSA の主な収集プラットフォームには、

① 「プリズム」計画
② （主として SSO による）通信基幹回線からの収集
③ 外国通信衛星の傍受
④ 特別収集サービス（SCS）
⑤ CNE(コンピュータ・ネットワーク資源開拓)

の大きく五つが挙げられる。

この内、①「プリズム」計画は、既に（第 2 章の 2 で）説明した様に、極めて情報価値の高い有用な計画であるが、データ要求はある程度絞り込まれているため、取得した

19　主たる出典資料は次の通り。
--ス資料 NSA、*XKEYSCORE,*　25 February 2008, accessed 1 August 2013, http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
--Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*, 31 July 2013, accessed 1 August 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
--Konrad Lischka and Christian Stoechker, "'Real Time': New Leaks Show Near Total Surveillance," *Spiegel Online,* 1 August 2013, accessed 17 August 2013, http://www.spiegel.de/international/world/new-nsa-leaks-describe-total-surveillance-system-xkeyscore-a-914244.html

データは、XKeyscore 一次記憶装置ではなく、NSA の基本的な記憶装置の「マリーナ」「メインウェイ」「ピンウェイル」「ニュークレオン」に直接記憶される。また、（上記には列挙しなかったが）愛国者法 215 条に基づき収集した米国内電話メタデータも、直接「メインウェイ」に記憶されると推定できる。更に、CNE で収集したデータも、特定のネットワーク資料源を標的にして収集した情報であるため、データの特定性が高く、この XKeyscore 一次記憶装置には記録されないと考えられる。従って、残りは②③④であり、これは内部資料で記載された XKeyscore データサーバーの設置場所の記述と一致する。

そして既述したように、世界中の特別収集サービス SCS の収集拠点は（遠隔収集を除くと）８０ヶ所弱、外国衛星通信の傍受拠点は（SCS との重複を除くと）１３ヶ所程度、合わせて約９０ヶ所である。従って、残りの約６０ヶ所は SSO による通信基幹回線からの収集拠点ということになる[20]。なお、通信基幹回線からの収集は、狭義の SSO によるもののみか、或は、セカンド・パーティ、サード・パーティ、その他の単独事業を含むのか、内部資料だけからは明確ではないが、基本的にはこれらも含んでいると考えるのが合理的であろう。

これらの資料源における収集の特徴は、データを大量に取得していることであり、大量取得したデータをそれぞれの収集拠点において一次記憶装置に記憶し、これらのデータの中から必要なデータを検索抽出する構造となっている。そして、この検索作業のため XKeyscore ウェブサーバーが構築されており、分析官はこのウェブサーバーを活用して必要なデータを世界中の一次記憶装置 700 台以上から検索抽出を出来るようになっている。

ウ　収集・記憶データ

各収集拠点では、アクセスできるデータの中から、資料価値が無いと考えられる形式のデータを自動的に削除する。インターネット回線の通信では音楽や映画のダウンロードなどデータ量は極めて多いが情報価値は低いものが相当量を占めると言われており、これらを排除(Massive Volume Reduction)して、その他のデータを一括して収集するのである。そして、一括収集されたデータは、E メールなり、VoIP なりの形式に復元され、メタデータの索引が付されて記憶される。また、これらのデータ中、既にデータ要求リストに登録されている E メールアドレス、IP アドレス、物理（MAC）アドレスなどの通信データは、抽出されてデータ要求者に提供される。

ある分析報道によれば、このようなデータの抽出収集システムは、ボーイング社の子

---

[20] 但し、2008 年の内部資料では、XKeyscore の資料源として、シギント衛星や軍用機の機上収集（Overhead collection）も上げられている。これが正しいとすれば、通信基幹回線からのデータ収集拠点は６０ヶ所よりは少なくなる。５０ヶ所程度であろうか。
--ス資料、“XKeyscore Sources,” circa 2008, SVT, accessed 23 April 2015, http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa

会社 NARUS が提供している可能性が高いとしている[21]。

一次記憶装置は、所謂「ローリング・バッファ」方式を取っており、収集拠点毎にサーバーの記憶容量の範囲内で、常に、新しいデータで古いデータを上書きしつつ、最大量のデータを保管しているとされる。データの保存目標期間は、コンテンツ・データで３日間、メタデータで３０日間である。但し、実際の保存期間は、拠点のサーバーの容量によって異なり、コンテンツ・データが３日から５日間保存されている拠点もあれば、２４時間しか保管できないこともあるという。

なお、対外諜報監視法 702 条に基づく特別資料源作戦 SSO による米国内収集では、米国人の情報を収集しないように制約がかかっている（従って、米国人間の通信は通常削除された形で NSA に提供されることとなっている）ため、国外に於けるよりも収集データは制限されていると見られる。

このようにして収集保管されているデータ量は、2007 年の NSA 内部資料によれば、当時、通話で 8500 億件とインターネット通信 1500 億件の記録が保管されており、毎日 10～20 億件の新規データが追加されていたという。

エ　NSA のデータベース構造

既述したように、NSA の基本的データベースには、次の４つがある。

- 「マリーナ」（デジタル通信メタデータ）
- 「ピンウェイル」（デジタル通信コンテンツ）保存期間５年
- 「メインウェイ」（電話メタデータ）
- 「ニュークレオン」（電話ボイス・コンテンツ）

これに対して、XKeyscore は世界各地の収集拠点でメタデータとコンテンツ・データを一次的に記録する「バッファー記録装置」であるが、保存期間は基本的にメタデータで 30 日間、コンテンツ・データで３日である。期間経過に伴い新しいデータで上書きされ消去される。

この XKeyscore は、データベースとしては新しく構築されたものである。例えば、Ｅメール・データであれば、メールアドレスやＩＰアドレス等から判断して情報価値があると判定されれば、自動的に「ピンウェイル」に記録保存されるが、これは各収集拠点で処理した通信の５％にも満たない。従来、その他の通信は廃棄されてきた。それが XKeyscore の構築により、従来であれば即時に廃棄されていた通信データも含めて「バッファー記録装置」に一定期間記録されるようになったのである。これによって、従来よりも広汎なデータの検索抽出が可能となったのである[22]。

---

[21] “INCENSER: or how NSA and GCHQ are tapping cables,” *Top Level Telecommunications*, 29 November 2014, updated 30 November 2014, http://electrospaces.blogspot.jp/2014/11/incenser-or-how-nsa-and-gchq-are.html

[22] ス資料 NSA slides, in “Read the Snowden Documents From the NSA,” *SVT,* 11 December

オ　検索・分析方法

XKeyscore を使ったデータの検索抽出と分析方法には次のものがあり、極めて有効であるという。

2013 年 6 月に、スノーデンがインタヴューで「メールアドレスが分かれば、その個人のメールを読むことができる。」と語っていたのは、正にこの XKeyscore のシステムのことである。

①　「ストロング・セレクター」のある場合

- 標的を容易に特定できる情報、即ちメールアドレス、IP アドレス、物理（MAC）アドレスや電話番号が判明しているような場合には、これによって XKeyscore ウェブサーバーを使用して検索すれば、典型的なユーザーがインターネットで行う殆どの活動に関するデータを取得できる。例えば、標的の E メールの内容、オンラインでのチャット、或はウェブサイトの閲覧履歴、ネットでサーチした検索単語、グーグルマップの検索利用状況などのデータを取得できる。
- また、「リアル・タイム」で標的がインターネットで行っている活動の傍受、監視も可能である。

②　「ソフト・セレクター」しかない場合

しかしながら、標的を特定できるデータを保有している場合は、必ずしも多くはない。その場合でも様々な検索分析を活用することにより、ウェブ空間で特異な活動を把握できるのが XKeyscore の利点である。特にメタデータの検索分析により、閲覧すべきコンテンツ・データを絞り込むことができる。それによって、直接的に情報成果を得ること、或は標的の特定「ストロング・セレクター」の入手に至る場合があるとされる。

データの抽出分析方法については、2008 年内部資料で説明されており、その内の幾つかを紹介すると次の通り。

- イランからの暗号化ワード文書通信リスト、或は、イランに於ける PGP（Pretty Good Privacy）暗号の利用通信リストを、検索抽出し、その中から情報価値のありそうな個別通信を抽出して分析する。
- 標的はドイツ語を話すが現在パキスタンにいるという場合に、パキスタンでのドイツ語通信リストを検索抽出し、その中から情報価値のありそうな個別通信を抽出分析する。
- テロリストがグーグルマップを利用して、攻撃対象の調査活動やテロ準備をする場合に、グーグルマップの検索利用状況（利用状況のテロリスト的特徴）から、特

2013, accessed 8 April 2015,
https://www.documentcloud.org/documents/894406-nsa-slides-xkeyscore.html

定の対象（容疑者）を検索抽出する。

- テロリストが作成した文書がインターネットで世界中に広まっている場合に、その作成者と作成場所を特定する。
- 特定国に於いてデータ収集可能な端末、システムを把握する。（TAO グループ作成のデータが XKeyscore に搭載されており可能。）
- 英語、中国語、アラビア語の通信に関しては、通信内容中のキーワードによる通信の検索抽出が可能。（例えば、オサマ・ビン・ラデンに言及した全ての通信の検索抽出）
- 特定の単語で検索をした者や特定のウェブサイトを閲覧した者を検索抽出する[23]。

ここに紹介したのは検索分析手法の一部であって、他の分析手法も可能であり、XKeyscore は極めて有用なシステムである。そこで、NSA 内部資料によれば、ドイツの連邦憲法擁護庁 BfV 副長官からの要請を受け、2013 年 3 月に XKeyscore ソフトウェアをテロ対策のため BfV に対しても供与することが決定された。但し、XKeyscore の技術的専門性に鑑み、その利用については既に供与を受けている連邦諜報庁 BND が技術的支援をすることとなっていた[24]。

カ　検索・分析方法～～追記

ウェブサイト The Intercept は、2015 年 7 月、XKeyscore による検索・分析手法に関する 1300 頁近い大量の NSA 内部資料を公表した[25]。

これらの資料によれば、XKeyscore システムとは正に NSA のデータ検索のための「グーグル」のようなもので、凡そ分析官がこういう検索をしてみたいと考えるものは全て可能になっていると言っても過言ではない程、極めて広汎なデータの検索ができるようになっている。上記オで述べた検索・分析方法は、正に全体の極く一部に過ぎない。

余りにも多様な検索・分析手法であるので、ここで全体について記述することは控えるが、一点だけ興味深い資料について述べる。それは、2011 年 3 月付の内部資料

---

[23] この例示は、2008 年資料ではなく、2010 年の使用の手引に記載されている。
--Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*.

[24] ス資料抜粋、"Document excerpt on the sharing of the NSA spy tool XKeyscore with BfV," *Spiegel Online*, undated, accessed 20 June 2014,
http://www.spiegel.de/media/media-34045.pdf
同、"Secret document on the cooperation between the NSA, BND and BfV in the fight against terrorism," 8 April 2013, accessed 20 June 2014,
http://www.spiegel.de/media/media-34046.pdf

[25] Morgan Marquis-Boire, Glenn Greenwald and Micah Lee, "XKeyscore: NSA's Google for the World's Private Communications," *The Intercept,* 1 July 2015, accessed 2 July 2015,
https://firstlook.org/theintercept/2015/07/01/nsas-google-worlds-private-communications

XKEYSCORE for Counter-CNE(XKeyscore による CNE 対策)[26]である。XKeyscore が、自らの CNE（コンピュータ・ネットワーク開拓）に活用できるのは当然のことであるが、本内部資料は、それに止まらず、第三国が行う CNE 活動を検知・発見して、これを利用し或は対抗手段をとるなど、CNE 対策での利用方法を説明したものである。XKeyscore は、それ程に力をもっているのである。

キ　成果

2008 年 2 月の内部文書によれば、XKeyscore を使用して作成した 2008 年までの情報成果によって、テロリスト 300 人以上の捕獲に繋がったという。

ク　余話～～2008 年ムンバイ・テロ事件

2008 年 11 月 26 日、インド最大の都市ムンバイで、パキスタンのイスラム過激派 10 人が計画的なテロ殺戮を敢行し、160 人以上（外国人２８人）を殺害し、300 人以上を負傷させた。

英米印の関係国の諜報諸機関は、テロを予想はしていたもののその抑止には失敗したが、事件発生時には、事件前からのシギント活動による情報及びデータ収集態勢が事案対処に貢献し、且つその後の同事件の実態解明に大きく貢献した。特に、英国 GCHQ はそのデータの検索分析に XKeyscore を使っていたと見られる。そこで、XKeyscore とテロ対策の理解に資するため、スノーデン資料や諜報関係者のインタヴューに基づく報道[27]を元に、同事件関連の GCHQ のシギント活動を紹介する。

①　テロ事件の概要

ラシュカル・エ・タイバは、パキスタンに拠点を置くイスラム過激派であるが、1990 年台にパキスタンの軍統合諜報局の（武器、資金、諜報、戦闘技術、通信技術等の）支援を受けて、成長したとされる。攻撃対象は、元々はインドであったが、次第に欧・米・オーストラリアをも対象とするようになった。

これがインド攻撃を計画し、欧米人やユダヤ人も同時に攻撃できるインド最大の都市ボンベイを標的に選んだ。攻撃参加者は、厳しい軍事訓練、コマンド訓練を受けた１０人が選ばれた。

この１０人は、2008 年 9 月中旬には、ボンベイの攻撃目標について情報ブリーフィングを受けているが、その際には、グーグルアースを使用したり、また、パキスタン系

---

[26] ス資料 NSA, “XKEYSCORE for Counter-CNE,” March 2011, accessed 2 July 2015, https://firstlook.org/theintercept/document/2015/07/01/xks-counter-cne/

[27] Sebastian Rotella, James Glanz and David E. Sanger, “In 2008 Munbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle,” *Pro Publica*, 21 December 2014, accessed 24 December 2014, http://www.propublica.org/article/mumbai-attack-data-an-uncompleted-puzzle

米国人が現地偵察をして入手したビデオや地図等が使用されたという。

攻撃は、天候等の理由で、９月下旬と１０月と２回延期されたが、遂に１１下旬に実行に移された。１０人はパキスタンのカラチ付近からアラビア海に出て、インド漁船を乗っ取り、これを使ってボンベイ近海にまで到達（漁船員は全員殺害)。その後ゴムボートでボンベイに上陸し、ここで概ね二人ずつに分かれてそれぞれの攻撃対象を攻撃した。使用武器は、自動小銃 AK47 の他、（中国製の）手榴弾、爆弾である。主たる攻撃対象は、ボンベイの（欧米人の宿泊客の多い）高級ホテル２軒（タージ・マハールとオベロイ・トライデント)、ユダヤ教徒のホテル（ハバド・ハウス）と中央駅であるが、その他にも有名なカフェや病院を攻撃、或は時限爆弾をタクシー内等に設置し爆発させている。攻撃は２６日夜に始まり、完全鎮圧には２９日朝までかかった。

この間、攻撃者はカラチ郊外の司令部と VoIP でリアル・タイムに通話しながら、司令部の指示を受けて攻撃をしていた。

この攻撃においては、立案と実行に於いて３０歳のコンピュータ技術者ザラル・シャーが大きな役割を果たした。彼は、２０歳代でラシュカルのメディア責任者となったが、その専門能力を活かして、イスラム過激派の中でインターネット使用のパイオニアと言われる存在になったという。この攻撃に於いても、立案段階ではインターネットを情報収集に活用している。また、攻撃実施中にカラチ郊外の司令室から攻撃実行者と時々刻々と連絡を取れるように、事前に VoIP による通話経路を設定している。それも、通信経路を秘匿するため、米国ニュージャージー州の通信会社と契約するなどして、カラチの司令部とムンバイの攻撃実行者の通話を秘匿する工作をしている。更に、攻撃実施中は、テレビやインターネットを使って、ボンベイ市内や本事件に関連する情報を収集して、首領による攻撃指示を支援している。その司令部と攻撃者間の会話が一部公開されているが、正に、攻撃する方も、インターネット時代のインフラを十分に活用しているのである。

② シギント機関、特に英 GCHQ の対応

インドや米英諜報機関は、2008 年初にはボンベイに於ける何らかのテロ攻撃の可能性を示す状況を認識しており、米英印のシギント機関はそれぞれ情報収集に努めていたというが、テロの具体的な時期と方法は不明であった。

そういう中で、９月迄には GCHQ はラシュカルのインターネット活動の監視を開始しており、先に述べたザラル・シャーがインターネットを使用して準備活動をしているのを把握していた。即ち、通信秘匿に関するウェブ閲覧や検索と共に、米国ニュージャージー州内の通信会社との契約、更には、ムンバイ市内の高級ホテルやユダヤ教ホテル、或は上陸予定地点等に関するグーグルアースやウィキマピア等を使った情報収集活動を把握していたという。

しかしながら、ザラル・シャーによるウェブ活動はこれだけではなく、その他の地域

にも広汎に及んでおり、ボンベイ攻撃の特定までには至らなかったとされる。即ち、ザラル・シャーは、この他にも、インドの観光施設や軍事施設、カシミール地方、ニューデリー、アフガニスタン、在独米陸軍、カナダ等についても、インターネットを使用して情報収集をしていたという。

また、米英印の諸機関は、事件発生前までは、本件に関して情報交換をしたことがなく、仮に事前にそれぞれの情報を持ち寄っていれば、結果は変わっていたかも知れないと指摘されている[28]。

こうして、テロ攻撃抑止には失敗した。しかし、事件発生後は、米英印の諸諜報機関は即座に協力関係を構築して、事件対処に貢献したと言われる。実際、ラシュカルのカラチ司令部と攻撃実行者の通話が公表されている位であるから、米英印当局はこれをリアル・タイムで収集していたと考えられる。更に、カラチ司令部におけるインターネットの利用についても、リアル・タイムで監視していたと考えられる。これらの情報は、事案対処に活用されると共に、事件の全体像を追及する事後捜査にも不可欠であった。実際、ラシュカルは犯行をインド国内のテロ組織によるものと見せかける偽装工作もしていたのである。しかし、米英印は、シギントのお蔭で、事件進行中に既に、カラチにいる事件の首謀者２人を特定していたという。シギントがなければ、パキスタン政府にラシュカルの犯行と認めさせることは出来なかったであろう。

今や、テロを実行する方もインターネットを活用し、これに対処するにもウェブ空間に対するシギント能力が不可欠の時代となったのである。

（２）Boundless Informant

ア　Boundless Informant とは何か[29、30]

28　上記註の Rotella, Glanz and Sanger, “In 2008 Munbai Attacks,…” *Pro Publica* に引用されている NSA 内部資料抜粋をみると、事件後の NSA による事後的分析ではあるが、「ザラル・シャー一味は、グーグルアースとウィキマピアを使って偵察分析を行っており、ザラル・シャーの閲覧習慣を分析すれば、事件前にも攻撃対象を推定し且つタージマハール・ホテルへの侵入口も推定できた。・・・閲覧習慣の行動分析は攻撃作戦計画を導出することができた。ザラル・シャーの完全な閲覧履歴を詳細に分析したところ、将来の攻撃対象となり得る他の対象を発見することができた。」と述べている。

29　主な参考資料は次の通り。

--“Boundless Informant NSA data-mining tool – four key slides,” *The Guardian,* 8 June 2013, accessed 11 June 2013, http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides

--Glenn Greenwald and Ewen MacAskill, “Boundless Informant: the NSA’s secret tool to track global surveillance data,” *The Guardian,* 11 June 2013, accessed 9 July 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

--ス資料 *Boundless Informant-FAQ 09-06-2012,* 13 June 2012, accessed 18 June 2014, http://www.spiegel.de/media/media-34054.pdf

第２章の収集態勢で見たように、NSA は多様且つ膨大なデータを収集しているため、その全体像を知ることは職員でも容易ではない。そこで、その収集能力と実態をニア・リアル・タイムで知るために作られたシステムである。このシステムによって、次のようなことが分かるという。即ち、

・　対象地域に、どれだけの収集拠点を持ち、どれだけのデータを収集しているか。
・　特定国に対する収集手段と収集能力はどのようなものか。
・　特定収集拠点の収集能力はどのようなものか。

NSA は、シギント・インフラを通過するデータから、通話メタデータとインターネット通信メタデータを（それぞれ FASCIA と FALLOUT という二つのシステムで）抽出し、NSA 本部に送付しているとされるが、このシステムではそのデータを利用して、収集能力の全体像を分かるようにしている。

但し、このシステムには、NSA の収集能力の全てが反映されている訳ではなく、秘密保全上の配慮から秘匿度の高いデータは反映されていない。また、技術的な理由から含まれていないものもある。前者（秘密保全上の理由から除外されているデータ）では、「トップ・シークレット」の中でも、更に秘匿を要する特殊管理情報 ECI(Exceptionally Controlled Information)や（改正前の）対外諜報監視法に基づく収集は含まれないとされる。（ECI として具体的にどのようなデータが除外されるかは不明。改正前の対外諜報監視法による収集には、通信基幹回線からの収集の内「ブラーニー」計画が挙げられる。）　後者（技術的理由から含まれていないデータ）では、通信基幹回線からの収集の内「マスキュラー」計画が挙げられている。また、マイクロ波通信も含まれないようである。

このように例外はあるものの、XKeyscore の対象となっているデータの多くは含まれていると考えられる。

イ　特定国の収集能力で分かること

特定国に対する電話通話とインターネット通信のデータ収集量の月次変化を見ることができる。また、それを収集している収集拠点毎のデータ量、通信の種類毎のデータ

---

[30] Boundless Informant は、グリーンワルド氏によって、NSA が欧州の一般市民の通信を監視している例証として幅広く報道されたが、この解釈は誤りであると指摘されている。Boundless Informant には、主としてテロ対策のために NATO 諸国が収集し、米国と共有したメタデータも多く含まれているとされる。更にそのメタデータにはアフガニスタン等を対象に収集したものも含むとされている。
--“BONDLESSIMFORMAT: metadata collection by Dutch MIVD instead of NSA,” *Top Level Telecommunications*, 8 February 2014, updated 15 March 2014, accessed 15 March 2015, http://electrospaces.blogspot.jp/2014/02/boundlessinformant-metadata-collection.html
--“Dutch government tried to hide the truth about metadata collection,” 17 February 2014, updated 8 March 2014, accessed 15 March 2015, http://electrospaces.blogspot.jp/2014/02/dutch-government-tried-to-hide-truth.html

量を見ることができる。

ウ　Boundless Informant で見る収集力[31]

実際のデータ収集量は時期に応じて変動しているが、2013 年 3 月 8 日から始まる 30 日間で、世界中で、971 億件のＥメール、1248 億件の通話データの収集が本システムに記録されている。通話データのトップ 5 は、アフガニスタン 220 億件、パキスタン 138 億件、サウジアラビア 79 億件、イラク 70 億件、インド 63 億件である。

また、Boundless Informant によって米国の収集力の地域的傾斜を見ると、矢張り中近東（アフガニスタン、パキスタンを含む）に最大の力点が置かれており、次に、インド、中国、ロシアなどの諸国である。全体的に見て、日本は、独仏など欧州諸国と対比しても、データ量は少ない状況である。これは、日本に対する収集力の反映なのか、或は情報関心の反映なのかは、不明である。

[31] "Overview of the use of Boundless Informant (world map)," *Spiegel Online,* accessed 18 June 2014, http://www.spiegel.de/media/media-34061.pdf

３　暗号対策

暗号解読・暗号攻略は、シギント機関にとっては、秘中の秘であり、スノーデン資料においても、その全貌が分かるような資料は現在までのところ見られない。但し、一部ながら関連資料が報道されており、それらに基づいて可能な限り描写すると次の通りである。

（１）前史

米国は、NSA 発足前から多彩な方法により、暗号解読に取り組んできた（その一部は、第１部第２章２（１）「米国シギントの成果の歴史」で記述)。ここでは、NSA による現在の暗号対策の理解を助けるため、前史として、２点を紹介しておきたい。

ア　スイス暗号機メーカー「クリプト AG」の協力[32]

秘匿強度の高い外交暗号機を自力で製作するのは、嘗てはそれ程容易なことではなかったので、第二次世界大戦後、多くの国は外国民間企業の販売する製品を使ってきた。ところで、「クリプトＡＧ」は 1952 年設立のスイスの暗号機メーカーであるが、「性能」が良く且つ中立国に所在することもあり、その製品は、２０世紀後半の５０年間世界１２０カ国で使われ、採用国にはイラン、リビア、アルゼンチン、アイルランドも含まれたという。

ところが、実はこのクリプト社は、発足以来、米国 NSA や独 BND と密接な関係を持ち、また、米モトローラ社や独ジーメンス社とも協力関係を築いていたとされる。即ち、NSA の支援を受け、且つ NSA による暗号解読が容易になるように暗号機が作られていたのである。従って、このクリプト社の暗号機を採用してきた国々の外交暗号は全て米国 NSA によって解読可能であった。その情報成果の一部として次のものが指摘されている。

- 1982 年のフォークランド戦争では、英国はアルゼンチンの外交暗号解読により、情報優位に立てたこと。
- 1986 年西ベルリンのディスコ「ラ・ベル」爆破事件には、リビア政府の関与があったことを把握。
- 1988 年パンナム機の英国上空での爆破事件には、イラン内務大臣モフタシェミの関与があったことを把握。
- 1991 年元イラン首相バクティアルの暗殺（於パリ）には、イラン諜報機関の関与があったことを把握。

---

[32] Wayne Madsen, “Greatest Intel Coup of The Century?　The NSA’s Crypto AG,” *Covert Action Quarterly 63*, 30 January 1999, accessed 17 December 2014, http://rense.com/politics2/crypto.htm

なお、NSA に協力した暗号機メーカーは「クリプト AG」だけではなく、他にも多々あったとされる。

イ　「クリッパー・チップ」問題

1990 年代、暗号通信が民間にも普及する趨勢となったが、NSA は民間暗号通信に「クリッパー・チップ」（暗号鍵を組み込んだチップ）の使用を義務付けようとした。当然の事ながらそのチップ内の暗号鍵は権限ある当局による解読が可能となるものである。この構想は 1993 年にクリントン政権により提唱されたが、反対論が強く、1996 年には完全に放棄された。その結果、NSA は秘密裡に暗号解読のための総合計画への取組を開始したと言われる。

（２）「ブルラン」(Bullrun)計画[33]

ア　概要[34]

「ブルラン」は、NSA のネットワーク通信で使用される暗号攻略の取組全体を総称する計画名である。その担当部署は、CES (Cryptanalysis and Exploitation Services: 暗号解読・資料源開拓サービス)であるが、その 2013 会計年度予算は、10 億 318 万ドル（１千億円以上）と巨額である。予算にはスーパーコンピュータなどの機器やシステム費用が含まれていると考えられるので、必ずしもこの金額が全て直接的に暗号攻略に向けられている訳ではないと考えられるが、それにしても巨費である。

暗号攻略は、また各種資源を活用した多様な取組であるとされている。即ち、高等数学やスーパーコンピュータを使用した（狭義の）暗号解読努力は当然含まれるが、その他にも、CNE(TAO によるコンピュータ・ネットワーク資源開拓)、物理的侵入による情報機器への工作、企業との関係の利用、諜報コミュニティ諸機関の協力等の取組が上げられている。

○　TAO～～TAO の CNE（コンピュータ・ネットワーク資源開拓）能力を利用して、

---

[33]　全体像は次の資料が詳しい。
--James Ball, Julian Borger and Glenn Greenwald, “Revealed: how US and UK spy agencies defeat internet privacy and security,” *The Guardian,* 6 September 2013, accessed 11 September 2013,
http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
--Nicole Perlroth, Jeff Larson and Scott Shane, “N.S.A. to Foil Basic Safeguards of Privacy on Web,” *The New York Times,* 5 September 2013, accessed 22 October 2013,
http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0

[34]　ス資料 NSA, Cryptanalysis and Exploitation Services,　*Classification Guide :PROJECT BULLRUN/2-16,* 16　June 2010, accessed 11 September 2013,
http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide

暗号解読に役立てている。即ち、ネットワーク・システムから所謂ハッキングをするなどして暗号解読資料を入手しているということである。

- 諜報コミュニティの協力～～NSA は暗号解読にもヒューミント資源を活用している[35]。即ち、必要とあれば、暗号資料の協力者からの入手、或は窃取なども行っているということである。
- セカンド・パーティ諸国との協力～～特に英 GCHQ との協力関係は緊密である。
- 民間への働き掛け、民間企業の協力

NSA には民間ソルーション・センター(Commercial Solutions Center: NCSC)があるが、ここを通じて、特定企業との機微且つ協力的関係を利用している。

即ち、NCSC は、民間企業と NSA の窓口であり、公式の任務としては、「国家安全保障システム」（インテリジェンス、軍事或は秘匿情報など国家安全保障に係わる情報システム）に採用可能な民間製品の審査窓口であることや、民間での新しい暗号技術（「二重楕円曲線暗号」計画）の推進を掲げている[36]が、更に民間企業との非公然の協力関係の窓口ともなっているとされる。実際、NSA の暗号攻略では、民間商用暗号のソフトウェアと機器に関して（解読し易いように）働き掛ける、或は、民間商用暗号の詳細を入手するなどを行う窓口になっているという。

これに関連して、2013 会計年度予算案には、上記 CES 予算項目とは別に「シギント可能化」項目に 2 億 5494 万ドル（250 億円以上）という少なくない金額が計上されている。そして、その説明書[37]には、主たる事業内容として次の二つが記載されている。即ち、①米国内外のＩＴ企業に働き掛けて、シギント収集を可能とするように製品デザインに影響を及ぼすこと、②民間企業との協力関係を強化し、新しい資料源を開拓し、現資料源の運営費用を削減し、ネットワーク作戦を拡大することにより、ネットワーク防衛とサイバー状況把握を進めて「包括的国家サイバーセキュリティ・イニシアチブ」を支援することである[38]。更に、具体的な実施事項の中には次の諸点が記載されている。

- 民間商用の暗号システム、ＩＴシステム、ネットワーク及び端末に（NSA が利用できる）弱点を挿入する。
- 民間商用の暗号技術についての政策、標準、規格に影響を与える。

---

35 ス資料　NSA, *Classification Guide for ECI PAWLEYS(PAW) 02-19,* 14 November 2005, accessed 11 October 2014, https://firstlook.org/theintercept/document/2014/10/10/nsa-classification-guide-eci-pawleys/

36 NSA の Commercial Solutions Center のウェブサイトを参照。https://www.nsa.gov/business/programs/ncsc.shtml

37 "Secret Documents Reveal N.S.A Campaign Against Encryption," *The New York Times*, 5 September 2013, accessed 22 October 2013, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0

38 この②の記載は、広汎すぎて具体的には何を指しているのか、現時点では良く分からない。更なる資料の報道が待たれるところである。

・　NSA により開発中の高度暗号解読能力にとってより扱い易くなるように、世界の商用暗号市場を形作る。

実際、民間企業に対する働き掛けにおいても、民間企業による任意の協力から、対外諜報監視裁判所による協力強制命令、或はヒューミントによる暗号取得、或は製品のソフトウェアやハードウェアの修正など多様な取組がなされているとされる。

このような総合的な取組の結果、ネットワーク通信に関しては、TLS／SSL、HTTPS、SSH、VPNs、暗号化 VoIP、暗号化 Chat 他の暗号に対して、一定の解読能力を保持しているとしている。

そして、NSA は、各種民間暗号鍵の内部データベース（「暗号鍵提供サービス」(Key Provisioning Service)）を構築しており、これにより自動的にメッセージを復号できるようにしているという。また、必要な暗号鍵がデータベースにない場合には、要求が「暗号鍵入手サービス」(Key Recovery Service)に送付され、暗号鍵入手の努力がなされるという[39]。

イ　具体的取組の例

このような暗号対策の具体例は、情報保全が厳しいためか現在までのところ余り判明していないが、顕在化している幾つか記載する。

① NSA 作成の（弱点を持つ）公開鍵暗号の標準化と普及

○ 暗号の国際基準への働き掛け[40]

2006 年に米国立標準・技術研究所は、４つの暗号を十分な秘匿強度があるとして認証し、これが更に国際標準化機構により認証されて、世界標準となった。これに関して、2007 年、マイクロソフトの技術者が、その４つの暗号の内の一つ、公開鍵暗号「二重楕円曲線暗号」には弱点があることを指摘したが、当時は関心を引かなかった。

ところが、2013 年に至り NSA 内部資料によって、その弱点を持つ「二重楕円曲線暗号」の開発には、NSA が関与していたことが、明らかになった。

○ 暗号企業 RSA の協力

暗号で有名な企業 RSA は、2004 年上記「二重楕円曲線暗号」を採用して、且つその販売する公開鍵暗号ソフト BSafe の基本(default)アルゴリズムとしており、これが同暗号の米国立標準・技術研究所による認証でも有利に働いたとされる。ところが、今回 NSA 内部資料により、RSA はこれにより NSA から１千万ドルを得

---

[39] Perlroth, Larson and Shane, "N.S.A. to Foil Basic Safeguards of Privacy on Web," *The New York Times*。

[40] Kim Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA," *WIRED,* 24 September 2013, accessed 17 December 2014, http://www.wired.com/2013/09/nsa-backdoor/all/

ていたことが、判明した[41]。但し、RSA は同暗号鍵を採用した時点において弱点があることは知らなかったと主張している[42]。

○ 普及

米連邦政府は、政府調達において、製品への同暗号の搭載を条件としたため、同暗号が政府調達以外でも普及したと言われる。なお、マイクロソフトは自社の技術者が欠陥を指摘していたにも拘わらず、2008 年 Vista 更新（アップデート）では同暗号を標準暗号の一つに搭載している（但し、基本(default)とはしなかった)。一旦標準暗号の一つとして搭載されれば、システムに侵入した際に同暗号を基本的に使用するように（即ち default に）設定し直してしまえば、その後の解読は怪しまれずに容易に可能となる。これこそが NSA の動機ではないかと指摘されている[43]。

なお、暗号研究者にしてコンピュータ・セキュリティ専門家のブルース・シュナイアー氏は、「米国の大企業の販売する暗号ソフトの多くは、NSA のためのバックドアが仕込まれている、と私は推定する。また、外国製品は当該国のためのバックドアが仕込まれていると考えるのが賢明である。」と述べている[44]。

② マイクロソフトの協力

マイクロソフトは、その提供する人気のあるサービスである、アウトルックのＥメール、スカイプによる通話やチャット、（クラウドデータ保管サービスの）スカイドライブに関して、NSA に暗号化以前のデータにアクセスを認めている。2012 年、アウトルックのウェブチャットに SSL 暗号を導入したが、NSA に対してわざわざ暗号を回避してデータにアクセスできるように便宜を図っているという。（第２部第２章２「プリズム」計画で既述。）

③ 2010 年のブレイクスルー

英 GCHQ に対する NSA の説明資料（2010 年のもの）によれば、NSA の暗号解読の総合的な取組に於いて突破口が開かれて、インターネット基幹回線から取得している

---

41 Reuter, "$10m NSA contract with security firm RSA led to encryption 'back door'," *The Guardian,* 20 December 2013, accessed 25 December 2013, http://www.theguardian.com/world/2013/dec/20/nsa-internet-security-rsa-10mi...

42 Charles Arthur, "Security Company RSA denies knowingly installing NSA 'back door'," *The Guardian,* 23 December 2013, accessed 17 December 2014, http://www.theguardian.com/technology/2013/dec/23/security-company-rsa-denies-installing-nsa-back-door.

43 Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA," *WIRED.*

44 Bruce Schneier, "NSA surveillance: A guide to staying secure," *The Guardian*, 5 September 2013, accessed 18 September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

膨大なデータが利用可能となるような（インターネット通信に使用する）暗号解読に大きな進展があったとされる。詳細は不明であるが、2010 年 6 月付内部資料[45]に記載されている「ネットワーク通信に関しては、TLS／SSL、HTTPS、SSH、VPNs、暗号化 VoIP、暗号化 Chat 他の暗号に対して、一定の解読能力を保持している」という表現から判断して、これら分野の暗号解読に於いて大きな進展があったと推定できる。

なお、2014 年 12 月に独シュピーゲル誌は、暗号対策関係の漏洩機密資料を大量にそのウェブサイトに掲載したが、これを見る限り、TLS／SSL、HTTPS、SSH、VPNs、暗号化 VoIP、暗号化 Chat に関しては、 NSA は（完全ではないものの）相当の解読能力を有していると見られる[46]。

ウ　英国の取組[47]

GCHQ も暗号解読には力を入れており、英国の取組について紹介しておく。

英国の暗号攻略の取組は「エッジヒル」(Edgehill)計画とされている。

- 2012 年現在、GCHQ は、ホットメール、グーグル、ヤフー、フェイスブック４社の暗号通信対策に取り組んできたが、2012 年現在は、グーグルへの新たなアクセスの機会が開発されているので、グーグルに力を入れているとされる。
- 2010 年の内部資料によれば、暗号化通信については、2010 年現在は、インターネット企業３社と３０の VPNs について取り組んできるが、2015 年までには、主要インターネット企業１５社及び３００の VPNs の解読を目標としている。
- GCHQ もヒューミント部門を持っており、世界の通信企業の中に非公然のエージェントを獲得し運営する任務を持っているとされる。

（３）TOR 対策[48]

45　ス資料 NSA, *Classification Guide :PROJECT BULLRUN/2-16.*

46　参考資料は次の通り。

--Jacob Appelbaum, et. el., “Inside the NSA’s War on Internet Security,” *Spiegel Online*, 28 December 2014, accessed 5 January 2015, http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

--Matthew Green, “On the new Snowden documents,” *A Few Thoughts on Cryptographic Engineering,* 29 December 2014, accessed 5 January 2015, http://blog.cryptographyengineering.com/2014/12/on-new-snowden-documents.html

47 Ball, Borger and Greenwald, “Revealed: how US and UK spy agencies defeat internet privacy and security,” *The Guardian.*

48　次の資料が不十分ながら、全体像を提供している。

--James Ball, Bruce Schneier and Glenn Greenwald, “NSA and GCHQ target Tor network that protects anonymity of web users,” *The Guardian,* 4 October 2013, accessed 7 October 2013, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

ア　TOR とは何か

TOR は暗号通信そのものではないが、インターネット通信の接続経路を匿名化することにより、発信者のＩＰアドレスを秘匿して匿名化する技術であり、NSA 内部資料でも、現時点では秘匿通信の王様であるとされる[49]。

具体的には、発信者と受信者の通信の接続経路に、幾つかの中継サーバーを経由することにより両端末の（間接的な）接続を秘匿するものであるが、中継サーバーは、世界中で登録されている何千もの中継サーバー（多くはボランティアの由）の中から通信毎にランダムに選択される。そして、接続経路内の中継サーバーと受信者端末には直接の中継サーバー以外の情報（ＩＰアドレス）は残らず、且つ芋蔓式に接続経路を究明できないようにプログラムされている（これが TOR の語源となった The Onion Router である）ので、接続経路の匿名化が可能となる。そして、この中継サーバーに関する最新情報を提供するため、世界中には中継サーバーのリスト提供サーバーが９台（米、独、オランダ、オーストリア、スウェーデン等）運用されており、１時間毎に中継サーバーリストが更新される。また、TOR についての使い方等を紹介した TOR のウェブサイトも運営されている。

TOR による匿名性は高く、現在、秘密の通信をしようとする者にとっては極めて重要な通信方法であり、中国やイランなどインターネット通信を監視する抑圧的な政権から通信の秘密を守るため、民主活動家、ジャーナリストなどにより広く使用されている。そもそも TOR は、米政府職員に秘匿の通信手段を提供するために、1990 年代に米海軍の研究所が開発を開始し資金援助をしたものである。その後一般公開され独自の進化を遂げてきたが、現在でもその費用の６０％は米国務省や国防総省が提供している（目的は、民主主義の推進や政府職員への秘匿通信方法の提供）。しかし他方、その匿名性がテロリストや犯罪者によって悪用されており、それが問題となっている。NSA にとって、テロリスト、犯罪者や対外諜報関心のある者による使用が問題となる。

イ　TOR 対策の現状

2012 年 6 月付の NSA 内部資料[50]によれば、TOR の匿名性と対策の現状について、次の２点を指摘している。

--Bruce Schneier, “Attacking Tor: how the NSA targets users’ online anonymity,” *The Guardian,* 4 October 2013, accessed 7 October 2013, http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

[49] ス資料抜粋、”Tor: ‘The king of high-secure, low-latency anonymity’,” *The Guardian,* 4 October 2013, accessed 7 October 2014, http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity

[50] ス資料、*Tor Stinks*, June 2012, accessed 7 October 2013, http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

- 常時全ての TOR 利用者を非匿名化（特定）するのは、現在も将来も不可能である。
- （自動分析ではなく）個別分析により、TOR 利用者の極く一部について非匿名化（特定）することは出来るが、特定の情報要求に応じて非匿名化すること（註：対象者を指定して同人の TOR 接続経路を把握して TOR 通信を捕捉すること）は出来ない。

即ち、TOR の秘匿性は高く、TOR 自体の攻略は、NSA にとっても困難である。しかし、だからと言って NSA は TOR 利用者の攻略を諦めた訳ではなく、そのため、総合的な取組をしている。その取組の全貌までは分からないが、一部がその内部資料から伺えるところであり、正にその取組に投入される努力、膨大なエネルギーに、NSA のインターネット支配に向けた意思を見ることが出来る。次に、判明している努力の一端について述べる。

ウ　TOR 利用者に対する総合的取組

既述の NSA 内部資料によれば、2012 年春には、NSA と GCHQ によって２週間に及ぶ TOR 対策共同ワークシップが行われ、ここでは、TOR 対策について総合的な検討がなされたようである。即ち、TOR 構造の分析把握、各種の攻撃手法の活用など、総合的に取り組んでいるが、主要な攻略方法は TOR 利用者を割り出して当該者の端末を直接攻撃する手法の様である。これらの資料によれば、他の手法を含め、TOR 対策の努力の一旦は次の通り。

①　基礎データ収集[51]

NSA は、TOR 利用者を把握するための基礎情報として、TOR のソフトウェアを探している者や TOR の中継サーバーにアクセスする者などのデータ（IP アドレス）を収集している。そのため、世界中の通信基幹回線など NSA が収集可能な膨大な（インターネット通信の）データの中から、次のような TOR 関連データを収集している。（この収集には、既述した XKeyscore という分析ツールを利用している。）

- TOR のウェブサイトにアクセスする者（のＩＰアドレス。以下同じ。）（現在、Tor Project はマサチューセッツ工科大学内にある）
- TOR の（中継サーバーの）リスト提供サーバー９台にアクセスする者（TOR 通信の前に必ずアクセスする）
- 世界に何千とある TOR 中継サーバーにアクセスする者（TOR 通信の際は必ずアクセスする）
- TOR の非公表中継サーバー（一般中継サーバーは公表されているため、中国な

[51] Kim Zetter, “The NSA Is Targeting Users of Privacy Services, Leaked Code Shows,” *WIRED*, 3 July 2014, accessed 19 December 2014, http://www.wired.com/2014/07/nsa-targets-users-of-privacy-services/

ど抑圧的政権はこれらのサーバーへの接続を出来なくしている。そこで非公表中継サーバーもあるが、これらの非公表サーバーを把握しようとしている。）

なお、NSA がこのような基礎データを収集しているのは、TOR だけではなく、その他の秘匿通信関連の各種サービス、Tails、HotSpotShield、FreeNet、Centurian、FreeProxies.org、MegaProxy 等にも及んでいるという。

② TOR 全体構造を分析把握して、TOR 利用者を特定する努力

- GCHQ は自ら TOR 中継サーバーを提供して運用しているが、現状では数が少なく、接続経路全体の割出には極めて不十分。（GCHQ は中継サーバーを運用している。）
- TOR 通信の入口、出口で捕捉する努力。
- TOR 通信をしていない時の通信（クッキー資料）から、TOR 通信利用を割り出す努力。

③ TOR 利用端末に対する攻撃

各種の攻撃方法があるようであるが、成功している一例に次のものが上げられている[52]。

- 「EgotisticalGiraffe」～詳細は不明であるが、特定のウェブサイト（TOR 利用者が良くアクセスする）に接続しようとする通信の中から、TOR 通信に特有なデータ状況から TOR 通信を探知すると、「クオンタム・インサート」など「クオンタム」攻撃を使って、これを偽装サイトに導き、マルウェアを注入する。この成功のためには、TOR 利用者が利用する FIREFOX ソフトウェアの脆弱性が利用されるという。

エ 余談～～TOR 対策への対策

現在の NSA の TOR 攻略方法の中心は、TOR 利用者を割り出して当該者の端末を直接攻撃する手法の様である。そうすると、TOR を使用する者からすれば、仮に端末を割り出されても、端末を守る手法が必要となる。そこで、Tails というシステムが良く使われているようである。Tails は、そのソフトウェアを DVD や USB にダウンロードしてこれをパソコン端末に接続して使用することによって、パソコン端末のハードドライブ等を使用しないで通信が可能である。その結果、端末にその使用の痕跡を一切残さないのである（唯一 RAM ランダムアクセスメモリーは使用するが、電源を切れば記憶

---

52 ス資料抜粋 *Peeling Back the Layers of TOR with EGOTISTIC GIRAFFE,* undated, accessed 7 October 2013, http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document

は消去される)。更に、現在 Tails は、通信では接続経路は TOR で匿名化し、メールや文書は PGP（Pretty Good Privacy)、チャットは OTR（Off-the-Record）で暗号化するなどにより、高度の秘匿通信が可能とされる[53]。

スノーデンが告発のためにローラ・ポイトラスらと連絡を取ったが、その際に使用したのも Tails であった。

秘密の通信を攻撃する側も、守る側も、厳しい闘いを続けているのが、世界の現状である。

---

[53] 現時点で NSA が解読できていないとみられる民間暗号としては、本文にも記載した PGP、OTR の他、Truecrypt、CSpace、ZRTP が挙げられている。これらの暗号の特徴は、①オープンソースの暗号で、研究者に相対的に良く研究されていること、②SSL や VPN と異なり、幅広く使われていないこと、③エンドツーエンド（端末から端末まで）の暗号であり、インターネット・サービス事業者やソフトウェア会社等が関与していないことである。即ち、①は暗号の秘匿強度が高く、（暗号解読の）裏口が設けられていないことを示し、②は NSA の解読努力がまだそれ程集中されていないことを示し、③はインターネット・サービス事業者やソフトウェア会社自体が NSA と裏取引をしたり、会社自体から暗号鍵が盗まれていたりする可能性がないことを示している。
--Green, “On the new Snowden documents,” *A Few Thoughts on Cryptographic Engineering,*

４　特定の対象・情報に対する収集事例

NSA の活動の内、特定の対象（標的）や事象に対するデータ収集事例の中で興味深いものを幾つか紹介して、NSA の活動実態の理解の資としたい。

（１）政府首脳(Chief-of-State)の情報収集[54]

ア　標的データベース TKB(Target Knowledge Base)

一国の政治の最高責任者は、当然に諸外国の政治の最高責任者について関心を持つものであり、米国は強力なシギント諜報能力を持っている以上、これら諸外国の首脳は NSA の諜報対象（標的）になっている。そこで、どのような国の首脳が標的になっているかについて知ろうとすると、標的データベース TKB(Target Knowledge Base)が参考になる。

これは、NSA が諜報対象としている人物について、分析官が分析したり報告書を作成するに当たり基礎資料となるデータベースである。標的データベースは従来、分析官が個別に作業をして作成していたが、余りにも煩雑であるため作成更新が進まず、そこで、NSA の各種データベースから関連データを自動で検索するシステムが構築されたようである。この対象となっている諸国首脳(Chief-of-State) の 2009 年時点でのリストが報道されており、そこには世界中の政府首脳１２２人がリストアップされている。政府首脳とは、大統領或は（大統領に政治の最高権限がない場合には）首相である。

１２２人中、報道された内部資料自体から読み取れるのは１１人だけであるが、他に８６人がリスト中のものであるとして報道されており、併せて９７人が判明している[55]。これらに９７人の属する諸国９６箇国は後述する。また、残り２５名は不明である。

これら判明している９７人の特徴として挙げられるのは、第１に、ロシアだけは当時のメドヴェージェフ大統領とプーチン首相の二人が掲載されていることである。ロシア

---

[54] 主な出典資料は次の通り。
--Laura Poitras, Marcel Rosenbach and Holger Stark, “GCHQ and NSA Targeted Private German Companies and Merkel,” *Spiegel Online,* 29 March 2014, accessed 14 January 2015, http://www.spiegel.de/international/germany/gchq-and-NSA-targeted-private-german-companies-a-961444.html
--Ryan Gallagher, “Der Spiegel: NSA Put Merkel on List of 122 Targeted Leaders,” *The Intercept*, 29 March 2014, accessed 14 January 2015, https://firstlook.org/theintercept/2014/03/29/der-spiegel-NSA-ghcq-hacked-german-companies-put-merkel-list-122-targeted-leaders/
--“New Ed Snowden NSA Leaks Target Knowledge Database(TDK) Marina, Nymrod, & List of SIGAD Designations Surveillance 3/29/2014,” *USNEWSGHOST,* 2 April 2014, accessed 19 August 2014, https://usnewsghost.wordpress.com/2014/04/02/NSA-new-ed-snowden-leaks-target-knowledge-database-tkb-marina-nymrod-list-of-sigad-designations-surveillance-3292014/

[55] “New Ed Snowden NSA Leaks Target Knowledge Database(TDK)…,” *USNEWSGHOST.*

の政治体制からすれば、大統領が政治の最高責任者であるが、当時の実際の最高権力者はプーチン首相と目されていたためであろう。第２に、日本では当時の麻生首相が掲載されている。インテリジェンスの論理を理解しない一部の者は、米国の同盟国日本の首相が諜報対象とされていることに違和感を持つかも知れないが、同盟国であろうと他国である限り（即ち、相互の利害が１００％一致することはあり得ないので）諜報対象にするのは当然である。寧ろ、仮に麻生首相が対象とされていなかったとすれば、日本はその首相を諜報対象とする程の価値も重要性もない国と評価されていることを示すものであり、その方が極めて問題である。

なお、不明の２５人について、推定する手掛かりとしては、第２部第２章６で述べた「特別収集サービス（SCS）」の収集拠点がある。NSA と CIA の共同事業として諸国の米国在外公館からシギント活動を行っているが、この SCS の主要情報関心が当該国の政治情報であるのは自明であり、当該国の首都に SCS 収集拠点がある国約６０数箇国の政府首脳が収集対象になっていないことは先ず考えられない。そこで、首都に SCS 収集拠点がありながら、９６箇国に含まれていない国を見ると、１４箇国がある。これら諸国は後述するが、中東諸国と中東欧諸国が多い。

なお、標的データベース TKB に登録されている標的者総数は、２０万人以下とされる。それは、従前分析官による個別作業で作成していたので、作成できる件数が限定されていたためという。限定されていたと言いながらも、少なくとも１０万人以上が登録されているという事実は、NSA の諜報活動が如何に広汎に及んでいるか示すものである。

イ　収集対象の諸国　８６箇国

- 欧州（２１箇国）
  ～独、仏、伊、西、ベルギー、アイスランド、
  ～露、ウクライナ、白ロシア、アゼルバイジャン、ジョージア、トルクメニスタン、ウズベキスタン、キルギスタン、カザフスタン
  ～セルビア、クロアチア、ボスニア・ヘルツェゴビナ、コソボ、ギリシャ、アルバニア
- 中東（７箇国）
  ～イスラエル、パレスチナ、トルコ、イラン、イラク、シリア、レバノン
- アフリカ（１７箇国）
  ～エジプト、リビア、スーダン、エチオピア、ソマリア、ジプチ、ケニア、ルワンダ、ウガンダ、コンゴ、ナイジェリア、象牙海岸、マリ、リベリア、ジンバブエ、マラウィ、南アフリカ
- 南アジア（６箇国）
  ～パキスタン、インド、アフガニスタン、ネパール、バングデシュ、スリランカ

- 東アジア（１５箇国）
  ～中国、香港、台湾、北朝鮮、韓国、日本、フィリピン、インドネシア、マレーシア、ブルネイ、ラオス、ベトナム、カンボジア、ミャンマー、東チモール
- 中南米（２０箇国）
  ～メキシコ、グアテマラ、ホンジュラス、エルサルバドル、ニカラグア、コスタリカ、パナマ、キューバ、ハイチ
  ～ベネズエラ、ガイアナ、コロンビア、エクアドル、ブラジル、ペルー、ボリビア、パラグアイ、ウルグアイ、チリ、アルゼンチン

ウ　収集対象と推定できる諸国　１４箇国

特別収集サービス（SCS）の収集拠点が当該国の首都にありながら、上記イに含まれていない国。

- 欧州～オーストリア、チェコ、ハンガリー、ブルガリア
- 中東～ヨルダン、サウジアラビア、クウェート、UAE、バハレーン、イエメン
- アフリカ～アルジェリア、ザンビア、アンゴラ
- 東アジア～タイ

エ　同盟国首脳に対する諜報は中断されたか。

2013 年 6 月のスノーデンによる NSA 告発と内部資料の漏洩を機に、NSA による広汎な情報収集が米国内で政治問題化し、また、メルケル独首相との関係が携帯電話の盗聴などで悪化した。これらを背景に、2014 年 1 月 17 日、オバマ大統領は、シギント活動の見直しに関して演説[56]を行い、連邦議会に対してシギント活動の改革を提案すると共に、同日シギントに関する新たな大統領政策指令[57]を発しシギント活動に一定の制約を課した旨表明した。同演説によれば、今後は「説得力ある国家安全保障上の必要が無い限り、米国の親密な友人や同盟国の政府首脳の通信は傍受しない」こととされた。これに関連して、NSA 広報官は、数十人の外国首脳は対象から除外されたと述べた[58]。

さて、これによって、メルケル独首相は、諜報対象から完全に除外されたのであろう

---

[56] US President Obama, *Remarks on Review of Signals Intelligence,* 17 January 2014, accessed 16 January 2015, http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[57] US Presidential Policy Directive/PPD-28(Signal Intelligence Activities), 17 January 2014, accessed 16 January 2015, http://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

[58] Ellen Nakashima and Barton Gellman, "Court gave NSA broad leeway in surveillance, documents show," *The Washington Post,* 30 June 2014, accessed 3 July 2014, http://www.washingtonpost.com/world/national-security/court-gave-NSA-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html

か。先ず、同演説で「説得力ある国家安全保障上の必要が無い限り」と述べているように、必要時には何時でもその諜報能力を運用することを表明していることから判断して、（携帯電話の傍受能力を含めて）収集能力自体は保持し続けることは明白である。また、オバマ大統領は同演説で、「米国の諜報諸機関は、世界中の諸政府の意図に関する情報は収集し続ける」と表明していること、及び常識から考えて、外国の政府首脳に関する情報収集を全く停止すると考えるのも非現実的であろう。外国政府の意図を知ろうとすれば、外国政府首脳の意図を知らなければならないからである。結局、これはメルケル独首相初め関係の深い国の首脳は、直接的な電話盗聴対象から外されたということに過ぎないと考えるべきではないだろうか。従って、首脳周辺者の通話は今後とも傍受され続けるであろう。更に、演説はともかく、公表された大統領政策指令を見る限り、指令自体の中に友好国首脳の通信傍受に関する直接的記載はない。従って、親密な友好国首脳の電話傍受も、何時秘密裡に再開されないとも限らないと覚悟すべきなのである。

（２）金融取引データの収集計画「Follow the Money」[59]

諜報機関が対象とする様々な活動には、金の動きが伴うものである。諜報機関が関心を持つ違法武器取引にしろ、抑圧的政権への支援、経済制裁破り、テロリスト支援、薬物密輸など、殆どの活動には金の動きが付随する。そこで、国際的な金の動き自体に着目して関連データを収集分析することによって、有効な諜報活動ができることとなる。

そのため、NSA には「Follow the Money」と呼ばれる金の流れに関するデータを収集分析する部門が存在するという。ここでは、金融機関間の送金やクレジット・カード取引情報など、世界中の金融取引データを大量に収集して、「トラックフィン（Tracfin）」というデータベースを構築して分析に活用している。このトラックフィンの保管データ量は、2008 年時点では約２千万件（データセット）であったが、2011 年では約１億８千万件の記録（データセット）と急増しており、その内８４％はクレジット・カード取引データである。

クレジット・カード取引データの取得整備は、2009 年に開始された「ディッシュ・ファイア」システム（テキストメッセージからのデータ抽出システム）を使用して、世界の銀行約７０行からテキストメッセージ形式で送信される取引データを取得し保管

59　資料は次の通り。但し、これらの報道は NSA 内部資料自体は掲載していない。
--Laura Poitras, Marcel Rosenbach and Holger Stark, “Follow the Money: NSA Monitors Financial World,” Spiegel Online, 16 September 2013, accessed 22 October 2013, http://www.spiegel.de/international/world/how-the-NSA-spies-on-international-bank-traNSActioNSA-922430.html
--“Follow the Money: NSA spies on International Payments,” *Spiegel Online,* 15 September 2013, accessed 22 October 2013, http://www.spiegel.de/international/world/spiegel-exclusive-NSA-spies-on-international-bank-traNSActioNSA-922276.html

している。更に、VISA やマスターカードなど特定のカード会社を対象にした収集も行っており、2010 年の内部資料では、VISA について欧州、中東、アフリカの利用者を主対象にして個別商店とカード会社間の支払承認の通信経路でのデータ収集を成功させているという。

また、銀行間送金決済情報も取得しており、国際銀行間通信協会（SWIFT）[60] の通信システムに侵入してデータを取得しているという。そもそも SWIFT 情報については、米国政府がテロ対策のために EU に対してその提供を要請してきたが、顧客の秘密保護の観点から交渉は難航し、漸く 2010 年に一定範囲のデータ提供で米国と EU が合意した経緯がある。米国は、一方で表口からデータ提供の交渉すると共に、裏口から NSA によって秘密裡にデータを取得してきたのである。NSA によるデータ取得は、既に 2006 年に銀行からのデータ通信の傍受で一部の収集が開始されており、2010 年の合意にも拘わらず 2011 年現在も継続しているという。2011 年現在の収集は TAO グループが関与しているということであるので、SWIFT の内部情報システムに侵入している可能性が大きいと考える。

但し、金融取引情報の収集には成功物語だけではなく、データ源を失う失敗談もある。国際送金の世界的企業であるウエスタン・ユニオンの送金データは、長らく取得できていたが、2008 年に同社が秘匿強度の高い暗号通信を導入したため、データ取得が出来なくなってしまったという。NSA も世界の通信方法の変化に常に対応していく必要があるということである。

なお、金融取引情報の分析については一定の専門知識を必要とするため、NSA は米財務省の協力を得て、NSA 分析官（複数）を財務省の関連部局に数ヶ月間研修に出しているという。（ここにも、シギント実施に於ける関係諸機関の協力態勢が見られる。）

（３）産業経済情報・科学技術情報の収集

ア　産業経済情報の収集

産業関連の情報収集に対する米国の公式の立場は、産業経済情報は収集しているが、それは対外諜報のためであり、産業スパイ行為はしていない、即ち、「米国企業の国際競争力を強化する為に、外国企業の秘密を収集したり、米国企業に提供したりはしていない」（クラッパー国家諜報長官）というものである[61]。一方、中国等に対しては正に産業スパイをしていると批判している。

ところで、米国が実際にどのような産業経済情報を収集しているかであるが、これに

60　正式名称は the Society for Worldwide Interbank Financial Communication。本部をベルギーに置く民間協会で、世界中の銀行 8000 行以上が利用している。

61　例えば、David E. Sanger, “Fine Line Seen in U.S. Spying on Companies,” *The New York Times,* 20 May 2014, accessed 12 September 2014, http://www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html?_r=0

ついては、2015 年 6 月に「ウィキリークス」に NSA 内部資料の一例が掲載されており、参考になる。（なお、本資料[62]はその内容から判断して、スノーデン資料ではなく、他の諜報関係者からの漏洩であると見られている[63]。）

本資料は 2012 年時点での「フランスの経済発展」[64]に関する「情報需要」（Information Needs）の詳細である。本資料は 2002 年に作成されその後更新されてきたものであるが、その中には更に収集すべき「主要情報要素」（Essential Elements of Information）11 項目が列挙されており、更に 11 項目中の 1 項目「外国契約、実現可能性調査、交渉」は次のように記載されている。即ち、

「フランスの国際貿易・国際投資についての差し迫った契約提案、実現可能性調査や交渉に関するものであって、ホスト国にとって重要な利益に係わる主要プロジェクトやシステム、又は契約額が 2 億ドル以上のものは報告する。」そして、「重要な利益に係わる」ものとして次の諸項目が列挙されている。

- 情報通信に関する施設、ネットワーク、技術
- 原子力や再生エネルギーを含む電力、天然ガス、石油に関する施設とインフラ
- 港湾、空港、高速鉄道、地下鉄を含む輸送に関するインフラと技術
- 環境技術
- バイオテクノロジーを含む健康ケアに関するインフラ、サービスと技術

ここで注目されるのは、その情報収集の対象とする貿易や投資の広汎さであり、契約額２億ドル以上の貿易、投資案件は全て収集しようとしているのである[65]。これはフランスに対する情報需要であるが、他の諸国に対しても同様な情報需要を設定しているものと推測でき、NSA の収集する産業経済情報は極めて広範囲に及んでいることが分かる。

イ　科学技術情報の収集

産業経済情報と類似の情報分野に、科学技術情報がある。これについては、既述（第２部第１章２戦略的任務リスト）したように、2007 年 1 月現在の NSA の「戦略的任務リスト」には、収集任務対象に次の項目がある。

「戦略的科学技術（軍事、経済、政治面で戦略的優位となりうる重要科学技術～～高

---

62 NSA 内部資料、”Information Need(IN) – France: Economic Developments(2012),” *Wikileaks,* 29 June 2015, accessed 30 June 2015, https://wikileaks.org/NSA-france/spyorder/

63 “Wikileaks published some of the most secret NSA reports so far,” *Top Level Telecommunications,* 26 June 2015, accessed 29 June 2015, http://electrospaces.blogspot.jp/2015/06/wikileaks-publishes-some-of-most-secret.html

64 2007 年 1 月現在の NSA の「戦略的任務リスト」の収集対象任務分野には、「経済発展」はないが、「経済的安定と影響力」の項目が見られる。第 2 部第 1 章 2 を参照。

65 Fabrice Arfi, et. al., “Revealed: the massive US industrial espionage against France,” *Mediapart,* 29 June 2015, accessed 30 June 2015, http://www.mediapart.fr/en/journal/france/290615/revealed-massive-us-industrial-espionage-against-france.

低エネルギー・レーザー、コンピュータ・情報技術の進展、指向性エネルギー兵器、ステルス・反ステルス技術、電子戦技術、宇宙観測・遠隔観測技術、電子光学、ナノテクノロジー、エネルギー物質）」

勿論、これ自体は、NSA が科学技術情報を収集している事実を示すものではあっても、必ずしも、それを米国企業の競争力強化の為に利用していることを示すものではない。

他方、「四年毎の諜報コミュニティ・レビュー」（2009 年 4 月）という内部文書が漏洩されている[66]。この文書は、米国諜報コミュニティが将来直面するであろう最重要な課題について 4 年毎にレビューをするものである。同文書は 2025 年という将来における状況を想定した上で、最重要課題を６つ提示している。その課題の一つが「あらゆる手段による科学技術情報の入手」である。

即ち、2025 年には、外国多国籍企業の技術的能力が米国企業を上回るなどして、米国の科学技術や革新性に於ける優位が減少し、エネルギー、ナノテクノロジー、医療、情報技術等の死活的な分野で劣勢に立たされる可能性がある。そこで、科学技術に於ける優位を喪失しないため、公開情報と非公開情報の総合的な収集努力と防諜に取り組むべきであるとしている。その上で、具体的な活動手法４つを提示しているが、その一つがサイバー作戦である。具体的には、外国の非公開・非公然の研究センターの情報を取得するため、外国研究者や外国企業が使用するソフトウェアやハードウェアにマルウェアやセンサーを仕込んだり、或は、外国の研究開発イントラネットに対してコンピュータ・ネットワーク資源開拓（CNE）を実施したりすることを挙げている。そして、外国の研究センターから入手した「調査結果」について米国産業界にとって有益か否か、どのような意味で有益かを判定すると記載している[67]。

この文書は、米国政府による（現在は兎も角として少なくとも将来の）産業スパイ実施の意図を示したものと解釈されても仕方がないのではなかろうか[68]。

66　ス資料、ODNI, *Quadrennial Intelligence Community Review Final Report, April 2009,* accessed 12 September 2014, https://firstlook.org/theintercept/document/2014/09/05/quadrennial-intelligence-review-final-report-2009/

67　*Quadrennial Intelligence Community Review Final Report,* 12-13.

68　2012 年の NSA 内部資料”Private Networks: Analysis, Contextualization and Setting the Vison,”では、潜在的な収集対象ネットワーク（仮想専用ネットワーク VPN を含む専用ネットワーク Private Network）の発見方法を議論しているが、その中で、既知の専用ネットワーク一覧表の存在が示されているという。その中には、通信、金融、石油や製造関連の世界主要企業が列挙されており、Rolls Royce Marine（英）、 Rio Tinto（英）、 RigNet（米）、 Royal Bank of Canada（加）、 Rogers Wireless（加）を含む１５企業の名前が読み取れるという。
--Colin Freeze and Christine Dobby, “NSA trying to map Rogers, RBC communications traffic, leak shows,” *The Globe and Mail,* 17 March 2015, accessed 19 March 2015, http://www.theglobeandmail.com/news/national/NSA-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/

（４）メキシコ、ブラジル、国連気候サミット他の収集

NSA が標的として取り組んでいる個別の国、組織、或は行事に関して大きく報道されたものの中から、参考事例として幾つか紹介する。米国は、隣国メキシコや南米の大国ブラジルに対しては、大きな情報関心を持っている。そこで、これらの国を含む幾つかについて記載することとする。

ア　メキシコ[69]

2013 年 4 月現在の NSA の収集優先度リストでは、メキシコは、薬物取引で（５段階中の最高）レベル１、国家指導部の意図、経済的安定、軍事能力、人権状態、国際貿易関係でそれぞれレベル３、防諜でレベル４に位置付けられているという。国境を接する隣国でもあり、薬物取引に対する関心が高いのが注目される。当然、メキシコに対して各種取組を継続的に行っていると見られるが、報道された事例は次の通り。

- 2009 年公安局のメールシステムからの情報収集

  CNE 作戦（第２部第２章の７）で既述したように、2009 年 8 月に「ホワイトタマーレ作戦」をメキシコ公安局のシステムに対し実施して成功した。

  作戦対象の公安局（2013 年に国家安全保障委員会に改組）は、メキシコにおいて国内治安を総括し、警察、テロ対策、刑務所、国境警備に責任を持つ 2 万人の組織である。その情報システムに浸透することにより、米国として関心の高い薬物取引、人の密輸、国境警備等に関する情報を収集できたのみならず、「外交発言要領（トーキングポインツ）」などの政治問題や国際投資に関する情報も入手できたという。

- 2010 年 5 年大統領府ネットワークの重要メール・サーバーに侵入成功

  2010 年 11 月付の NSA 内部資料[70]によれば、同年５月、大統領府の重要メール・サーバーへの侵入に成功して、大統領に加えて閣僚のメール・アカウントにもアクセスできるようになった。その結果、外交、経済、政治指導に関する通信を入手できるようになり、メキシコの政治体制や国内的安定に関する洞察力を得た。情報成果は、NSA の本部、テキサス地方本部に加えて、メキシコ市所在の SCS（特別収集サービス）でも活かすことができたとしている。

- 2012 年初夏、次期大統領候補に対する情報収集

  2012 年 6 月付の NSA 内部資料を元にした報道によれば、次期大統領の有力候

---

[69] Jens Gluesing, et. al., “NSA Accessed Mexican President’s Email,” *Spiegel Online,* 20 October 2013, accessed 22 October 2013, http://www.spiegel.de/international/world/NSA-hacked-email-account-of-mexican-president-a-928817.html

[70] ス資料、*Computer-Network Exploitation Successes South of the Border*, 15 November 2010, accessed 3 February 2015, https://NSA.gov1.info/dni/index.html#mexico

補であったニエト氏とその側近９人の間の通信を収集分析した。その際、後述する「ディッシュ・ファイア」というシステムを使用して、彼らの間の携帯電話による膨大なテキストメッセージ(ショートメールサービス)の遣取りを分析したという。

イ　ブラジル

ブラジルに対する収集優先度リストも、メキシコと類似しているが、国家指導部の意図が中心となり、更に核開発計画も優先度が高いという。

- ルセフ大統領の主要助言者の割出

2012 年頃の NSA 内部資料[71]によれば、NSA はルセフ大統領と側近の助言者の間の通信の方法を調査し、接触連鎖分析により有力な対象を発見したという。

- ブラジル鉱山エネルギー省に対する情報収集[72]

2012 年 6 月のカナダ CSE の内部資料[73]によると、カナダ CSE はブラジル鉱山エネルギー省を標的として、情報収集に取り組んでいる。

- ブラジル石油公社ペトロブラスの VPN 侵入

ブラジル石油公社の使用する VPN（仮想専用ネットワーク）への侵入に取り組んでいる。(侵入の成否は明瞭でないが、成功している可能性が大とみられる。)[74]

ウ　フランス外務省の VPN（仮想専用ネットワーク）[75]

2012 年 6 月の内部資料によれば、フランス外務省の世界中の公館と外務本省を結ぶ

---

[71] ス資料、*Intelligently filtering your data: Brazil and Mexico case studies,* undated, accessed 18 September 2013, http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html

[72] "American and Canadian Spies target Brazilian Energy and Mining Ministry," *Globo*, 6 October 2013, accessed 21 January 2015, http://g1.globo.com/fantastico/noticia/2013/10/american-and-canadian-spies-target-brazilian-energy-and-mining-ministry.html

[73] "Olympia: How Canada's CSEC maps phone and internet connections," *Top Level Telecommunications*, 13 March 2014, accessed 3 February 2015, http://electrospaces.blogspot.jp/2014/03/olympia-how-canadas-csec-maps-phone-and.html

[74] Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014), 135.
同本に掲示されている NSA 内部資料には、VPN（仮想専用ネットワーク）への侵入取組対象としては、ペトロブラスの他に、ロシアのガスプロム、同アエロフロート、国際銀行間通信協会（SWIFT），グーグル、アブダビのワリッド通信会社、フランス外務省が挙げられている。この内、他資料から、SWIFT とフランス外務省の VPN への侵入は成功していることが分かっているので、他の VPNs への侵入にも成功している可能性が高いと考えられる。

[75] "'Success Story': NSA Targeted French Foreign Ministry," *Spiegel Online*, 1 September 2013, accessed 29 January 2015, http://www.spiegel.de/international/world/NSA-targeted-french-foreign-ministry-a-919693.html

通信網である VPN への侵入に成功しているという。フランス外務省が、VPN を介してどれだけの情報を遣取りしているかは分からないが、これではフランス外務省の手の内も相当程度米国に把握されているということになる。

エ　欧州連合（EU）本部侵入の試み[76]

2008 年頃、EU 本部ビルの電話システムを遠隔管理するための電話番号に類似した番号の電話に、外部から不審な電話が数回架かってきた。そこで、セキュリティ担当者がその発信元を調査したところ、NSA が使用する NATO 本部別館から架かってきたものであったことが判明した。NSA 職員が EU 本部内の電話システムに侵入しようとして、電話番号を間違えた可能性が高いと見られる。これは失敗事例であるが、NSA の取組の一端が分かる事例である。なお、本件はスノーデン資料とは関係なく発覚した事例である。

オ　2009 年国連気候サミットの収集[77]

2009 年 12 月 7 日からデンマークで国連気候サミットが、米大統領や我が国首相を含む世界の政府首脳１１０人を集めて開催された。このサミットは、地球温暖化防止のための温室効果ガスの削減について、（拘束力を有する）京都議定書の有効期限が 2012 年迄であったため、それに続く拘束力ある国際的合意を目指す重要なものであった。しかし、先進国特に米国と、中国やインドなど新興国との利害対立が激しく、結局合意に至らなかったものである。

国益に絡む重要な会議であったので、当然、NSA とセカンド・パーティ諸国は協力してこの会議の情報収集に当たることになる。

その結果、この会議を振り返って、デンマークの交渉担当官は、個別の裏交渉の内容について、「米国と中国、特に米国は、奇妙にも常に良く知っていた」と述べている[78]。また、多数の新興国グループを代表して交渉した某氏は、米国は開催前から新興国の主張を良く掌握していたし、会議期間中も必ず盗聴していると感じていたと述べている。

---

[76] Laura Poitras, “NSA Spied on European Union Offices,” *Spiegel Online*, 29 June 2013, accessed 15 August 2015, http://www.spiegel.de/international/europe/NSA-spied-on-european-union-offices-a-908590.html

[77] John Vidal and Suzanne Goldenberg, “Snowden revelations of NSA spying on Copenhagen climate talks spark anger,” *The Guardian,* 30 January 2014, accessed 7 February 2014, http://www.theguardian.com/environment/2014/jan/30/snowden-NSA-spying-copenhagen-climate-talks

[78] Sebastian Gjerding, et. al., “For the NSA, espionage as a means to strengthen the US position in climate negotiations,” *Information,* 30 January 2014, accessed 4 February 2015, http://www.information.dk/486360

この間の収集努力について、会議開始当日の 2009 年 12 月 7 日付 NSA 内部文書[79]によれば、政策決定者に対して、中国がインドとその主張を調整している状況の詳細について報告書を 11 月下旬に作成し、また、別の報告書で（会議が行き詰った場合のために準備された）デンマーク案の詳細を事前に入手し報告していたとして、それまでの成果を誇示している。また、今後も、会議に対する主要国の準備状況、目標、内部議論や交渉戦略について、ユニーク且つタイムリーで貴重な洞察を提供し続けると述べた上で、２週間の会議期間中、シギントは間違いなく情報提供で主要な役割を担うであろうと述べている。

このようなシギントを活用した交渉については、一人だけが相手の手札を知って行うポーカーゲームのようなもので、公平ではないという批判をする者もいるが、1923 年のワシントン海軍軍縮交渉（英米日仏伊）では、我が国の外交暗号が解読され、米国は我が国の手札を知りつつ交渉に臨んだ故事を想起すべきであろう。批判するより前に、先ずこれが世界の現実であること（そして将来も変わらない現実であろうこと）を認識することが重要である。米国に限らず、世界中の多くの国、少なくとも主要プレーヤーは皆、国益を賭けてインテリジェンスに取り組んでいるのである。

なお、中国も裏交渉状況を良く知っていたということであり、中国も各種インテリジェンス、特にシギントに注力していたことが伺われるのではなかろうか。

（５）過激派に対する人格攻撃、信頼性攻撃（積極工作）[80]

インテリジェンスについて、我が国の識者の多くは、「政策決定者に提供される情報」の側面に傾斜して考える傾向が伺われるが、当然のことながらインテリジェンスには「情報提供」を超える「積極工作」もあれば「特別工作」も含まれる。

しかしながら、今回、NSA 内部資料に関して現在まで報道されている中では、米国 NSA に関しては積極工作的なものは少ない。これは、嘗て、FBI や NSA など米国諜報機関が、キング牧師初め多くの政治活動家或は政治家の（性的嗜好や婚外関係などを含む）個人情報を違法に収集した過去を反省して、NSA が対外的にも実際にそのような積極工作には慎重なためか、或は、盛んに実施しているが単に関係内部資料が報道されていないだけなのか、或は、サイバー空間における積極工作は寧ろ CIA 主体とされているのか、不明である[81]。（註：後述するが、英国 GCHQ はサイバー空間に於ける各

---

[79] ス資料、*UN Climate Change Conference in Copenhagen—Will the Developed and Developing World Agree on Climate Change?* 7 December 2009, accessed 7 February 2014, http://www.information.dk/databloggen/486321

[80] Glenn Greenwald, Ryan Grim and Ryan Gallagher, "Top-Secret Document Reveals NSA Spied On Porn Habits As Part of Plan To Discredit 'Radicalizers'," *Huffington Post,* 26 November 2013, accessed 25 August 2014, http://www.huffingtonpost.com/2013/11/26/NSA-porn-muslims_n_4346128.html

[81] あるスノーデン資料は、「インターネットを使ったヒューミント作戦」（Human intelligence

種の積極工作に積極的である。）

但し、極めて少ないながら、積極工作のためのシギント活動が報道されているので、これについて紹介する。

即ち、これは、世界的に影響力のあるイスラムの過激思想家達の人格や信頼性に関する情報を収集して、これを一定の方法で流布させることにより、同人達の権威を失墜させ影響力の弱体化を図ろうとするものである。

内部資料によれば、NSA 長官の指示により、過激思想家６人について、2008 年 1 月から 2012 年 9 月迄の間の情報について、主としてシギントデータを基に取り纏めたようである。６人は中近東から南アジアに居住するイスラムの宗教指導者、学者・研究者、メディア出演者等（但し、内１人は米国籍又は永住権を保持）で、アルカイダを支持したり非イスラム教徒に対するジハードの正当性を主張したりする者である。これらについて、ポルノサイトなど性関連ウェブサイトの閲覧、寄付金の私的流用、法外な講演料など金銭欲や名誉欲などの情報を取り纏めたところ、ポルノサイト等の閲覧２人、基金の流用１人、法外な講演料の要求１人、極めて贅沢な生活１人が見られたという。報道された内部資料と報道自体からは、収集後の工作方針が明確ではないが、同人達は、支持者達とユーチューブやフェイスブックを利用して通信をしているため、これらの通信への介入や、これを利用したスキャンダル情報の流布を検討している様にも見える。

なお、本件は対象となった６人中１人が米国人であったためメディアの関心を引いたのであるが、対象が全て外国人であれば、それ程の関心を引かなかった（即ち、そのような工作は当然に許される）という論理なのであろう。

---

operations undertaken via the Internet）の存在に言及しており、米国がサイバー空間における積極工作自体に取り組んでいないと考えることは合理的でないと考える。
--ス資料、US Presidential Policy Directive/PPD-20, undated(October 2012), accessed 4 February 2015, https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf

5　特定の情報通信機器・サービスに対する収集努力

NSA の活動の内、スマートフォンやウェブカメラなど特定の情報通信機器やサービスに対する収集努力の中で興味深いものを幾つか紹介する。

（1）スマートフォン攻略

ア　概要[82]

スマートフォンは、革新的な情報通信機器であるが、それ故に同時にインテリジェンスの対象としても極めて重要なものである。従って、米 NSA、英 GCHQ 初め各国機関はスマートフォン攻略に大変な努力を傾注しているのは間違いない。

しかし、本件については、現在までに幾つかの分析と内部資料が報道されているものの、まだ断片的であり、取組の全体像を知り得る状態には至っていない。そこで、断片的ではあるが判明した限りでスマートフォンに対する NSA 等の取組を紹介する。

先ず、スマートフォン端末にある記録情報は「宝の山」と言われる。それは、端末には諜報機関が興味を持つ持主の個人情報が集積されるからである。便利であるが故に、持主がスマートフォンを愛用し活用すればする程、持主の生活記録、個人情報がスマートフォンを経由し、またその上に記録されることとなる。即ち、交友交際情報、行動と位置情報の履歴[83]、（検索履歴等から）興味関心、写真、時にはクレジット・カード番号やパスワード情報まで、スマートフォンを通過し、また記録される。

そこで、NSA では、アイフォンと iOS、グーグルのアンドロイド、ブラックベリーの基本ソフトに対して、それぞれ専門の分析チームを置いて侵入方法やデータ抽出方法等を分析して来たと言う。

その成果として例示されているのが、例えば、某元米国防長官の息子が若い女性の身体に手を回している姿を自撮した写真や、外国の政府高官がテレビを見ながらソファに座っている姿を自撮した写真である。即ち、遠隔侵入で、通信回線を通じてハッキングして端末に記録されていた写真データを入手できるということである[84]。

---

[82] Marcel Rosenbach, Lura Poitras and Holger Stark, “iSpay: How （e NSA Accesses Smartphone Data,” *Spiegel Online,* 9 September 2013, accessed 22 October 2013, http://www.spiegel.de/international/world/how-the-NSA-spies-on-smartphones-including-the-blackberry-a-921161.html

[83] アイフォン端末に記録される位置情報の履歴は、従来相当長期間に及んでいたため、端末から持主の長期間の行動位置履歴を遡って取得することができたが、iOS4.3.3 のソフトでは、記録期間が 7 日間に制限された。

[84] スマートフォン端末情報を入手する方法としては、スマートフォンから直接データを収集する方法の他、パソコンから収集する方法もある。人によっては、パソコンにスマートフォンを同期させて、スマートフォン・データをパソコンに自動的に複写するように設定している場合があるが、この場合には、パソコンからスマートフォンのデータを取得することが可能であるとしている。

イ　個別端末の攻略

個別の端末を如何にして攻略するかについては、その一例が2010年11月付のGCHQ内部資料[85]に記載されている。本資料は、アイフォンを攻略する一方法として、アイフォンのUSID（機器毎に付与される識別コード）を利用して端末機器と利用者を特定した上で、「クオンタム」諸計画（第2部第2章7CNEで既述）によりマルウェアを端末に注入する方法を記述している。また、別の内部資料[86]によれば、2011年から2012年にかけてはサムスンやグーグルのアプリ提供サーバー（App Store Server）をハッキングすることにより、アプリをダウンロードしたり更新したりするため接続してくるスマートフォンに対して、マルウェアを注入する技術も開発されていた。これらを含む種々方法によりスマートフォンを攻略しているものと推定できる。

スマートフォン端末を攻略した上で何が出来るかについては、GCHQでは「スマーフ」（有名なベルギーの漫画に出てくる架空の種族）というコード名の様々なプログラムが準備されている[87]。それによれば、次の機能がある。

○　「ノイジィ・スマーフ」～端末のマイクを起動し収集した音を送信

--Rosenbach, Poitras and Stark, "iSpay:…" *Spiegel Online.*

85　ス資料GCHQ、 *iPhone target analysis and exploitation with unique device identifiers*, 12 November 2010, accessed 29 January 2015, http://www.spiegel.de/media/media-35662.pdf

86 ス資料、NTAT, "Synergising Network Analysis Tradecraft,"　(undated), accessed 22 May 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/2083944/uc-web-report-final-for-dc.pdf

--Ryan Gallagher, "NSA Planned to Hijack Goole App Store to Hack Smartphones," *The Intercept,* 21 May 2015, accessed 22 May 2015, https://firstlook.org/theintercept/2015/05/21/NSA-five-eyes-google-samsung-app-stores-spyware/

ス資料のNTATとは、UKUSA５ヶ国の合同研究チーム（Network Tradecraft Advancement Team）であり、2011年秋以降合同してアプリ提供サーバー攻略を研究している。それによれば、先ず、XKeyscoreを使用して、関心ある地域のアプリ提供サーバーを特定する。実際、仏、キューバ、セネガル、モロッコ、スイス、バハマ、蘭、露等のサーバーが特定されている。次に、そのサーバーを乗取ることにより、次の作戦が可能になるとしている。

①　サーバーに接続してくるスマートフォンにマルウェアを注入する。

②　接続してくる標的スマートフォンに特定の偽情報を送る。(これは第３部第１章で述べる「オンライン秘匿活動」の一種である。)

③　接続してくる標的スマートフォンからデータを抽出する。

④　サーバー自体から有用データを収集する（例として、サムスンのサーバーは、顧客と端末についてのデータをドイツ国内のサーバーに定期的に送信しているとしている)。

なお、2012年２月の時点では、実際にアプリ提供サーバーの乗取りまで進んだかは不明である。

87 James Ball, "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data," *The Guardian*, 27 January 2014, accessed 27 January 2015, http://www.theguardian.com/world/2014/jan/27/NSA-gchq-smartphone-app-angry-birds-personal-data

- 「トラッカー・スマーフ」～高精度の位置情報を取得して送信
- 「ドリーミィ・スマーフ」～電源が入っていないように装ったまま、電源を起動
- 「パラノイド・スマーフ」～スパイウェアの存在を秘匿する機能

これに加えて、端末に記録されているデータは、基本的に全て取得できるとしている。

正に、諜報機関は、スマートフォン端末を、持主に対するマイクや位置情報発信の監視機材として使用できる能力を有しているということである。

なお、このような能力を裏書する UKUSA 諸国首脳の発言がある。即ち、ニュージーランドのジョン・キー首相は、2015 年 6 月ラジオのトーク番組で次の趣旨を述べている。「携帯電話は電源の入り切りに拘わらず盗聴器として使われる可能性があるので、自分は携帯電話は 3 ヶ月毎に交換しているし、機微な会合には持ち込まない」と[88]。

ウ　通信回線・システムからのデータ収集・利用[89]

個別の端末を攻略しなくても、シギントデータの収集態勢（第２部第２章）で述べた通信基幹回線等から収集する大量のデータから、スマートフォン関連のデータを抽出利用することが可能である。

スマートフォン関係で通信回線を通過するデータには多様なものがあり、NSA と GCHQ はそれらのデータを、典型的なメタデータの他に、ソーシャル・アプリ（social apps）、地理アプリ(geo apps)、ウェブサイトへの接続(http linking)、ウェブメール（web mail）、画像等の通信（MMS: multimedia messaging service）、モバイル広告（mobile ads）通信、その他に分類して利用分析しているとされる。

①　位置情報

メタデータ分析（第２部第３章の１）で述べたように、NSA は FASCIA という位置情報データベースを構築して、スマートフォンを含む世界中の携帯電話の位置情報を大量に収集してデータベースを構築して分析に使用している。

このための位置データは、主に移動通信体としての通信回線接続のための位置特定情報の他、スマートフォンへの位置情報関連サービスから取得されているとされる。そして、例えば、アイフォンだけで、位置情報を利用（即ち、送信）するアプリが 200 以

---

88 New Zeeland, PM John Key, interview on 11 June 2015, Si and Gary, *More FM*, accessed 12 June 2015, http://www.morefm.co.nz/Si--Gary-PM-John-Key-11-June/tabid/96/articleID/24419/Default.aspx/ 同首相の携帯電話はそれ自体に相当の保安措置が採られているのであるが、更に首相自身もこれだけの秘密保全措置を採っているのである。注目すべきであろう。

89 Ball, "Angry Birds and 'leaky' phone apps…," *The Guardian*,
--James Glanz, Jeff Larson and Andrew W. Lehren, "Spy Agencies Tap Data Streaming From Phone Apps," *The New York Times,* 28 January 2014, accessed 27 January 2015, http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0

上あるとされ、これらのアプリを使用する度に、持主の位置情報が発信されているということになる。

なお、詳細は不明であるが、位置情報では、特にスマートフォンによるグーグルマップ地図検索が有益なデータ源であるとされ、GCHQ の内部資料では「スマートフォンでグーグルマップを使用する者は、皆 GCHQ（データ収集）システムの支援者である」と述べている程である[90]。

② 各種アプリ使用に伴うデータ収集

スマートフォンには大量の各種アプリが有償、無償で提供されている。ところで、これらのアプリには、アプリ利用者に有益な広告を提供するなどの目的で、アプリ利用と同時に、自動的に端末内の一定のデータを広告会社や分析会社に送信するものが多い。つまり、利用者が広告付きのアプリを開くと、自動的に広告ネットワーク・サーバーに接続要求が出されるが、その要求には、端末の機種、機材固有番号、携帯端末識別番号 IMEI、位置情報等のデータの送信が付随している。

これらに加えて、スマートフォンが如何なるデータを送信するかは、それぞれの広告会社や分析会社と端末との関係による。

そして、ネットワーク広告を手掛けるグーグル社の広告部門や「バーストリ」社（2014 年アップルが買収）などは、広告関連アプリ利用の際に、一般的に電話番号、年齢、性別等を収集している。更に、「ミレニアム・メディア」というモバイル広告会社に至っては、収入、教育レベル、民族、婚姻状態、子供の数、性癖（異性愛、同性愛、両性愛、その他）などのデータまで収集しようとしているという。そして、利用者がこれらのデータを（意識しているか否かに拘わらず）広告会社に提供すれば、それに伴い NSA や GCHQ はそのデータを傍受して利用できるということになる。

なお、「アングリー・バード」というゲームソフト（フィンランドのゲーム会社が制作）は１７億回以上ダウンロードされているという世界で最も人気のあるゲーム・ソフトであるが、その内の特定の特別版は「ミレニアム・メディア」社が関係を持っているという。その特別版を利用している者は、その求めに応じて個人情報を入力すれば、それは同時にシギント機関に傍受されている可能性が高いということである。

③ データ抽出ソフト BADSS

上記のように、各種アプリ使用に伴い膨大なデータが通信回線上を往来しており、それを NSA や GCHQ は収集しているのであるが、余りにもデータ量が膨大であるため、必要なデータの検索抽出に膨大な労力を割かなければならないとされる。そのため、2011 年頃の GCHQ 内部資料[91]によれば、BADASS というデータ検索抽出システムを

---

[90] Ball, “Angry Birds and ‘leaky’ phone apps…,” *The Guardian*,

[91] ス資料 GCHQ、*Mobile apps doubleheader: BADASS Angry Birds*, undated, accessed 27

開発して、作業の省力化と迅速化を図ったという。それによれば、情報関心に沿って一定の事項を入力して検索すると関連データが自動的に抽出できるというものであり、これによって、従来6週間も要した作業が6分間に短縮されたとしている。

エ　「金の塊」

2010年5月付NSAの内部資料[92]によれば、標的がソーシャル・メディアにスマートフォンで撮った写真を掲示しているのは、分析官にとって「金の塊」だそうである。それから検索抽出できるデータは数多く、写真の他、位置情報、メールアドレス、電話番号、友達リスト他の交友交際関係のデータを収集できるとしている。

ソーシャル・メディアに自分の写真を掲示（アップロード）する人は、それが如何なる効果を及ぼすかを良く理解して行うべきであろう。

（2）携帯電話通信網に対する取組

ア　「オーロラゴールド」作戦[93]

携帯電話網からデータを収集するには、その前提作業として、携帯電話網の現状を把握して、その脆弱性を確認する必要がある。そのための作戦が、「オーロラゴールド」である。

「オーロラゴールド」では、IR.21という資料、これは世界中の携帯電話の接続に関する技術資料とされるが、常に最新のIR.21を収集することにより、最新の通信網の状況を把握しようとしている。併せて、（IR.21資料やシギント活動から把握した）主要な携帯電話会社の運用関連のメールアドレスを（2012年5月現在）1200以上から情報を収集している。

January 2015, http://www.spiegel.de/media/media-35670.pdf
--Micah Lee, "Secret 'BADASS' Intelligence Program Spied on Smartphone," *The Intercept,* 26 January 2015, accessed 27 January 2015,
https://firstlook.org/theintercept/2015/01/26/secret-badass-spy-program/

[92] ス資料NSA, *Converged Analysis of Smartphone Devices*, May 2010, accessed 27 January 2015,
http://www.propublica.org/documents/item/1009550-converged-analysis-of-smartphone-devices-NSA-may

[93] Ryan Gallagher, "Operation Auroragold," *The Intercept,* 4 December 2014, accessed 5 December 2014,
https://firstlook.org/theintercept/2014/12/04/NSA-auroragold-hack-cellphones/
--ス資料NSA、"Auroragold Project View 2011," *The Intercept,* accessed 5 December 2014,
http://www.documentcloud.org/documents/1374175-auroragold-project-overview.html#document/p1
--ス資料NSA、*Auroragold Working Group*, 6 June 2012, accessed 5 December 2014,
http://www.documentcloud.org/documents/1374178-auroragold-working-group.html#document/p1

これらの結果、2012 年 5 月現在で、世界の携帯電話事業者が 985 社あると推定されるが、その内 701 社について必要な技術情報を収集済みであるとしている。

このようにして、通信システムの最新状況を把握することにより、データ収集に利用できる脆弱性を特定し、或は脆弱性を装入することが可能であり、また、事業者が導入する通信暗号についての詳細情報を得ることができるとしている。

イ　携帯電話で使用する暗号解読

NSA は携帯電話で使用する暗号解読にも努めており、内部資料[94]によれば、第 2 世代通信 GSM 通信について、最も広汎に使用されている A5/1 方式通信は暗号鍵が無くても解読できると述べている。

また、別の 2010 年 2 月付の内部資料[95]によれば、第 4 世代通信の TD－LTE について、2010 年初めには収集が可能となったとしている。同資料によれば、TD－LTE 通信は同 2010 年に始めて市場でサービスが開始される予定であるが、それよりも早く収集を成功させたとしている。

（3）テキストメッセージのデータベース「Dishfire」計画[96]

「Dishfire」とは、収集した（携帯電話による）テキストメッセージ通信（SMS 通信）を保管するデータベースであり、且つその中から有益なデータを自動的に抽出処理するシステムである。

ア　テキストメッセージ（ショートメールサービス）の普及

2011 年 6 月付の NSA 内部資料[97]によると、2011 年現在、全世界では携帯電話が 53 億台も普及しているが、その携帯電話通信ではテキストメッセージが主体であり、その量は 2010 年で 6 兆件を超え、2013 年には 10 兆件を超える見込みであるという。更に、

94　ス資料 NSA　"How the NSA pinpoints a mobile device,"　*The Washington Post*, undated, accessed 29 January 2015,
http://apps.washingtonpost.com/g/page/world/how-the-NSA-pinpoints-a-mobile-device/645/

95　ス資料 NSA、*Site Makes First-Ever Collect of High-Interest 4G Cellular Signal,* 23 February 2010, accessed 30 January 2015,
http://www.documentcloud.org/documents/1374180-site-makes-first-ever-collect-of-high-interest.html#document/p1

96 James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian,* 16 January 2014, accessed 22 January 2015,
http://www.theguardian.com/world/2014/jan/16/NSA-collects-millions-text-messages-daily-untargeted-global-sweep

97　ス資料 NSA、*Content Extraction Enhancements For Target Analytics: SMS Text Messages: A Goldmine to Exploit, 9 June 2011,* accessed 22 January 2015,
http://www.theguardian.com/world/interactive/2014/jan/16/NSA-dishfire-text-messages-documents

通信内容も送金など重要な内容も含んでいる。

そこでNSAとしては、当然ながら、このテキストメッセージを保管分析して情報分析に使用することとなる。そのシステムが「Dishfire」である。

イ　Dishfire

NSAのシギント収集態勢により収集している携帯電話テキストメッセージは、2011年4月現在で一日平均約2億件（1年間で700億件）である。これは、そのままDishfireの保管データベースに蓄積される[98]。但し、そのままでは使い道が限られているので、そのデータベースには「Prefer」というソフトウェアが付加されており、これがデータを自動的に分析して一定のデータを抽出加工して、さらに分析し易い形式に変換している。

ウ　「Prefer」で抽出処理されているデータ

「Prefer」で抽出処理されているデータの種類と1日当りの件数の一部は次の通り。

- 名刺情報　～～11万件以上
- 位置情報（地理案内サービス等から抽出）　～～ 7万件以上
- 国境通過情報（ネットワーク接続情報から抽出）　～～160万件以上
- 経済取引情報（クレジット・カード支払、携帯電話間の送金、銀行送金等）　～～80万件以上
- 旅行予定情報（旅行会社の連絡情報から抽出）　～～ 5千件以上

このデータベースは、有効性が高いとされている。

（4）ウェブカメラを使用した監視

ア　ウェブカメラによる監視

ウェブカメラは、本来インターネットを利用した遠隔地間の画像の生中継用に開発されたようであるが、現在は、多くのパソコン端末に標準装備され、ビデオチャット（画像付きの通話）に利用されている。ヤフー・メッセンジャー、グーグル・ハングアウト、アイチャット、スカイプ等にその機能がある。また、パソコン端末搭載のウェブカメラの性能が向上したため、これで動画を作成しビデオ投稿する者もいる。

NSAが、ウェブカメラを装備したパソコン端末をハッキングして、そのウェブカメラを使用して持主の行動を監視するなど情報収集に使用できることは、NSAの技術から見れば、当然可能である。但し、現在迄に報道されたNSA内部資料にはこの関係の資料が見られない。そこで、傍証として、NSA以外の個人、組織がその能力を有することを見てみたい。

---

98 このデータはコンテンツ情報であるので、米国人の携帯電話によるテキストメッセージ通信は排除されている。

イ　FBI などによるウェブカメラの使用

2013 年 10 月に米国で起きた刑事事件では、ある男が高校生の同級生の女性のパソコンを Remote Administration Tool(RAT)という遠隔操作ソフトを使用して支配し、そのウェブカメラを起動して、ヌード写真を撮影し取得したものがあった。ウェブカメラは起動すると起動中を知らせる LED が点灯するが、この事件では LED を点灯しないように操作していたため女性はその起動に気が付かなかった。ところが、男が女性にヌード写真を送ってきたので発覚したという[99]。

また、FBI は、捜査のため必要があれば、令状を得て、犯罪容疑者のパソコン端末をハッキングして、パソコンに記録されたファイルや写真、Ｅメール等を入手しているが、更に、2012 年のある事件捜査に関連して、秘密裡にパソコンのウェブカメラを起動する能力を有することが明らかになった。同事件は、居所不明の男が盛んに米国各地に爆弾を設置したとの脅迫を送付してくるため、同人のパソコンを突き止め、これをハッキングしてウェブカメラを使用して情報を収集しようとしたものである。FBI ではウェブカメラの使用能力は抑制的に運用しており、主としてテロ事件と最重要犯罪の捜査に限定しているという[100]。

ウ　中国等によるウェブカメラの使用

ウェブカメラを使用した情報収集は、米国以外でも幅広く行われているようである。

欧州企業ガンマ・グループ社は FinFisher という監視用ソフトウェアを開発して、世界中の諜報機関や治安機関に販売しているが、その製品は、秘密裡に標的情報システ

---

[99] Ashkan Soltani and Timothy B.Lee, "Research shows how MacBook Webcams can spy on their users without warning," *The Washington Post,* 18 December 2013, accessed 20 January 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/

[100] Craig Timberg and Ellen Nakashima, "FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance," *The Washington Post*, 7 December 2013, accessed 2 February 2015, http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story_2.html

本事件では、爆弾テロの脅迫者は、Ｇメールやヤフーメールを使用して連絡を取ってくるため、脅迫者の所在地とパソコン端末を特定できないが、通信内容の分析から、イラン居住の可能性が大であるとされた。FBI は、脅迫者のパソコン端末を特定出来ないため、脅迫者がヤフーメールのアカウントにアクセスしたら、世界中の何処の如何なる端末からアクセスして来たとしても、その端末にマルウェアを送付するようにソフトウェアを設計したという。但し、上記記事からだけでは、ヤフーメールのアカウントにアクセスしただけで、当該端末にマルウェアが送付されるのか、或は、同アカウントに FBI のマルウェア注入用サイトに誘引するメールを送信していたのか、明確ではない。

ムに侵入して、ウェブカメラとマイクを使用したリアルタイム監視が可能であるとしている[101]。

また、2009年にカナダ・トロント大学が発表した研究報告書[102]によれば、2008年から2009年にかけて海外チベット人社会に対する中国によるサイバー諜報活動を研究したところ、中国海南島を拠点とするグループが、ダライ・ラマ事務所とチベット人諸組織に対する情報収集を行うために、世界１０３カ国に所在するチベット諸組織関係の1295台以上のコンピュータ端末に侵入していたことを発見したという。そして、そのマルウェアには、秘密裡にパソコン端末を起動してウェブカメラとマイクを使用する能力があったとしている。

このようにウェブカメラを使用した監視活動や情報収集が蔓延している以上、NSAだけが実施していないと考える合理的理由は見出せないであろう。

（５）顔画像収集と生体情報による個人識別[103]

従来NSAは、収集データとしては、文字データや音声データに焦点を当ててきたが、今や顔画像、指紋、虹彩、歩き方など生体情報による自動個人識別にも力を入れているという。

ア　顔画像

特に顔画像については、組織的収集努力を始め、2011年の内部資料によれば、一日数百万の画像を入手しているが、その中に識別可能な顔画像が５万５千件ほど含まれるという。

NSAは顔画像を入手するため、通信基幹回線からの収集データの中から、Eメール、テキストメッセージ、ビデオ通話の中の顔画像情報を抽出収集している。

関連して、英国GCHQは、NSAの支援を受けて、「オプテック・ナーブ」というプログラムを実施している。これは、ヤフーのビデオチャットから大量の顔画像取得を目指すものであり、2008年の半年間で、世界中のヤフーの利用者のアカウント180万以上から画像を収集したという。データが過大になるのを防止するため、５分間のビデオチャットに付き１枚の画像を抽出保管しているという。（但し、問題は、想定以上に性的な画像が多いことであるという。あるサンプル調査では、取得画像の７％が性的画像

---

101 Soltani and Lee, “Research shows how MacBook Webcams can spy …,” *The Washington Post,*

102 University of Toronto, Munk Centre for International Studies, *Tracking GhostNet: Investigating a Cyber Espionage Network,* 29 March 2009, accessed 2 February 2015, http://www.nartv.org/mirror/ghostnet.pdf

103 James Risen and Laura Poitras, “NSA. Collecting Millions of Faces From Web Images,” *The New York Times*, 31 May 2014, accessed 30 June 2014, http://www.nytimes.com/2014/06/01/us/NSA-collecting-millions-of-faces-from-web-images.html?_r=0

であり、これらの画像を除去して自動的に識別可能な顔画像を抽出する課題があるとしている。）[104]

更に、顔画像の収集では、様々なデータベースからの取得に取り組んでおり、例えば航空旅客データからの収集、或は、他国の国民登録カード・データベースからの収集にも取り組んでいる。そのため、パキスタン、サウジアラビアやイランのデータベースに侵入しようと試みている。

米国政府機関は、それ自体の行政権限に基づき膨大な顔画像を保持しており、運転免許証、米国旅券、外国人の米国査証申請などが大きなものであるが、NSA の報道官は、取材に対して運転免許証と米国旅券に付随する顔画像には NSA はアクセスしていないと述べたが、外国人の米国査証申請についてはコメントを避けたという。外国人の米国査証申請に伴う顔画像は、NSA のデータベースに記録されている可能性が高いということになる。

NSA は、現在進行形で、顔画像による個人識別のための研究深化とデータベース構築を進めていると考えられる。

イ　その他の個人識別情報など

NSA は、顔画像の他、個人識別できる生体情報の収集分析にも努めているようであり、外国人の虹彩情報を収集しているとされる。

また、NSA は CIA と国務省と協力して、「パイシーズ（魚座）」というプログラムを推進しており、様々な国の国境の検問所において、生体情報を収集していると言われる。

更に、画像情報では、国家地理空間諜報庁 NGA と協力して、屋外の観光写真などの特徴を、NGA の地理画像などデータと照合して、場所を特定する能力を保有しているという。

104　Spencer Ackerman and James Ball, “Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ,” *The Guardian,* 28 February 2014, accessed 2 February 2015, http://www.theguardian.com/world/2014/feb/27/gchq-NSA-webcam-images-internet-yahoo.

６　その他収集の為の基礎作業

NSA によるインターネットに対する取組は、正に世界のインターネット空間の支配を目指すものである。そのために NSA（及びセカンド・パーティ諸国）は大変な努力をしている。その努力の程を理解するために、幾つかの基礎作業を紹介する。

（１）「ハシエンダ」計画他～一国全体のポート・スキャン[105]

インターネットでコンピュータが通信をする際には、IP アドレス（インターネット上の端末のアドレス）に加えて、「ポート番号」を使用している。ポート番号とは、インターネット通信でコンピュータが使用する通信プログラムを識別する番号であり、0 番から 65535 番までである。そしてこのポート番号には、①定型的に良く使われる公知の番号（例えば、HTTP 通信用のポート 80 番）、②登録され開示された番号、③その他の誰でも自由に使用できる番号の３種類がある。このように、ポート番号には多種多様なものがあるが、一部のポートの通信プログラムには欠陥や脆弱性があることがあるという。

そこで、特定の端末に浸透しようとすれば、端末の使用する IP アドレスに加えて、その端末の脆弱性を発見するための基礎作業として、特定端末の全てのポートがどのような状態になっているかを把握（ポート・スキャン）することが有効である。

ここまでは当り前の話であるが、注目されるのは、この「ポート・スキャン」を NSA とセカンド･パーティ諸国の英加豪あわせて４箇国が分担協力して特定国の全ての端末に対して行い、これを予めデータベース化しておく作業「ハシエンダ」計画他が存在することである。内部資料によれば、2009 年現在で既に２７箇国に対してスキャンが完了し、５箇国に対して一定範囲のスキャンを実施したという。この成果はデータベース化され、米英加豪諸国の諸機関が利用できるようにしている。

更に、「ポート・スキャン」の成果は、単に将来の為にデータベース化するだけではなく、「作戦中継機」の開拓にも使用されている。「作戦中継機」（Operation Relay Box）とは、コンピュータ・ネットワーク作戦を実施するに当たり、脆弱性を有する第三者のコンピュータ端末を勝手に利用して踏み台にすることにより、作戦実施機関を秘匿するためのものである。内部資料によれば、2010 年 2 月にカナダの機関 CSE 通信保全局では職員２４人の１日（５～８時間）の作業で、潜在的「作戦中継機」3000 台以上を特定することができたという（要するに、必要な時に何時でも利用できる脆弱性を有する端末を特定したということである）。

105　“August 15 NSA GCHQ Leaks Hcienda, Mugshot, Olympia, ORB Slides, Internet Colonization, Edward Snowden 2014,” *USNEWSGHOST*, 18 August 2014, accessed 15 January 2015, https://usnewsghost.wordpress.com/2014/08/18/august-15-NSA-gchq-leaks-hacienda-mugshot-olympia-orb-slides-edward-snowden-2014-spying-program-monstermind/

インターネット空間を支配するには、インターネット上の全ての端末に関して重要なことは全て理解しなければならず、そのためにはこのような取組までしているということである。

（２）連絡先リスト、友達リストの大量収集[106]

情報収集対象とする可能性のある者に対する基礎資料として、インターネット通信から個人の連絡先リストや友達リストを大量に収集してデータベースを構築している。これにより、隠れた交友関係や特定集団内の人間関係などの分析の材料となるという。但し、米国内でこれを実施するには、米国人データの収集に関連して対外諜報監視裁判所による令状が必要となる。そこで、データ取得は裁判所の関与が不要な米国外で実施している。

先ず連絡先リストであるが、Yahoo　Mail、Hotmail、Gmail や Facebook などのメール・サービスでは、連絡先リストをシステム上に作成保管できる。但し、これらデータは端末に保存される訳ではなく、各社のデータセンターに保管されている。利用者がメール・サービスを利用しようとして各社のデータセンターにアクセスし連絡先リストを見ようとすると、利用者端末に連絡先リスト・データも送信されてくる。そこで、その送信されてくる連絡先リストを通信途中の通信基幹回線に設置してある設備で傍受取得するという。或は、（第２章３の「マスキュラー」計画で）既述したようにグーグルやヤフーのデータセンター間通信を英国内で傍受しており、そこからデータを取得している可能性もある。これらのリストには、通常、連絡先のメールアドレスと名前の他に、電話番号、住所、勤務や家族関係情報が含まれることも多く、情報価値は高いという。

このリストの取得は大量であり、2012 年１月の某日１日間で６９万件、年間では２億５千万件にも及ぶ件数である。

また、Facebook 等の友達リストも収集している。これも、連絡先リスト同様の方法

106　出典資料は次の通り。
--Barton Gellman and Ashkan Soltani, “NSA collects millions of e-mail address books globally,” *The Washington Post,* 14 October 2013, accessed 22 October 2013, http://www.washingtonpost.com/world/national-security/NSA-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html
--ス資料　“The NSA‘s　problem? Too much data,” *The Washington Post*, undated, 22 October 2013, http://apps.washingtonpost.com/g/page/world/the-NSAs-overcollection-problem/517/
--ス資料　“SCISSORS: How the NSA collects less data,” *The Washington Post*, undated, 22 October 2013, http://apps.washingtonpost.com/g/page/world/how-the-NSA-tried-to-collect-less/518/
--ス資料　“An excerpt from the NSA’s Wikipedia,” *The Washington Post*, undated, 22 October 2013, http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/

で収集している。この収集量も巨大であり、一日平均５０万件程収集している。
実に大変な基礎作業である。

（３）シギント・ユーザーに対する関係者電話番号の提供呼掛け[107]

NSA 内部資料や国務省秘密文書に、シギントの基礎となるシギント・ユーザーとの協力関係を示す具体例があるので、紹介する。

ア　NSA 担当官からの要請

2009 年 10 月、NSA の担当者はシギント・ユーザーとのリエゾン担当者に対して内部メモを送付して、ユーザーに対してユーザーが交流を持つ外国政府高官の電話番号情報の提供を呼び掛けるように要請した。同内部メモによれば、従来も、時々米国政府高官から政治・軍事部門の外国政府高官の各種電話番号やファックス番号の提供を受けることがあった。更に、最近、ある米国職員から、世界の指導者３５人の電話番号２００個の提供を受け調査したところ、その内４３個は未把握の番号であった。現在までのところ、この４３の電話自体は機微な内容の通信には使われていないようで、直接的に有益な情報を得るには至っていないが、他方、これらの番号から他の有益な電話番号を把握することができた。ついては、ユーザーに対して番号提供を働き掛けて欲しいというものである。

米国では、当然の事ながら、このようにインテリジェンス・ユーザーを含めてインテリジェンスに協力する風土があるのが注目される。

イ　国務省からの要請

関連して想起されるのが、2010 年のウィキリークスによる米国秘密情報の大量公表である。これは、同年、米陸軍の情報分析官ブラッドレー・マニング（後に改性・改名してチェルシー・マニング、現在、反スパイ法等で懲役３５年の服役中）が、軍の秘密情報システム SIPRNet から取得して漏洩したものであるが、その中には軍事報告５０万件と外交公電２５万件が含まれていた。その外交公電の中でも興味深いのが、2009 年７月に国務省が国務長官名で世界の公館に送付した公電である[108]。

同公電は外交官に報告すべき情報関心を示したものであるが、その中で注目されるのが、外交官に対して諸外国要人の個人情報を報告するよう要請していることである。外交官が収集した個人情報は、国務省諜報調査局（Bureau of Intelligence & Research）に集約され諜報コミュニティに配布されるが、諜報コミュニティは個人情報に関しては

---

[107] James Ball, “NSA monitored calls of 35 world leaders after US official handed over contacts,” *The Guardian,* 24 October 2013, accessed 25 October 2013, http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/

[108] “US embassy cables: Washington calls for intelligence on top UN officials,” *The Guardian,* 28 November 2010, accessed 24 December 2010, http://www.theguardian.com/world/us-embassy-cables-documents/219058

国務省に依存するところ大であるとしている。個人情報として例示されているのは、名前、所属、肩書、その他名刺記載事項、固定電話番号、携帯電話番号、ファックス番号、イントラネット等のハンドルネーム、Ｅメールアドレスや URL、クレジット・カード番号、航空会社のマイレージカード番号、勤務スケジュール等と広汎に及んでいる。これらの情報が、シギント機関としても有用なことは、先に述べた NSA 担当官からの電話番号の提供呼掛けを見ても自明であろう。

なお、同公電では、北朝鮮高級外交官については指紋、署名等の生物的情報まで要求している。

国務省がこのような情報を収集して諜報コミュニティに配布していることが、正に国務省諜報調査局が諜報コミュニティに属していると言う所以であろう。それと同時に、諜報コミュニティが存在すると言うには、関係諸機関を諜報コミュニティと呼ぶだけではなく、その間に諜報活動に関してこのような一定の協力関係が存在することが前提となることも理解できるであろう。

第４章　コンピュータ・ネットワーク作戦（CNO）と NSA

１　CNO に対する NSA の役割

既述（第１部第２章の３任務）したように、NSA の広報資料[1]によれば、その主任務はシギントと情報保証の二つであるが、これに加えて、コンピュータ・ネットワーク作戦（Computer Network Operations: CNO）を可能とすることが、NSA の任務として挙げられている。なお、同広報資料では、この CNO はネットワーク戦争（Network Warfare）と同義として扱われているのが注目される。

そこで、ここで言う CNO とは何か、そして NSA の活動が如何なる意味で CNO を可能とするのかなど、NSA の活動と CNO の関係を見ることによって、シギント機関である NSA がネットワーク・セキュリティやネットワーク戦争に果たす役割について、明らかにして行きたい。

（１）コンピュータ・ネットワーク作戦（CNO）とは何か。

NSA や国防総省の公表資料[2・3]によれば、コンピュータ・ネットワーク作戦 CNO は、コンピュータ・ネットワーク攻撃（CNA）、コンピュータ・ネットワーク防禦（CND）、コンピュータ・ネットワーク開拓（CNE）の三つで構成される。それぞれの定義は概ね次の通りである。

- コンピュータ・ネットワーク攻撃（CNA）～コンピュータやコンピュータ・ネットワーク自体、或いはそれらに存在する情報に対して、コンピュータ・ネットワークを通じて、妨害、使用不能、機能低下、破壊をもたらす行為。
- コンピュータ・ネットワーク防禦（CND）～国防情報システムやネットワークに対する攻撃、侵入、妨害その他権限なき行為に対して、コンピュータ・ネットワークを通じて、防護し、監視し、分析し、探知し、対応する行為。
- コンピュータ・ネットワーク開拓（CNE）～コンピュータ・ネットワークを通じて行う、標的又は敵の情報システムやネットワークからデータを収集する作戦、及びその収集する能力を構築する行為。

---

[1] US NSA/CSS, *The NSA/CSS Mission,* accessed 26 August 2014, http://www.nsa.gov/about/mission/index.shtml.

[2] US NSA/CSS, *Computer Network Operations,* accessed 6 February 2015, https://www.nsa.gov/careers/career_fields/netopps.shtml
これは NSA の職員採用向けの広報資料である。

[3] US Air University, *Computer network operations & network warfare operations (citing Joint Publication 3-13 Information Operations, 27 November2012),* accessed 7 February 2015, http://www.au.af.mil/info-ops/netops.htm.

そして、国防総省の定義では、CNO とは、CNA、CND そしてこれに付随する CNE とされており、CNO の中心は攻撃 CNA と防禦 CND であることが注目される。また、（NSA 広報資料で CNO と同義的に扱われている）ネットワーク戦争も、国防総省の公表資料では、ネットワーク攻撃、ネットワーク防禦とこれらの支援活動と定義されており、ここでも攻撃 CNA と防禦 CND が主体である。

この定義は、NSA が可能とし軍が直接担当するコンピュータ・ネットワーク作戦とは、主としてコンピュータ・ネットワークを通じて行う攻撃と防禦であることを反映したものであろう。

それでは次に、このような CNO に対して NSA が如何に密接な役割を果たしているのか、考察してみたい。

（２）CNO に対する NSA の役割～CNA、CND、CNE の三位一体関係

ア　CNE（コンピュータ・ネットワーク開拓）

先ず、CNE については、NSA の主任務はシギントと情報保証であるが、CNE、即ち、コンピュータ・ネットワークにおける資料源開拓は、既述（第 2 部第 2 章の７）したようにシギントの重要構成要素であり、NSA の本来任務そのものである。

イ　CNA（コンピュータ・ネットワーク攻撃）

次に、CNA については、一言で言えば、NSA による（CNE を含む）シギント活動が正にその基盤をなしているということである。

第１に、先ず、標的や敵を攻撃するには攻撃対象の実態が分かっていなければならない。何処に如何なるコンピュータやコンピュータ・ネットワークが存在し、その脆弱性が何なのかを知らなければ、有効・効果的な攻撃はなし得ない。NSA は、そのネットワークに対するシギント活動の基礎として、世界中のコンピュータやネットワークに対するデータを収集し、実態を把握している。これは既述した「宝地図」（第２部第２章１の（３））を見ても明白である。攻撃の前提としての実態把握は、NSA のシステムと活動に依存するところが大である。

第２に、NSA はその CNE によって、既に多くの潜在敵のネットワークに侵入し、多くのマルウェアを注入し、システムの実態を解明し支配している。そこで、攻撃するとなれば、これらのマルウェア（インプラント）はそのまま攻撃の手段を提供することとなる。或いは、攻撃に際しては、多くの作戦中継機（プロキシ）を必要とすることがあるが、「ハシエンダ」計画（第２部第３章６の（１））で見たように、NSA はこれも既に確保しているのである。

第３に、NSA のシギントのためのネットワークのインフラ自体が、攻撃のためのインフラとなる。第 2 部第２章の収集態勢（シギント・プラットフォーム）で見たよう

に、NSA はサイバー空間に対して、米国内だけでなく世界中でさまざまなアクセス施設を構築している。このインフラは、攻撃の際のインフラともなるのである。

実際、NSA の内部文書[4]でも、CNE 活動は容易に CNA 能力に転換できると述べられている。

ウ　CND（コンピュータ・ネットワーク防禦）

コンピュータ・ネットワークの広義の防禦を考えると、先ず、攻撃され難いシステム構築（これはここで言う CND というよりも、それ以前の基礎である）が必要となる。これは、NSA の情報保証の業務そのものである。それ故、NSA 長官は、米国の国家安全保障（通信情報）システムの責任者に指定されているのである。

その上で CND については、第１に、敵対勢力からのネットワークに対する攻撃、或いはその前提となる侵入からの防禦システムの構築、運用には、常日頃 CNE という矛を運用している NSA のノウハウが基礎になる。

第２に、攻撃を受けた場合に、効果的に敵対勢力の CNA の発信源に対して反撃し、攻撃を停止させる、或いは、攻撃を事前探知して防禦態勢を構築する、状況によっては予防的先制攻撃を行うためには、普段から、潜在敵の攻撃能力を把握し、無害化する備えをしておかなければならない。そのためには、潜在敵対勢力による CNE を解明し、当該勢力の CNE と CNA のためのシステムに侵入しておく必要がある。そして、これは正に NSA のシギント活動、CNE 対策（Counter – CNE）である。NSA による中国や北朝鮮に対する CNE 対策の一端は、第２部第２章７の（５）で言及した通りである[5]。

第３に、NSA のシギントシステムは、また、防禦 CND のためにも利用できる者である。NSA 内部資料[6]によれば、QFIRE というシギントシステム（2011 年現在開発中）は、（どのように機能するかはよく分からないが）、防禦的機能もあるという。このように、NSA のシギントシステムは CND にも貢献するのである。

---

4 ス資料、NSA, Office of General Counsel, “CNO Legal Authorities,” circa 2010, p.51, 64, accessed 8 June 2015, https://www.documentcloud.org/documents/2092794-document-cyber-surveillance-documents.html#document/p9. 本資料では、CNE 要員による CNA 任務の兼任も言及されている。

5 David E. Sanger and Thom Shanker, “N.S.A. Devises Radio Pathway Into Computers,” *The New York Times,* 14 January 2014, accessed 26 March 2014, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0

6 ス資料、NSA, Technology Directorate, *Getting Close to the Adversary: Forward-based Defense with QFIRE,* 3 June 2011, accessed 9 February 2015, http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html

上記第２、第３に関連して、ロジャース NSA 長官（2014 年春就任）は、上院公聴会で米国に対するサイバー攻撃を抑止する方策を質問されて、方策の一つは「最新の技術を使って、攻撃後ではなく、攻撃前や攻撃中に攻撃者を特定することである」、また、「米国は、攻撃が何処から来ているのかを知っており報復する用意があることを、明確にすることである」と述べている[7]。

以上述べたことから分かるように、CNO を構成する CNA、CND、CNE は三位一体で不可分の関係にあり、また、NSA のシギント活動・情報保証と CNA、CND も不可分の関係にある。それ故に、NSA 長官がサイバー軍（2010 年発足）司令官を兼任しているのである。サイバー防衛やサイバー・セキュリティを真剣に考える者は、当該分野に於けるシギント機関の役割も理解するべきであろう。

（３）防禦システム

各種資料と報道を総合すると、サイバー攻撃からの防禦用のシステムとして、NSA は次のシステムを構築していると考えられる。

ア　Tutelage～～国防関係システム[8]（後述）

防衛関係情報通信システムに対する攻撃を、シギントを活用して事前に探知し、その侵入を阻止し或いは無害化して監視するなど、ダイナミックな防禦システム。

イ　Einstein 3～～米連邦政府一般官庁システム[9]

一般官庁のシステムを保護するシステム。所管は国土安全保障省であるが、技術は NSA が提供。諸通信事業者の協力を得て、一般官庁のインターネット通信網との通信を監視して、攻撃を探知し、侵入を阻止し或いは無害化する。そのため、通信事業者のシステムに NSA の監視システムを設置して、一般官庁とのインターネット通信はすべてそれを経由するようにし、そこで NSA のデータベースと照合して、過去にサイバー攻撃に関与した、或いは潜在敵と判明した通信パターン（コンピュータ・コードやシグニチャ）を検出し、侵入を阻止或いは無害化する。

---

[7] David E. Sanger, "N.S.A. Nominee Promotes Cyberwar Units," *The New York Times*, 11 March 2014, accessed 26 March 2014, http://www.nytimes.com/2014/03/12/world/europe/nsa-nominee-reports-cyberattacks-on-ukraine-government.html?_r=0

[8] Robert Sesek, "Unraveling NSA's TURBULENCE Programs," *IC Off the Records*, 15 September 2014, updated 26 January 2015, accessed 3 February 2015, https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html

[9] Ellen Nakashima, "DHS Cybersecurity Plan to Involve NSA, Telecoms," *The Washington Post,* 3 July 2009, accessed 7 February 2015, http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html

ブッシュ政権が 2008 年に開始した総合サイバー・セキュリティ計画の主要構成要素であり、2009 年オバマ政権もその実施を承認した。現時点では既に導入されていると見られる[10]。

ウ　MasterMind～～米国のサイバー空間全体[11]

2014 年 6 月にスノーデンがバムフォード氏のインタヴューで言及した進行中のプログラム。米国外から米国内への攻撃を、通信パターンから自動的に検知して、米国内通信回線への侵入を阻止する。但し、そのためには、米国外から米国に到達する通信を全て点検する必要があり、当然、通信基幹回線の米国上陸地点等の全てに監視検知システムを設置することとなる。また、同計画には、外国からの攻撃を検知した一定の場合には、その発信元に対して、自動的に反撃するプログラムも含まれているという。この場合には、攻撃中継機（プロキシ）とされた多くの第三者のシステムに損害を及ぼす可能性があるとされる。

このプログラムが現実にどれだけ進行しているかは不明であるが、このプログラムの存在は、サイバー空間のセキュリティを真に高めるためには、単なる端末や個別事業者のネットワークのセキュリティを高めるだけでは十分ではなく、一国のネットワーク全体を包含したセキュリティ対策も必要となることを示唆している。

（4）Tutelage システム～ダイナミックな防衛

Tutelage トゥートリジ・システムとは、国防関係情報通信ネットワークに対する侵入攻撃を、シギントを活用して事前に探知するなどして防禦するダイナミックな防禦システムであり、2009 年までには導入されたと見られる。NSA の内部資料[12]によれば、その概要は次の通りである。

ア　これまでの防禦システム

国防総省の情報ネットワーク NIPRNet は、秘密情報未満の機微な或は部内用の情報を扱うネットワークであるが、インターネット網と接続されている。その結果、インターネットを経由したサイバー攻撃を頻繁に受けている。

---

[10] ス資料、NVIOCOM, *NIOC Maryland Advanced Computer Network Operations Course,* circa April 2012, accessed 1 May 2015, http://www.spiegel.de/media/media-35657.pdf

[11] Edward Snowden, interview by James Bamford in June 2014, *Wired magazine*, August 2014, accessed 18 August 2014, http://www.wired.com/2014/08/edward-snowden.

[12] ス資料、NSA, NTOC, *TUTELAGE*, circa 2011, accessed 28 April 2015, http://www.spiegel.de/media/media-35685.pdf

インターネットとの接続点（gateway）は、内部資料では米国領土内７ヶ所、ドイツ２ヶ所、日本１ヶ所[13]が上げられているが、これらの接続点には当然ファイアウォールが設置され、既知のマルウェア等は遮断している。しかし、未知のマルウェアなどは即時に遮断できず、ネットワーク内に侵入を許してしまう事例も多いと考えられる。

そこで、従来は、接続点（gateway）を通過した全通信を記録した上で、事後的に記録を分析して、マルウェア等の容疑通信を抽出して、侵入報告を作成し、標的端末の管理者に通報して対策を求めていたという。しかし、この分析報告には数日間を要し、損害が発生する前に、侵入報告が関係者に到達するか課題があった。

イ　Tutelage システムの特徴

Tutelage システムでは、国防関係情報通信ネットワークに侵入されてから対処するのではなく、シギント能力を活用してネットワークに侵入される前から対抗措置を採ることに特徴がある。

即ち、攻撃者がマルウェアを作成している段階で、シギント活動により攻撃者の道具や技術を探知して、これに対する対処対抗手段を開発してインターネット接続点に配置する。更に、攻撃者の意図や標的を探知して、実際に侵入攻撃が実施される場合には、インターネット接続点（gateway）で侵入攻撃に対処しようとするものである。

ウ　対処対抗手段

インターネット接続点に設置する対処対抗手段にも色々なものがあり、既に開発された手段は次の通り。

- 警告（Alert/Tip）～国防関係情報通信システムへの侵入を検知して、防禦システム部門とシギント部門関係者に警告を発する。
- インターセプト（Intercept）～侵入通信は接続点で捕獲してその標的端末には到達しないようにするが、攻撃発信端末には、標的端末への侵入成功を偽装した通信を送信する。
- 代替（Substitute）～侵入させるが、侵入通信は変換して無害化し、他方攻撃発信端末には解読不可能な暗号通信を送信する。
- 転送（Redirect）～侵入させ活動させるが、そのマルウェアがデータを外部に送信しようとすると、その送信先が NSA の別サーバーに改変されて外部にデータが流出しないようにすると共に、そのマルウェア関連のシギント活動に利用する。

---

[13] 接続点は何れも米軍関係施設であり、米国内７ヶ所はワシントン DC の国防総省、バージニア州ノーフォーク、カリフォルニア州サンディエゴの各海軍基地、テキサス州サンアントニオ、カリフォルニア州ビール、ハワイ州ヒッカムの各空軍基地、オハイオ州コロンバスの兵站施設。国外は、ドイツのファイニンゲンとヴィースバーデン、日本の横田である。

- 遮断（Block）～接続点で通信を遮断する。発信端末或は標的端末の IP アドレスや（データ通信の）ポート番号に基づき一定の発信や受信通信を遮断する。
- 遅延（Latency）～接続点の通信通過速度を低下させ、時間を稼ぐ。
- TCP リセット（TCP　Reset）～攻撃者がアクセスしたいウェブサイトやファイルが既に存在しない､或は通信状況のため接続できないと思わせる信号を送信する。

内部資料作成時点（2011 年頃）には、既に２８の脅威グループに対してこれらの対処対抗手段を発動していたという。即ち、その時点で、世界中から国防関係情報通信システムへの侵入を図る脅威グループ２８について、CNE 対策のシギント活動によりその活動や技術の少なくとも一部は探知解明し、対策を採っていたということである。

エ　開発中の対処対抗手段

NSA では、更に多くの対処対抗手段を開発中であるが、興味深いものとしては次のものが挙げられる。

- Quantum Tip 或は Quantum Shooter～攻撃発信端末からの侵入通信を利用して、攻撃端末に対する逆攻撃（マルウェアの送信）を自動的に実施する。

相手方からの侵入攻撃を、即時に利用して、攻撃発信端末にマルウェアの侵入攻撃を行うというのは、正に、CND と CNE、Counter – CNE の一体化、一体的運用である。

オ　Tutelage システムの成功例

成功例として挙げられている中から、次の二つを紹介する。

- 2010 年国防総省高官に対するフィッシング攻撃の阻止

  シギント情報に基づいて、中国のハッカー集団「ビザンチン・ヘデス」内の特定グループによる攻撃手段に対する対処手段を 2009 年に開発し配備しておいた。すると、2010 年 10 月 21 日、22 日の両日、統合参謀本部議長、海軍作戦部長ら４高官に対して、PDF ファイルを使ったスピア・フィッシング攻撃があったが、NTOC（脅威作戦センター）が対処手段を発動し侵入を阻止した。
- 2010 年（？）12 月クリスマス・シーズン

  NTOC（脅威作戦センター）では、メリークリスマス・メールを大量に送付してマルウェア ZEUS を感染させようとする動きを探知したため、関連する特定ドメインへの通信を遮断して感染を防止した。

２　大統領政策指令第２０号「サイバー作戦政策」と標的リスト作成[14]

次に、実際の CNO の運用について、CNO と殆ど重複すると考えられる「サイバー作戦」関係文書を見てみよう。

それは、大統領政策指令第２０号（Presidential Policy Directive/PPD—20）「米国のサイバー作戦政策」である。この最大の特徴は、米国によるサイバー攻撃の潜在的標的のリスト作成と攻撃態勢の樹立維持を指示したものである。米国のサイバー作戦（戦争）準備も遂にここまで進展してきたのかと考えさせられるものである。

本大統領指令は、厳密に言えば、NSA というよりは米国サイバー軍に関係する指令である。しかし、NSA 長官はサイバー軍司令官を兼任し、且つ、NSA とサイバー軍は密接な関係にあるので、本指令の内容を紹介したい。

（１）広報資料とサイバー軍の大増強

2013 年 1 月の米国政府の広報資料[15]によれば、大統領は、最近、大統領政策指令２０号に署名した。同指令は秘密指定されているので、内容は非公開であるが、その骨子は、「同指令は、サイバー作戦の原則と手続を定めて、サイバー作戦を使用可能な国家安全保障のための諸手段に統合するものである。作戦の原則と手順は、我々の有する能力のより有効な計画、開発、使用を可能とすることを目的としている。」と述べて、サイバー作戦が実用段階に達していることを示唆している。

また、同広報資料は「我々の方針は、脅威に対抗するため必要な最小限の行動をとること、脅威対応では（サイバー作戦よりも）ネットワーク防禦や法執行を優先することである。」とも述べている。

他方、同年１月の報道によれば、国防総省は、サイバー軍の規模を（当時の）900 人から数年間で 4900 人程に増強する決定をしたという[16]。この大増強は、明らかに、大統領政策指令の決定と連動したものであろう。

その後 2013 年 6 月、本指令案の全文（2012 年 10 月時点のもの）[17]が漏洩報道された（大統領は 2012 年 11 月に署名したという[18]）ので、次に同指令案の内容をより詳しく見て行きたい。

---

[14] Glenn Greenwald and Ewen MacAskill, “Obama orders US to draw up overseas target list for cyber-attacks,” *The Guardian,* 7 June 2013, accessed 9 June 2014, https://epic.org/privacy/cybersecurity/Pres-Policy-Dir-20-FactSheet.pdf

[15] US, *Fact Sheet on Presidential Policy Directive 20,* January 2013, accessed 9 June 2014, https://epic.org/privacy/cybersecurity/Pres-Policy-Dir-20-FactSheet.pdf

[16] Ellen Nakashima, “Pentagon to boost cybersecurity force,” *The Washington Post,* 27 January 2013, accessed 5 February 2015, http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html

（２）政策指令の目的、定義

政策指令の目的は、2004 年 7 月の国家安全保障大統領指令（NSPP）第３８号を改正して、サイバー作戦についての最新の原則と手順を定めることである。

ここでいうサイバー作戦は、防御的作戦と攻撃的作戦とからなる。防御的作戦とは、差し迫った脅威、進行中の攻撃、或は悪意あるサイバー活動から、米国の国益を防禦し保護する目的で行う作戦で、その（妨害・拒否・破壊等の）効果が米国政府のネットワーク外に及ぶものである。即ち、防禦的作戦といっても、ネットワークを通じた情報収集（サイバー収集）やネットワーク自体の防護措置（ネットワーク防禦）は含まない。寧ろ攻撃発信元に対する反撃を含む概念である。

（３）作戦の原則と手順

ア　原則

- サイバー作戦は、他の諸々の手段、即ち、外交、広報、軍事、経済、金融、諜報、防諜、法執行等の諸手段と統合して運用する。
- また、国内のシステムやネットワークに（妨害拒否破壊等の）効果を及ぼすサイバー作戦は、大統領の承認を必要とする。但し、緊急サイバー活動に当たる防御的作戦においては、各省庁の長官が実施することができる。
- 更に、人の死亡、米国に対する重要な反撃、米国外交や経済に大きな悪影響を及ぼすなど、重要な結果を生じ得るサイバー作戦（サイバー収集を含む）については、大統領の承認を必要とする。

イ　防御的サイバー作戦

- 米国は、次の場合に防御的サイバー作戦を実施することを留保する。
  - ネットワーク防禦や法執行の手段では、不十分、或は時間的に余裕がなく、事前に承認したその他の方法ではより適切な対応が出来ないとき。又は、
  - 防禦的作戦の方が、他の手段より、効果的、適時的、効率的であると認められるとき。
- 防御的作戦では、脅威に対抗するための侵害行為は、実効的な最小限の措置を採るものとする。
- （緊急サイバー活動）差し迫った脅威や進行中の攻撃に対して、大統領の承認を得る暇がないときは、国防長官と所管省庁の長官は、緊急に防御的サイバー作戦を

17　ス資料、US Presidential Policy Directive/PPD-20, undated(October 2012), accessed 4 February 2015
http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text

18 “Pentagon creates 13 offensive cyber teams for worldwide attacks,” *RT,* 13 March 2013, accessed 9 February 2015, http://rt.com/usa/alexander-cyber-command-offensive-209/

実施することができる。緊急サイバー活動を行ったときは、速やかに大統領に報告するものとする。

ウ　攻撃的サイバー作戦

- 攻撃的サイバー作戦は、独特且つ非在来型の能力、即ち、敵対者に対して事前に全く或は殆ど気付かれずに、軽微から重大な損害を与え、世界中で米国の国家目的を推進する能力を提供することができる。しかし、攻撃的作戦能力は、特定標的に対するアクセスや攻撃手段が既に存在していなければ、その開発と維持には相当の時間と努力を要する。

  そこで、米国政府は、国家的重要性を持つ潜在標的を特定して、（他の攻撃能力と統合して）攻撃的サイバー作戦能力を樹立維持し、必要な場合には、その能力を行使する必要がある。
- 国防長官、国家諜報長官と CIA 長官は、６ヶ月以内に、その為の計画を立案するものとする。同計画は、攻撃的サイバー作戦能力を樹立維持すべき潜在標的（システムやインフラ）を特定し、攻撃発動の要件を提案し、その実施の為に必要な資源と手順等を提案するものとする。安全保障担当補佐官を経由して大統領の承認を得るものとする。

エ　継続的な悪意あるサイバー活動への対処

- 継続的な悪意あるサイバー活動に対しては、所管省庁は対応の基準と手続を定め、大統領の承認を求める。
- その基準と手続には、次の事項を含むものとする。
  - ネットワーク防禦や法執行の手段では、不十分、或は時間的に余裕がない場合には、サイバー作戦を実施することを留保する。
  - サイバー作戦の実施においては、重大な結果をもたらさないように、また、悪意あるサイバー活動に対抗するため必要とする最小限の措置を採るものとする。

（４）余話

米国は、以前からサイバー作戦を実施してきた。有名なものには、イランの核燃料施設に対する攻撃「オリンピックゲーム」（後述）がある。しかし、アレクサンダー前 NSA 長官によれば、その８年に及ぶ任期中に実施した攻撃作戦は、数える程(only a handful of times)しかないと伝えられている[19]。

---

[19] David E Sanger, “Syria War Stirs New U.S. Debate on Cyberattacks,” *The New York Times*, 24 February 2014, accessed 25 November 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0

但し、今回の大統領政策指令第２０号の内容から分かるのは、サイバー作戦を更に進めて、普段から潜在的攻撃標的リストを作成し、これに対する攻撃準備を行い、必要な場合には攻撃できる態勢の構築を決定したということである。それと同時に、サイバー軍の大増強を決定している。サイバー軍は基本的に攻撃的要素が強いと見られ[20]、今後の動向が注目される。

なお、米国の場合は内部資料が漏洩されたため、サイバー作戦政策が判明したが、北朝鮮や中国、ロシアの現状は如何であろうか。既に、米国以上の態勢を取っている可能性があるのではないだろうか。世界はここまで進んでいるのである。

因みに、スノーデン[21]によれば、打撃の大きな攻撃とは、一国の中枢ルーター、インターネットエクスチェンジ（IX：インターネット相互接続点）に対する攻撃であるという。ここを破壊されると、一国のインターネット通信はほぼ麻痺状態となるが、出来合いの部品交換で直ぐ回復できるようなものではなく、被害は大きいという。実際、2012 年 11 月 29 日にシリアで発生した中枢ルーターの障害は, NSA 職員のミスで発生させたと言われるが、大きな被害をもたらしたという[22]。

--David E Sanger and Thom Shanker, “N.S.A. Director Firmly Defends Surveillance Efforts,” *The New York Times*, 12 October 2013, accessed 9 February 2015, http://www.nytimes.com/2013/10/13/us/nsa-director-gives-firm-and-broad-defense-of-surveillance-efforts.html?pagewanted=all

[20] Edward Snowden, interview by James Bamford in June 2014, *Nova Next,* 8 January 2015, accessed 22 January 2015, http://www.pbs.org/wgbh/nova/next/military/snowden-transcript/.
本インタビューで、スノーデンは、サイバー軍は攻撃部署（attack agency）であると述べている。

[21] Snowden, interview by Bamford in June 2014, *Nova Next.*

[22] Snowden, interview by Bamford in June 2014, *Wired magazine*.

３　CNA、サイバー作戦の具体例

今後コンピュータ・ネットワーク攻撃やサイバー作戦がどういうものになっていくのかを予測するため、幾つかの具体例を取り上げ見てみたい。

（１） イランの核開発と米国 NSA「オリンピックゲーム」

ア　「オリンピックゲーム」[23]

イランは、独自に核開発を進めており、米国やイスラエルはそれが核兵器開発に結び付くとして、反対してきた。そこで、イランの核開発の解明、妨害を目的として、米国 NSA が実施したのが「オリンピックゲーム」計画である。

同計画によるサイバー攻撃は、ウラン濃縮用遠心分離機を多数破壊したが、重大な物理的破壊を齎した攻撃としては、米国 NSA にとっても初めてのものであったという。

計画は、ブッシュ政権時代の 2006 年頃開始され、当初はイランのナタンツにあるウラン濃縮による核燃料施設の制御システムの解明にあったようである。同システムは、ドイツのジーメンス社の遠隔監視制御・情報取得システムを基盤としていたが、このシステムは外部のインターネット回線やその他のネットワークと接続されていないスタンドアローンのシステムであった。同システムへのマルウェアの注入方法としては、職員の UBS メモリーにマルウェアを仕込んで、職員が規則を守らずに当該メモリーをシステムに接続した際に感染させたと見られる[24]。この他に、何らかの部品にサプライチ

---

[23] David E. Sanger," Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* 1 June 2012, accessed 9 February 2015, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
--Kim Zetter, "Report: Obama Ordered Stuxnet to Continue After Bug Caused It to Spread Wildly," *WIRED,* 1 June 2012, accessed 9 February 2015, http://www.wired.com/2012/06/obama-ordered-stuxnet-continued/all/

[24] 本来スタンドアローンのシステムは、セキュリティを高めるためにインターネットなど外部のネットワークと接続していないのであるから、同システムに接続した USB メモリーをインターネットと繋がっているコンピュータ端末に接続してはいけないのであるが、往々にして職員はこの禁止事項を守らないものである。そこで、先ず特定職員のインターネットと繋がった端末にマルウェアを注入して支配し、次にこれに接続された USB メモリーにマルウェアを仕込む。そして、この USB メモリーがスタンドアローンのシステムに接続されると、そこで仕込んでおいたマルウェアが与えられた作業をこなし、再度、インターネットと繋がった端末に接続されると、その結果をサイバー作戦の基地に報告する。そして、この手順を反復することにより、スタンドアローンのシステムに対しても相当の支配力を及ぼすことが出来ると指摘されている。ロシアのカスペルスキー研究所は、発見した（NSA 作成と見られる）当該マルウェアに Fanny という名称を付けている。
--Kaspersky Lab. *Equation Group: Questions and Answers*, (February 2015), 13-14, accessed 18 February 2015,

ェーン介入（第２部第２章７の（３）物理的侵入）でマルウェアを注入する方法を併用した可能性もあると考えられる。

何れにしろ、マルウェアを仕込んでから数ヶ月で、(多数の遠心分離機を制御する)コンピュータの制御システムの詳細情報を得ることができたという。

他方、平行して、CIA は闇市場でイランにナタンツ施設向けの欠陥部品や欠陥設計図を売り込んでいたが、これらのサボタージュ（破壊活動）は殆ど効果が無かったという。

そこで、米国はイスラエルとも協力して、遠心分離機を破壊するためのマルウェアを開発して核燃料施設の運用を妨害することとした。同マルウェアは、ナタンツの核燃料施設に特化したもので、遠心分離機の回転速度を混乱させて破壊しようとするものである。

同マルウェアが何時ナタンツの施設に仕込まれたのかは明確ではないが、2008 年又は 2009 年とみられる。当初は、少数の遠心分離機に障害を発生させ、これにより施設の運用者に自分達の技術水準が低いと誤解させ、開発運営を妨害することを狙ったようである。結局は、ブッシュ政権からオバマ政権に代わった後の 2010 年前半、多数の遠心分離機の破壊に移行し、少なくとも、1000 基以上を破壊したとされる。オバマ大統領は本作戦について逐一報告を受け、命令を発していたとされる。

なお、このナタンツのシステムはスタンドアローンであるので、マルウェアは外部に流出しない筈であったが、施設の技術者が施設のシステムに接続したパソコンをインターネットに接続したため、既に 2010 年の夏にはマルウェアが世界中に拡散してしまった。そして、これを分析した民間研究者によって「スタックスネット Stuxnet」と命名されると共に、米 NSA の関与が疑われたのである。

更に、2011 年には、米国ニューヨークタイムズ紙のデイビッド・サンガー記者が米国 NSA の関与について記事を何本か掲載し、更に 2012 年 6 月には本件についての米国の関与の内幕を暴露した本を出版した。（なお、米国 NSA はスタックスネットの他にも、フレイム Flame やドゥクーDuqu というマルウェアを使用したとされる。）

他方、イランは、2011 年に軍にサイバー部隊を創設した。

イ　イランによる反撃（と考えられるサイバー攻撃）[25、26]

---

http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf

--Kim Zetter, “Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet,” *WIRED*, 16 February 2015, accessed 18 February 2015, http://www.wired.com/2015/02/kapersky-discovers-equation-group/

[25] Ellen Nakashima, “U.S. rallied 120 nations in response to 2012 cyberattack on American banks,” *The Washington Post,* 11 April 2014, accessed 22 April 2014, http://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to

2012 年 8 月から 2013 年にかけて、米国の主要銀行に対して、過去最大の DDOS 攻撃が展開された。これは世界の多数の国のデータセンターを踏み台（作戦中継機）として、DDOS（分散型サービス妨害）攻撃を掛けたものである。攻撃対象は、バンクオブアメリカ、シティグループ、ウェルスファーゴその他の米国主要銀行のオンライン取引サイトであり、攻撃を受けるとオンライン取引が利用停止に追い込まれ、多大の業務妨害と対策のための出費を強いるものであった。

この攻撃については、「イズ・アディン・アル・カッサム[27]・サイバー戦士」と名乗るハッカー集団が犯行声明を出し、預言者モハメッドを嘲笑した反イスラムビデオに対する報復であると称したが、攻撃の規模、対象範囲、効率性は、DDOS 攻撃として過去に例を見ないものであり、国家規模の関与が疑われた。イランは関与を否定したものの、米国は、攻撃元はイランのサイバー部隊であり、上記の米国によるサイバー攻撃に対する報復攻撃と解釈した。

攻撃への対応策について、NSA は、防御的サイバー作戦により、DDOS 攻撃を停止させることは可能であると提案したが、採用されなかったという。代わりに、米国は世界１２０カ国以上に呼び掛けて、諸国のデータセンターが、DDOS 攻撃の中継機として使われないように、データセンターのサーバーからマルウェアを除去するよう要請したという。

この対応は、米国としては極めて自制したものであったが、2013 年春にはこの DDOS 攻撃も下火になったと言う。

-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html

--Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times,* 8 January 2013, accessed 9 February 2015, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0

[26] イランは、対米攻撃と平行して、2012 年 8 月、サウジアラビアの石油会社サウジ・アラムコにサイバー攻撃をかけ、同社のコンピュータ端末数万台のデータを全て消去したとされる。これに関して、NSA 内部資料は、2012 年 4 月にイランの石油産業に対して、アラムコ社に対する攻撃と同種の攻撃があったが、イランは他組織の能力と行動からの学習能力があると警戒感を示している。なお、同資料は、2013 年 1 月 NSA、GCHQ、イスラエル ISNU の３機関が（従来の２機関毎のではなく）初めて一同に会し、イランに関するシギント分析ワークショップを行った旨記載している。2012 年 4 月の対イラン攻撃の主はこれら３機関に含まれる可能性が高いと思われる。

--ス資料、NSA、*Iran—Current Topics, Interaction with GCHQ*, 12 April 2013, accessed 12 February 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/1658374/iran-current-topics-interaction-with-gchq.pdf

[27] イズ・アディン・アル・カッサム(Izz ad-Din al-Qassam)は、２０世紀初め、中近東、特にパレスチナで反植民地運動を行ったイスラム教指導者。

米国オバマ政権の対応が抑制されたものであった背景には、米国が最初にサイバー攻撃を仕掛けた負い目もあったのではないかと、考える。

（２） 北朝鮮によるソニー攻撃と米国の対応

ア 「ソニー・ピクチャーズ」攻撃とコメディ映画の上映中止要求

ソニー・ピクチャーズ・エンターテインメント（以下、ソニー映画）は、「インタビュー」というコメディ映画を製作していたが、これは北朝鮮の独裁者・金正恩の暗殺を主題としたものであり、これに対して 2014 年 6 月北朝鮮外務省は、同映画は絶対に容認できないとの声明を発していた。

同映画の上映予定日（12 月 25 日）を 1 ヵ月後に控えた 2014 年 11 月 24 日、ソニー映画のコンピュータ数千台からあらゆるデータが消去され、システム全体の運用を停止せざるを得ない状況となった。更にそれから数日間に亘り、事前にシステムから窃取していたとみられる膨大なデータの中から情報漏洩が開始された。内容は、職員の個人情報や有名俳優に関するゴシップ情報、未公開映画のコピーや台本などであり、これも会社にとっては大きな損害であった。

これらの攻撃に関して、12 月 16 日「平和の守護者」を名乗る者から、コメディ映画「インタビュー」の上映を中止しなければ、大規模テロを含む更なる攻撃を示唆する脅迫がもたらされた。ソニー映画は、多くの映画館チェーンが上映中止を決めたこともあり、映画自体の上映中止を決定した。

イ 米国政府は北朝鮮の犯行と断定

12 月 19 日 FBI は、北朝鮮の犯行と断定する広報資料を発表した[28]。

それによれば、ソニー映画は捜査に於ける偉大なパートナーであり、11 月 24 日攻撃の数時間後には FBI に通報があったため、迅速に捜査が開始され、攻撃元が特定できた。他の政府省庁とも協力して捜査した結果、北朝鮮政府に責任があることを示す十分な情報を得た。その一部を示すと次の通りであるとしている。

① 犯行に使われたマルウェア（データ消去プログラム）の分析により、技術的に北朝鮮による他のマルウェアと関連性があることが判明したこと。

② 攻撃に使用されたインフラが、北朝鮮が敢行した他の攻撃と重複していること、即ち、（隠匿し忘れた）北朝鮮インフラのＩＰアドレスが検出されたこと。

③ 犯行に使われた道具が、北朝鮮による 2013 年韓国の銀行やマスメディアに対する攻撃と類似性があること。

---

[28] FBI National Press Office, *Update on Sony Investigation*, 19 December 2014, accessed 10 February 2015,
http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

同日、オバマ大統領は、記者会見で「彼らは大きな損害を発生させた。そこで我々は対応する。（損害の程度に）均衡した対応をする。時と場所と方法は我々が選ぶ」と述べ[29]、報復を示唆した。

ウ　NSA の貢献

2015 年 1 月、FBI 主催のサイバー・セキュリティ国際会議に於いて、ロジャース NSA 長官は、北朝鮮の犯行であるとする十分な自信があると述べると共に、捜査に於いては、NSA の技術力だけではなく、NSA が提供したデータも貢献している旨を述べている。また、FBI 長官と同様に、ソニー映画による迅速な通報を賞賛した[30]。

NSA 長官の発言により、NSA はその技術力だけではなく、保有するデータにおいても、北朝鮮の犯行断定に貢献していることが分かるが、その具体的内容は如何であろうか。

先ず、XKeyscore が貢献した可能性である。NSA によるシギントデータ収集の中では通信基幹回線等からの収集が主要部分を占めるが、ここには XKeyscore という収集データの一次記憶装置（第２部第３章の２分析ツールで既述）が設置されている。記憶期間は、基本的にメタデータが１ヶ月、コンテンツ・データが３日間である。NSA 長官もソニー映画の迅速な通報を賞賛していることから考えると、XKeyscore に記録されていたデータが分析に貢献した可能性が高いのではないか。（註：但し、この点を指摘した英文文献は見つからなかった。）

次に、NSA による C-CNE（CNE 対策）である。既述（第２部第２章の７CNE）したように NSA 内部資料にも、NSA が北朝鮮による CNE の解明のために北朝鮮のネットワークに侵入していることが記載されている。

ある報道記事によれば[31]、NSA は、北朝鮮のネットワークへの本格的浸透努力を 2010 年に開始したという。北朝鮮と関係する中国のネットワーク（北朝鮮と外部のインターネット世界を繋ぐ唯一の窓）へ浸透したり、北朝鮮がつながりを有するマレーシアでの接点へ浸透したり、或は韓国の協力を得たりして、取組を抜本的に強化した。その結果、

---

[29] The White House, *Remarks by the President in Year-End Press Conference,* 19 December 2014, accessed 10 February 2015, http://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference

[30] Jana Winter, “NSA Played Key Role Linking North Korea to Sony Hack,” *The Intercept,* 9 January 2015, accessed 12 January 2015, https://firstlook.org/theintercept/2015/01/09/nsa-played-key-role-linking-north-korea-sony-h

[31] David E. Sanger and Martin Fackler, “N.S.A. Breached Into North Korean Networks Before Sony Attack, Officials Say,” *The New York Times*, 18 January 2015, accessed 10 February 2015, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

北朝鮮のシギント部隊（偵察総局傘下約 6000 人）のコンピュータ・ネットワークにその動向を監視するマルウェアを注入して一定の監視能力を保有していた。そのため、今回の北朝鮮による攻撃を事前に探知するまでには至らなかったが、事後的な分析により、北朝鮮は 2014 年 9 月にはスピア・フィッシングという手法によってソニー映画のシステム管理者の権限を盗んだこと、それを使って９月中旬から１１月中旬に掛けて、ソニー映画のネットワークを調査して、重要なデータファイルを特定し、また、コンピュータやサーバーへの攻撃方法を計画してきたことが判明したとされる。

この事件から分かるのは、本件の捜査でも FBI の能力だけでは不十分であり、NSA というシギント機関のシステム能力と専門能力による支援が必要であったということである。

エ　北朝鮮に対する「対応」（報復）

ところで、オバマ大統領が記者会見で述べた「均衡した対応」はどうなったのであろうか。その後の米国の対応を見ると、公式な制裁は 2015 年 1 月 2 日北朝鮮の政府職員と軍事企業に対して発動されたが、北朝鮮は既に制裁の対象となっているので象徴的意味しかないと言われる。

他方、2014 年 12 月 20 日前後に北朝鮮のインターネット通信に断続的に障害が発生し、合わせて１０時間程度、通信不能状態に陥ったと報道されている。

オバマ大統領は、ソニー等米国が被った損害と「均衡した対応をする」と述べており、常識的に考えて、この通信不能状態は「対応」の一部であろう。また、北朝鮮の被害は、単に通信不能状態に陥っただけではない可能性もあるのではなかろうか。そうでなければ、到底「均衡した対応」とは言えない。それが、外部世界の常識であろう。

第３部　セカンド・パーティとサード・パーティ

第１章　セカンド・パーティ（英国との特殊な協力関係を中心に）

米国の強大なシギント能力は、NSA 単独で構築したものではなく、UKUSA 協定に基づくセカンド・パーティ諸国との密接なシギント協力の成果でもある。

セカンド・パーティ諸国とは、英国、カナダ、豪州、ニュージーランドの４ヶ国であり、各国で NSA に対応するシギント機関は、それぞれ、英 GCHG 政府通信本部、加 CSE 通信保全局、豪 ASD 豪信号局、ニュージーランド GCSB 政府通信保全局である。これらの諸機関は UKUSA 協定に基づき緊密に協力している。その協力関係は、漏洩された内部文書を見ても、単にインテリジェンスの成果物を交換するというレベルを遥かに超えて、NSA の主導の下に、共同しての収集分析、更にはそのシステムの共用・統合運用など、正に一体となってシギント活動を行っている状況にある。

本章では、そのセカンド・パーティ諸国中、最も強力で且つ NSA との協力関係も長い英国 GCHQ を主として取り上げ、その概要、米国との協力関係の沿革、更に、興味深いシギント活動を見ることとする。また、カナダ CSE による興味深い幾つかの取組を紹介する。これによって、NSA とそのセカンド・パーティ諸国の特殊な協力関係を理解できるのではないかと考える。

１　英 GCHQ 概観と NSA との協力関係

（１）政府通信本部 GCHQ（Government Communications Headquarters）概観

ア　任務

GCHQ の任務は、1994 年のインテリジェンス・サービス法（諜報機関法）第３条[1]に定められており、①シギント、②情報保証、それに③統合技術言語サービスの三つである。

シギントは、GCHQ の本来の業務であり、統合信号局（Composite Signals Organization）が担当している。

情報保証に関しては、GCHQ 内に CESG（通信電子保全グループ）があり、これが国家の情報保証技術当局として、政府の機微な情報保全、公的部門の情報通信システムのセキュリティ維持に加えて、産業界と協力してクリティカル・インフラストラクチャの保護について、政府を支援するとしている[2]。

また、統合技術言語サービスは、政府機関全体のために技術的な言語支援を行う機関

---

[1] UK Intelligence Services Act 1994, Sec. 3.

[2] GCHQ Website,“CESG-the Information Security arm of GCHQ”, accessed 16 February 2015, http://www.gchq.gov.uk/what_we_do/Information_Security/Pages/index.aspx・

であるとされる。シギントの必要上、特殊な言語要員を擁しているということではないかと推定する。

イ　目的

GCHQ の特色は、その目的の広さである。インテリジェンス・サービス法第３条によれば、GCHQ 活動目的は、次の三つに限定されるとされている。即ち、

①　国家安全保障（特に、国防政策、外交政策）上の利益

②　（国外にある者の行動や意図との関連において）英国の経済的福利上の利益

③　重要犯罪の防止と探知についての支援

国家安全保障は、正に米国の諸諜報機関が任務とする対外諜報、防諜、テロ対策などと同一であるが、それに加えて、英国は、対外関係における経済的福利（economic well-being）の追求を堂々とその活動目的に掲げている。また、重要犯罪の防止と探知についての支援も掲げている。後述するが、GCHQ には内務省からも相当額の予算が支出されており、公表はされていないものの GCHQ が治安関係でも相当の活動をしていることが伺われる。即ち、「限定される」(only)としながら、実は、「限定される」目的自体が広汎であり、従って GCHQ の活動範囲も広汎であり得るということである。

なお、活動目的が広汎なのは対外ヒューミント組織である秘密諜報機関（Secret Intelligence Service 旧 MI6）も同様である[3]。

ウ　予算・人員・組織

①　公表資料による予算・人員[4]

当然の事ながら、諜報機関である GCHQ の予算と現在の人員は公表されていない。公表されているのは、諜報機関全体の予算・人員であり、それによれば、諜報機関全体の予算規模は、年間約２０億ポンド（１ポンド 180 円換算で 3600 億円）、人員合計は約１万２千人である。

三つの諜報機関、即ち GCHQ と秘密諜報機関(Secret Intelligence Service: 旧 MI6)、セキュリティ・サービス（Security Service:旧 MI5）を併せて、統合諜報会計（Single Intelligence Account）が設定されており、本会計は首相府が所管している。この他に、

---

[3] 秘密諜報機関の活動目的の規定は、政府通信本部の規定と全く同じである。
-- UK Intelligence Services Act 1994, Sec. 1.（諜報機関法第１条）参照。

[4] UK　Principal Accounting Officer, *Security and Intelligence Agencies,: Financial Statement 2013-14*(19 June 2014), 18, accessed 16 February 2015, https://www.gov.uk/government/publications/security-and-intelligence-agencies-financial-statement-2013-to-2014
--UK, *Intelligence and Security Committee of Parliament: Annual Report 2012-2013*(July 2013), 34, 40, accessed 19 February 2015, http://isc.independent.gov.uk/committee-reports/annual-reports

国家サイバー・セキュリィ計画予算がある。これも会計上は、上記三諜報機関の予算として計上されているが、実際の予算執行は他の省庁も含め政府全体で行われているとされる。それらの予算額と人員は次の通りである。

	2011 年度	2012 年度	2013 年度	2014 年度
統合諜報会計	19.28 億	19.91 億	19.08 億	18.83 億ポンド
サイバー・セキュリティ	0.70 億	0.95 億	1.71 億	1.23 億ポンド
三機関人員合計	12136 人	12328 人	12190 人	12475 人

また、2015 年度は予算、人員とも増加（統合会計予算 3.4%増、人員 370 人増）が予定されている。（なお、GCHQ の過去の平均実員数は、2009 年度 6485 人、2010 年度 6361 人、2011 年度 6132 人である。）

② 内部資料による予算・人員[5]

GCHQ の内部資料自体は報道されていないが、同資料に基づいた報道によると、GCHQ の予算額は、約 10 億ポンド（1800 億円）で統合諜報会計予算の過半を占めている。また、先に述べたとおり、GCHQ の人員は約 6100 人で三諜報機関全体の半分を占めている。

更に、GCHQ 予算には、他省庁分として計上された中から支出されるものがある。その金額は、2010 年度は 1 億 1800 万ポンド、2011 年度は 1 億 5070 万ポンドであり、邦貨 200 億円以上と相当額に上る。供出元は、内務省、国防省、米国 NSA の 3 機関であるが、内務省が最大の供出元であるとされている。この事実、及び GCHQ の活動目的に「重要犯罪の防止と探知についての支援」が明記されていること、更に後述するリエゾン・オフィサーの配置等から考えると、詳細は不明であるが、GCHQ は治安維持目的の活動に相当関与していると推定して間違いないであろう。

③ 組織[6]

本部は、嘗てはロンドン市近辺に分散していたが、チェルトナム市（ロンドン西北西約 150 キロ）郊外に、巨大なドーナツ型の本部を建設し 2004 年に移転した。この地に

---

[5] --Nick Hopkins and Julian Borger, "Exclusive: NSA pays £100m in secret funding for GCHQ," *The Guardian,* 1 August 2013, accessed 16 February 2015, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden
--Nick Hopkins, Julian Borger and Luke Harding, "GCHQ: inside the top secret world of Britain's biggest spy agency," *The Guardian,* 2 August 2013, accessed February 2015, http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden

[6] 主な資料は次の通り。
--UK , GCHQ Website, accessed 17 February 2015, http://www.gchq.gov.uk/Pages/homepage.aspx
-UK Principal Accounting Officer, *Security and Intelligence Agencies,: Financial Statement 2013-14.*

は、シギント担当の統合信号局、情報保証担当の CESG、そして統合技術言語サービスが所在する。また、本部建物の写真を見れば分かるが、それ自体が電波受信施設にもなっている。

この他、英国内の施設としては、スカーボロウ市（ロンドン北方約 350 キロ、北海沿岸の都市）に、第 1 次大戦以来の収集分析基地がある。更に、バッド（ロンドン西方約 350 キロ、コーンウォール地方）には、インターネット基幹回線や衛星通信の傍受施設がある。

英国外の施設としては、キプロス島内の英国領土（デケレア地区）のアイオス・ニコラオスに衛星通信とインターネット基幹回線からの収集施設がある。また、オマーンのセエブにも衛星通信とインターネット基幹回線からの収集施設がある。

GCHQ の担当大臣は外務大臣である。しかし、GCHQ は外務省の外局ではなく、附置機関でもない。外務大臣が直率する組織であり、GCHQ 長官は外務次官と同格(permanent secretary)である。また、先にも見たように、GCHQ 予算は外務省予算の一部ではなく、他の諜報機関と共に首相府の統合諜報会計に位置付けられている。そして、GCHQ 長官は、直接、首相にも報告する。英国は、内閣官制を採りながらも諜報機関の秘密保持と有効機能のために、極めて特徴ある制度を採っていると評価できる。この位置付けは、秘密諜報機関 SIS も同様である(要するに、英国の外務大臣は、外務省と GCHQ と秘密諜報機関という三つの機関を所管している)。

なお、2009 年の GCHQ 内部文書によれば、GCHQ は、数年前までの単なる情報の提供者から、今や、軍とシビリアンの顧客のための真の作戦パートナーとなったとしており、その活動範囲と重要性が拡大していることが伺われる。GCHQ は、秘密諜報機関とセキュリティ・サービス、そして SOCA（重大組織犯罪庁）にもリエゾン・オフィサーを配置している。また、サイバー・セキュリティ戦略を担当する首相府にも人員を派遣している[7]。

エ　シギント活動の法的規制

英国内に於けるシギント活動を規制する法律は、調査権限規制法 Regulation of Investigatory Powers Act 2000 であり、英国内における通信傍受は同法によって規制されている。

但し、同法による規制は、米国の対外諜報監視法と比較すると相当緩いものである。GCHQ の内部資料[8]によれば、米国と比べて「英国の監督体制は軽い」(a light oversight

---

[7] Hopkins, Borger and Harding, "GCHQ: inside the top secret world …," *The Guardian.*

[8] 内部資料は、"UK Operational Legalities"という名称の GCHQ の文書で、NSA 職員に対して英国の法的規制について説明した資料という。資料自体は報道されていないが、同資料に基づいた次の報道がある。
--Ewen MacAskill, et. al., "The legal loopholes that allow GCHQ to spy on the world," *The Guardian,* 21 June 2013, accessed 16 February 2015,

regime）とされている。

具体的には、先ず、同法の規制は英国内での活動に適用され、国外に於ける活動には適用されない（この点は、米国と同様)。次に、英国内で通信を傍受するには、令状を必要とするが、令状は原則として国務大臣（緊急時等には更に下部への委任規定あり）が発出するものであり、米国と異なり裁判所の関与がない。同法によって、調査権限裁判所（Investigatory Powers Tribunal）が設置されているが、同裁判所は寧ろ紛争の事後的対処を任務としており、令状の発布には関与しない。

更に、国務大臣の令状は、国内通信については個別令状を必要とするが、国外通信については概括的令状が可能である。即ち、英国居住者間の国内通信の傍受には同法 8 条 1 項によってその傍受対象を特定する必要がある。他方、国外通信については同法 8 条 4 項によって傍受対象を特定しなくても令状の発出が可能である。そして、通信当事者の一方が英国外にある場合は、国外通信であり、また、英国外に拠点を置くインターネット通信（web-based platform abroad）も国外通信とされる[9]。

国外通信の傍受では、国務大臣が、その目的が国家安全保障、重要犯罪の防止と探知、英国の経済的福利のためとして、傍受対象の概要を示す「証明書」を発出すれば、概括的令状が可能とされる。ここで言う対象の概要は、「外国諸政府の政治的意図」や「外国の軍事能力」「テロ情報」「国際薬物取引情報」など極めて概括的なものであり、これらを足し合わせると、実は GCHQ のインテリジェンスの対象領域を全て網羅していると言う。即ち、国務大臣による「証明書」は実は何の制約にもなっていないという。

このように、英国は米国と比較して、その弱い監督体制と柔軟な法律運用に特色がある。

なお、令状の発布は、GCHQ の担当大臣である外務大臣によってなされる。

（2）GCHQ の沿革と UKUSA 協力関係[10]

ア　GCHQ 発足

GCHQ の前身は、1919 年に設置された政府暗号学校（Government Code and Cypher School）である。第一次世界大戦中には戦争遂行のためコミント（通信情報）が大いに活躍したが、大戦終了後、平時にもコミント組織が必要であるとの提言に基づき、陸海軍のコミント組織を統合して発足した。暗号学校の名称は、政府機関が使用する暗号に関する支援という表向きの任務から命名したもので、同時に任務とされた諸外国の暗号通信の解読研究は秘匿されていた。

---

http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

[9] Owen Bowcott, "Social media mass surveillance is permitted by law, says top UK official," *The Guardian,* 17 June 2014, accessed 27 June 2014, http://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr

[10] UK, GCHQ Website.

発足当初は海軍省に属していたが、1922 年には外務省に移管された。

その後、更にカバーネームとして政府通信本部 GCHQ が使用されたが、これが、1946 年に正式名称として採用されて今に至っている。

イ　米英協力関係の進展

米英両国は、米国の第二次世界大戦参戦前の 1940 年、既に秘密裡にインテリジェンスの協力を開始し、大戦中、両国は密接に協力した。そして大戦後の 1946 年に BRUSA 協定という秘密協定を米英両国で締結して、戦後の協力関係を定めた。その後、米国内のシギント組織改編等を受けて、1952 年これを UKUSA 協定として改定した。この間、UKUSA の協力関係には、1949 年にカナダが、1956 年に豪州とニュージーランドが参加したとされる[11]。

この協力関係では、同じ英語国であり、第二次世界大戦を共に戦ったという事実と共に、地理的補完関係も大きな役割を占めていたのではないかと考える。詰まり、英国は大戦後も嘗ての植民地大国として世界各地に領土を保有し、香港初めシギント収集のための拠点を豊富に提供できたと考えられる。時間の経過と共に、英国の海外領土の多くが英国の手を離れていったが、豪州、ニュージーランド、カナダが加わることにより、全世界を覆うシギントの収集態勢を維持することが可能となったのではなかろうか。

ウ　情報漏洩と情報開示の動き

シギント機関は、諸諜報機関の中でも最も秘匿の度合いが高く、多くの国はその組織構成のみならず存在自体をも秘匿し、また、他国との協力関係の存在自体も秘匿するのが常であった。そして、それは、UKUSA 諸国 5 ヶ国も例外ではなく、何れの国も当初はシギント機関の存在自体を秘匿し、まして UKUSA 協定の協力関係の存在も秘匿していた。

しかし、1972 年米国でウォーターゲート事件が起こり、これとの関連で、諜報機関員による違法な国内活動の存在が暴露され、諜報機関に対する関心が増大した。その様な風潮の中で、シギント機関の存在が次々と表面化して行く。

先ず 1974 年、カナダにおいて、テレビ報道が加シギント機関 CBNRC（当時、現在の CSE）の存在を暴露、これに続いてカナダ政府もその存在を認めた。

次に 1975 年、米国では上院チャーチ委員会の公聴会で、NSA の存在が初めて明らかにされた。

更に 1976 年、英国で「タイム・アウト」誌が GCHQ の存在を暴露した。政府はこれを無視していたものの、1982 年 GCHQ 内のソ連スパイ事件で有罪判決があり、漸

---

11 Richard Norton-Taylor, “Not so secret: deal at the heart of UK-US intelligence,” *The Guardian,* 25 June 2010, accessed 13 February 2015, http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-releasedko

く GCHQ の存在を認めざるを得ない状況となった[12]。

豪州では 1977 年、インテリジェンスに関する調査委員会が、豪シギント機関 DSD（当時、現在 ASD）の存在を明らかにした。

ニュージーランドでは 1980 年、シギント機関 GCSB の存在が初めて内閣と野党党首に報告されたが、1984 年に至り、そのシギント任務と存在が公認された[13]。

こうして相次いで、5 ヶ国のシギント機関の存在が表面化したが、更に 1990 年代になり、ソ連邦が崩壊し米ソ冷戦が終結すると、UKUSA 諸国の協力関係について欧州議会で取り沙汰されるなど、注目を集めるようになった。そして 1999 年豪州の DSD 長官が、初めて UKUSA の名を出して五ヶ国の協力関係を認めた[14]。

その後、情報公開の流れが強まり、遂に 2010 年に米英両国が同時に UKUSA 協定に関する基本文書を開示した。但し、開示文書は 1956 年迄の文書であり、且つ多数の黒塗りがなされている。その為、必ずしも UKUSA の全貌や最近の協力関係が分かる資料とはなっていない。

エ　英国の法律の整備

英国においては、嘗ては、そもそも GCHQ など諜報機関の存在自体を国民や議会に対して秘匿され、その運営はあくまで首相の行政責任に基づいてなされてきたため、関係法律は存在しなかった。それが、情報開示の流れの中で存在が公認され、その結果、法律の制定となった。主要関係法律は次の通り。

1989 年　Security Service Act（セキュリティ・サービスが対象）

1994 年　Intelligence Services Act（GCHQ と秘密諜報機関 SIS が対象）

2000 年　Regulation of Investigatory Powers Act（調査権限規制法）

これらの法律は、調査権限規制法について先に触れたように、諜報諸機関に広汎な権限を付与するものとなっている。

なお、Intelligence Services Act によって、諜報及び国家安全保障委員会（Intelligence and Security Committee）が設置された。本委員会は、諜報諸機関、即ち、セキュリティ・サービス、GCHQ、秘密諜報機関の三機関を監督する委員会で、委員 9 名は議会議員の中から首相が任命する。

---

12 Richard Norton-Taylor, “Surveillance secrecy: the legacy of GCHQ’s years under cover,” *The Guardian,* 21 August 2013, accessed 13 February 2015、
http://www.theguardian.com/uk-news/2013/aug/21/surveillance-secrecy-gchq.

13 NZ GCSB Website, “History of the GCSB,” accessed 17 February 2015,
http://www.gcsb.govt.nz/about-us/history-of-the-gcsb/.

14 Duncan Campbell, “Australia first to admit ‘we’re part of a global surveillance system’,” *Heise Online,* 28 May 1999, accessed 17 February 2015,
http://www.heise.de/tp/artikel/2/2889/1.html

（３）米英特殊関係

ア　米英特殊関係とは何か。

世間に良く「米英特殊関係」と言われるが、筆者は、その根幹は UKUSA 協定に基づくシギント協力関係ではないかと考える。

米英特殊関係と言っても、それが単に英米両国の政治指導部による対外国家戦略であるならば、政権担当者の交代と国際政治情勢の変化によって、容易に変わり得るものであろう。第二次世界大戦後 70 年間に亘って特殊関係が維持されて来たが、このような長期に亘る特殊関係の存続には制度的基礎が不可欠であり、その根幹がシギント協力であったと見られる。このシギント協力によって、米国も利益を得て来たが、英国の得て来た利益は米国を上回る膨大なものである。何しろ、米国のシギント力（NSA だけで 3 万 5 千人の職員と 100 億ドルを超える予算。米国シギント全体の予算・人員は更に多い）を、英国の国家利益のために利用できるのである。

なお、英国のインテリジェンスは、相対的に小さな諸組織でありながら、合同情報委員会を中心に効率的に運用されていると評価されている。日本も（米国は見習う対象としては巨大過ぎるので）英国に学ぶべきであると主張する有識者も多い。しかし、確かにその側面はあるとしても、英国のインテリジェンス力の背景には、UKUSA 協定に基づくシギント協力に依拠する膨大且つ正確・有用なシギント情報があるのを忘れてはならない。英国 GCHQ は、UKUSA 協定によるシギント協力によって、その資源（職員約 6 千人、予算 10 億ポンド）を遥かに超えるインテリジェンス成果物を英国政府に提供しているのである。（最近 GCHQ はその独自の収集能力を飛躍的に強化しているが、それでも）、英国のインテリジェンス成果物の６０％は NSA の報告書或は NSA の収集データに基づく報告であるとされる[15]。

それ故、英国の 2010 年戦略防衛・国家安全保障レヴューを受け、GCHQ は「GCHQ の国際同盟及び協力関係：英国の世界における地位と影響力を維持する助け」(GCHQ's international alliances and partnership: helping to maintain Britain's standing and influence in the world)という名前の文書を作成したという[16]。UKUSA の協力関係が、英国の国益に大きく貢献していることを示す表題である。

イ　NSA にとっての GCHQ の価値

英国にとって極めて価値あるシギント協力関係を維持するため、英国 GCHQ は米国 NSA に対して自らの価値を高めることに熱心である。2010 年 6 月付の GCHQ 内部文書によれば、GCHQ は四つの「利点」（unique selling points）を有するとしている。

---

[15] Hopkins and Borger, "Exclusive: NSA pays £100m ...," *The Guardian.* 本資料では、英国のインテリジェンス成果物の６０％と記述されているが、インテリジェンス全般ではなく、シギント成果物の６０％と解釈する余地もあり、この点は明確でない。

[16] 同上資料。

それは、①地理条件、②協力関係、③英国の法律制度、④熟達した職員である[17]。

この内、注目に値するのは、①の地理条件と③の英国の法律制度である。既述（第 2 部第 2 章の 3 通信基幹回線からの収集）したように、英国領土内では、通信基幹回線からのデータ収集計画として、「インセンサー」「マスキュラー」両計画が運用されており、欧州と北米大陸を結ぶ通信基幹回線からのデータ収集やグーグルやヤフーのデータセンター間通信からのデータ収集をしている[18]。これらのデータ収集は、英国の柔軟な法律制度と軽い監督体制のため、収集対象データについて法律的制約を殆ど受けることなく大量膨大に行われていると見られる。また、キプロス内の英国海外領土等でもデータ収集を行っている。これらの価値が高まっているということである（2011 年現在、GCHQ がインターネット通信網から収集した素データの内３６％が実際に NSA に提供され、且つ、システム的には 100%の提供が可能となっていたとされる[19]）。

また、英国内の英空軍基地メンウィズ・ヒル（ロンドン北方約 350 キロ）では、1950 年代から米国に場所を提供し、NSA の巨大施設が存在する。同施設は、米国外で最大の NSA 施設とも言われ、衛星通信の傍受施設や米国が運用するシギント衛星や画像衛星の管制施設が所在するとされる。

ウ　NSA による GCHQ 支援

先に見たように、英国のインテリジェンス成果物の６０％が NSA 由来であるとされている。このように英米間の情報のギブ・アンド・テイクをみれば、明らかに英国の入超であり、英国が大きな利益を得ている。

通常このような関係では、米国 NSA が英国 GCHQ に対して、資金的な支援をすることは考えられないが、実際には行われている。

内部文書によれば、2009 年度から 2011 年度までの 3 ヵ年で、NSA から GCHQ に合計約 1 億ポンド（約 180 億円）の支払がなされている。即ち、2009 年 2290 万ポンド、2010 年 3990 万ポンド、2011 年度 3470 万ポンドである。2010 年度の内訳は、Mastering the Internet（MTI）プロジェクトに 1720 万ポンド、バッド施設の再開発に 1550 万ポンド、アフガニスタンの NATO 軍支援活動に 400 万ポンドである。また、他にキプロスのシギント施設の費用は NSA が半額を負担しているとされる[20]。

---

[17] Hopkins, Borger and Harding, “GCHQ: inside the top secret world …,” *The Guardian.*

[18] 世界中のインターネット通信回線容量の内１１％が、英国内のインターネット相互接続点（ＩＸ）を経由しているとの見積りもある。
--Richard Esposito, Matthew Cole and Mark Schone, “Sowden docs reveal British spies snooped on YouTube and Facebook,” *NBC News*, 27 January 2014, accessed 28 January 2015,
http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook

[19] Hopkins, Borger and Harding, “GCHQ: inside the top secret world …,” *The Guardian.*

[20] Hopkins and Borger, “Exclusive: NSA pays £100m …,” *The Guardian.*

MTI プロジェクトやバッド施設、更にはキプロスの施設は、既述した「インセンサー」や「マスキュラー」計画、或は後述する「テンポラ」計画に関連している。即ち、インターネット基幹回線等から大量にデータを収集して、それを一次記憶して分析するためのものである。NSA がこれらのプロジェクトに資金を提供しているということは、これらのプロジェクトが NSA にとって資金を提供する程の重要性があるということを示している。

実際、これらの事業はもはや GCHQ の事業というよりも、GCHQ と NSA の共同事業となっていると見られる。正に協力関係の更なる深化が進んでいることを示すものである。

エ　米英特殊関係の揺らぎと例外

①　特殊関係の揺らぎ 1973 年

米国 NSA と英国 GCHQ の関係は、共同収集、共同分析から進んで、更に、組織の一体化と言える程に良好であるが、それでも、波風が立たない訳ではない。

その一例が、「1973 年の大災厄」（the calamity of 1973）であるという。1973 年、時の英国ヒース首相が欧州大陸諸国に接近して米国に対して傲慢であるとして、ニクソン大統領が快く思わず、米英の情報協力を停止させたとされる。そのため、英国の諜報諸機関は驚愕することとなったが、関係が回復して混乱が治まったのは、両首脳が退任した後であったという[21]。

過去にこのような事案があったこともあり、特に GCHQ は NSA に対して自己の価値を高めて NSA との関係を良好に保つのに必死であることが伺われる。

②　例外～～互いの国民を標的とした収集

セカンド・パーティ諸国間では、互いの国民を情報収集の標的にしないという了解があるとされているが、本課題についての NSA の 2005 年 1 月付の内部指示案[22]がスノーデン資料に含まれている。

それによれば、1946 年にシギント協力協定（当初 BRUSA 協定）を締結して以来の米英の協力関係では、締約国の最高の国益に資する場合（when it is in the best interest of each nation）を除いて、互いの国民を情報収集の標的としない事を共通の了解事項としている。そして、その例外事態の具体的運用方法としては、セカンド・パーティ諸

---

[21] Hopkins, Borger and Harding, "GCHQ: inside the top secret world …," *The Guardian.*

[22] "Collection, Processing and Dissemination of Allied Communications,"という文書。文書全体は報道されていないが、一部が次の資料に引用されている。
--James Ball, "US and UK struck secret deal to allow USA to 'unmask' Britons' personal data," *The Guardian,* 20 November 2013, accessed 6 December 2013, http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

国の国民或は通信システムの標的化が、両国の最高の国益に資する場合には、関係国の理解と協力の下に、許されるとしている。

また、この標的化の制限は、セカンド・パーティ諸国の国民が自国外にあるときは適用されない[23]。

ところが、NSA の内部指示案は、これに加えて、セカンド・パーティ諸国にも非開示の米国内部用だけの部分で、次のように述べる。即ち、締約国は、各国の最高の国益に資する場合は、他国の国民に対する一方的なコミント行動を取る権利を留保している。従って、セカンド・パーティ諸国の国民や通信システムを一方的に標的とすることが、許され或は望ましい場合がある。具体的には、計画中の標的情報のセカンド・パーティ国との共有が米国の国益に反する場合、或は、セカンド・パーティ国が協働の提案に同意しなかった場合は、シギント総局長の承認を得て実施することができる旨を定めている。その際は、その収集が極めて重要なことを示すと共に、収集情報はセカンド・パーティのアクセスできない通信網で処理することとしている。

この内部指示案で分かるのは、米英初めセカンド・パーティ諸国のように密接に協力し合う間柄ですら、最高の国益に資するとなれば、了解無しに同盟国を標的とするということである。「インテリジェンスの世界には、永遠の味方も永遠の敵も存在しない。100%の味方も 100%の敵も存在しない。そこにあるのは（唯一の判断基準は）国益だけである。」と言われるが、この内部指示案はその論理を明確に示していると言えよう。

---

[23] James Glanz, "United States Can Spy on Britons Despite Pact, N.S.A. Memo Says," *The New York Times*, 20 November 2013, accessed 27 November 2013, http://www.nytimes.com/2013/11/21/us/united-states-can-spy-on-britons-despite-pact-nsa-memo-says.html?_r=0

２　「テンポラ」計画

（１）「テンポラ」（TEMPORA）計画

ア　「テンポラ」の特徴

「テンポラ」計画とは、英国版 XKeyscore のことである。即ち、通信基幹回線から取得した大量のデータを一次的に記録するバッファ記憶装置であり、また、この一次記憶装置から必要なデータを検索抽出し分析するための分析システムである。

その特色は、NSA の Xkeyscore は世界各地の１５０ヶ所の拠点に設置されているが、それらと比べると、「テンポラ」は圧倒的に容量が大きく、且つ、大量のデータを保有し、高い効果が見込まれていることである。それ故にこそ、GCHQ 側が自慢をし、NSA も資金負担を厭わない計画である。

NSA の内部資料[24]によれば、「テンポラ」は謂わば世界最大の XKeyscore であり、二番目に大きなもの（即ち NSA　最大のもの）と比べても、１０倍以上の大きさであり、1000 台以上のサーバーで構成されているという[25]。そして、毎日 400 億件のコンテンツ情報を処理し分析に供することができる。主要なターゲットは、中東、北アフリカ、欧州である。データ源は、GCHQ「インセンサー」や「マスキュラー」計画による通信基幹回線からの収集、外国衛星通信の傍受など、GCHQ のデータ源である。

イ　「テンポラ」による分析

「テンポラ」は、2012 年 3 月には、試験運用を開始、5 月には GCHQ300 人、NSA250 人の分析官が、その運用、特に標的発見作業を行い、大きな実績が上がった。そこで、2012 年 9 月 19 日から一定の技量水準を持つ全ての NSA 分析官は、自動的にアクセス許可が与えられたという。

「テンポラ」は、他の XKeyscore と同様、コンテンツ・データは３日間保管され、メタデータは３０日間保管される。分析方法としては、先ず大量のメタデータの分析ができる。また、コンテンツ・データについては、所謂「ストロング・セレクター」と呼ばれる電話番号やメールアドレス、IP アドレス等での検索抽出ができる他、所謂「ソ

24　ス資料 NSA、*TEMPORA —"The World's Largest XKEYSCORE" – Is Now Available to Qualified NSA Users,* 19 September 2012, accessed 20 February 2015, http://www.spiegel.de/media/media-34090.pdf
--ス資料 NSA、"GCHQ report on the technical abilities of the powerful spying program TEMPORA, which allows for a "full take"," *Spiegel Online*, 18 June 2014, accessed 20 February 2015, http://www.spiegel.de/media/media-34103.pdf

25 XKeyscore に関する NSA 内部資料では（第２部第３章３の（１）XKeyscore で既述）、世界全体の XKeyscore で 700 台以上のサーバーを使用しているとしている一方、テンポラでは 1000 台以上の「マシーン」を使用していると述べている。テンポラのサーバー数は NSA の XKeyscore サーバー数には入れていないと推定できるが、或は「マシーン」とはサーバーのことでないのか、若干疑問が残る。

フト・セレクター」による内容分析に基づくデータの検索抽出が可能である。即ち、Eメールやチャット・メッセージ、文書などの内容からキーワード検索でそのEメールやチャット・メッセージ、文書を抽出することができる[26]。或は、暗号のかかった通信やVPN通信、TOR通信などを特定して検索抽出することもできる。これにより、対象を特定できない場合でも、この検索抽出システムによって、テロ容疑者や過激な主張の持主など新たな標的を発見して、監視対象に加えることができるなど、効果が高いとされている。

ウ　データ処理の方法[27]

通信基幹回線から収集したデータの処理手順は、先ず、基幹回線から収集したデータをMVR(massive volume reduction)というシステムにより、類型的に情報価値の低いデータを削除するという。即ち、動画等のダウンロードを自動的に検知して削除する。その後に、登録されている「ストロング・セレクター」で自動的に検索を行い標的が検知されれば、これを自動的に抽出する。2012年の時点で登録されている「セレクター」は、GCHQが4万件、NSAが3万1千件である。この検索の後、削除されていない全てのデータは、バッファ記憶装置に記録される。これが、先に述べたように様々な分析対象になるのである。

（2）「テンポラ」を支えるデータ

「テンポラ」という巨大XKeyscoreには、それを支える膨大なデータが存在する。GCHQの主なデータ収集源は、既に第2部第2章で見たように、通信基幹回線からの収集計画である「インセンサー」「マスキュラー」「トランシャント・サリブル」、外国衛星通信の傍受基地である英国本土内バッドの「カーボーイ」やキプロス内アイオス・ニコラオスの「サウンダー」等があるが、この中でも特に「インセンサー」計画の貢献度が高い。これは、英国が大西洋間通信の欧州のハブであり、北米と欧州を結ぶ基幹通信回線の殆どは英国を経由するためである。「インセンサー」計画は、回線経由地の英国コーンウォール地方でデータを収集して、近くのGCHQ施設であるバッドに送信するという。

「インセンサー」計画は、2008年に始動したが、これが本格的に稼働を始めるとGCHQの取得するデータが激増した。2012年8月のGCHQ内部資料によれば、過去

---

[26] 但し、現在、検索抽出対象言語は、英語、アラビア語、中国語である。
--"Incenser, or how NSA and GCHQ are tapping internet cables," *Top Level Telecommunications,* 29 November 2014, updated 5 January 2015, accessed 20 February 2015, http://electrospaces.blogspot.jp/2014/11/incenser-or-how-nsa-and-gchq-are.html

[27] Ewen MacAskill, et. al., "GCHQ taps fibre-optic cables for secret access to the world's communications," *The Guardian,* 21 June 2013, accessed 23 October 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

５年間で、光回線に対するアクセスは７０倍、分析処理されるデータは３０倍になったという[28]。

既に 2010 年には、GCHQ は、NSA 以上にインターネットにアクセスを持ち、NSA 以上にメタデータを収集していると豪語していた[29]。

[28] Hopkins, Borger and Harding, "GCHQ: inside the top secret world …," *The Guardian.*
[29] MacAskill, et. al., "GCHQ taps fibre-optic cables …," *The Guardian.*

３　GCHQ の特色ある活動・作戦類型

GCHQ と NSA は密接に協力しているので、GCHQ によるシギント活動も基本的には NSA と同様であると推定できる。ところが、如何にも英国らしいと感じさせる活動・作戦類型についての内部資料が幾つか報道されているので、これらについて取り上げて紹介したい。但し、これらの活動・作戦類型は、実は（GCHQ に特有ではなく）NSA も既に取り組んでいるものの、単に NSA 関連の内部資料が報道されていないだけの可能性もある。

（１）「ロイヤル・コンシェルジェ」（王立コンシェルジェ・サービス）

ア　概要

「ロイヤル・コンシェルジェ」とは、外国政府高官による世界のホテル予約の探知通報プログラムであり、その通報に基づき次の作戦を立てるものである。内部資料は極く一部しか報道されていないが、解説報道と総合して見ると、次の姿が浮かび上がる[30]。

本プログラムは、世界中の高級ホテル約 350 の予約用メールアドレスと関心ある諸外国政府のＥメール・ドメイン間の通信を監視して、高級ホテルから諸外国政府宛の予約確認メール送信を探知し、これを GCHQ 担当官に通報するものである。対象ホテルの所在地としてはチューリッヒとシンガポールが例示されており、英国内に限らず、世界中の高級ホテルが対象となっている。また、外国政府のドメイン名としては、国防省「@mod.gov. ××」が例示されており、従って、対象ドメインは外務省に限らず、国防省その他標的としている省庁が含まれると見られる。通報は毎日なされるが、通報を受けた担当者、特に情報収集が困難な外国高官（標的）を担当している分析官は、これを基に以降の作戦を考えることができる。こうした作戦としては、内部資料や報道から見ると、次のように幾つもあるようである。

- 宿泊ホテルが、「友好的」な場合は、ホテルの協力を得て、対象者が宿泊する部屋の電話やファックスの傍受、或は、ホテルネットワークに接続したコンピュータの監視を行う[31]。
- 「技術的攻撃(Technical Attack)」～～ホテルの協力を得られない場合、或は傍受設備が無い場合で、情報価値の高い標的に対しては、技術専門チームを派遣して工

---

[30] Laura Poitras, Marcel Rosenbach and Holger Stark, "'Royal Concierge' GCHQ Monitors Diplomats' Hotel Bookings," *Spiegel Online*, 17 November 2013, accessed 20 December 2013, http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html

[31] そもそも、（日本を除く）世界の多くの国では、政府迎賓施設は当然として、民間の高級ホテルにも通信傍受用の各種設備を標準装備させていることが間々あると見られるので、このような場合は、ホテルの協力さえ得られれば、作戦は容易であろう。

作を行う。米国について既述した（第２部第２章７の CNE）物理的侵入(close access)の手法を活用すると見られる。

- 借上車工作[32]
- ヒューミント発動
- その他（その他の方策として、宿泊ホテルの選択に影響を与えられないか、或は訪問そのものを中止させられないか、も検討事項として掲げられている。）

本作戦は、2010 年に試験実施をしたが、成果が上がったため本実施に移されたようである。

イ　教訓

世界中を対象にして政府要人の外国訪問の情報を探索し、探知した場合には、英国外に於いてさえ、通信傍受等の作戦をしようという英国の意欲に注目すべきであろう。

この事実から明白なことは、外国でさえ通信傍受をしようとしている以上、英国外よりも遥かに条件の良い英国内では、必ずホテルや宿泊施設に於いて通信傍受をしているに違いないということである。また、国内では借上車での傍受もしているであろう[33]。そして、この点において、英国が特別な人権軽視、或は非礼な国家なのではなく、近代民主政治の祖国と言われる英国でさえ行われているということは、寧ろこれが世界標準、世界の常識であると理解すべきなのである。外国を訪問する政府高官には心して頂きたいものである。

もう一つ興味深いのは、「ロイヤル・コンシェルジェ」では、シギントとヒューミントの一体化が見られる点である。ヒューミントの発動という選択肢さえ明示されているが、宿泊ホテルや借上車に対する工作においても GCHQ の職員だけでは困難な場合も想定される。「ロイヤル・コンシェルジェ」の国外作戦では、英国の秘密諜報機関（Secret Intelligence Service）との緊密な協力が不可欠であろう[34]。また、英国内で同様な作戦を実施するには、セキュリティ・サービス(Security Service)の協力を得ているのであろう。諜報諸機関の間にこのような協力関係があってこそ、諜報コミュニティが存在すると言い得るのである。

---

[32] 内部資料には「借上車」としか記載がないが、常識的に考えると借上車に対するマイク発信機や録音機の設置が考えられる。往々にして政府高官は、借上車で移動中に重要事項について感慨を漏らすものである。発信電波の受信は、第２部第２章の６特別収集サービス(SCS)の活用も考えられよう。

[33] 政府高官用に借上契約をするようなハイヤー会社は、どの国でも限定されており、通常、政府の息がかかっていると考えて間違いがないであろう。

[34] 秘密諜報機関 SIS との連携について、下記の GCHQ 内部資料には、GCHQ が通常アクセスを有しない通信を傍受する場合には、SIS の協力を得て GCHQ が技術職員を派遣して傍受装置を設置するなどしている旨記載されている。
--ス資料、GCHQ, GCWiki, “TECA Product Centre,” (undated), accessed 23 June 2015, https://firstlook.org/theintercept/document/2015/06/22/teca-product-centre-gchq-wiki/

（2）「スクーキー・ドルフィン」（イルカの鳴き声）

「スクーキー・ドルフィン」とは、GCHQ が開発した社会事象の予測プログラムである。個別の秘密情報を扱うというよりは、所謂ビッグ・データを分析利用するものであるが、シギント機関によるビック・データ分析の取組を示すもので興味深い。本プログラムの背景と内容は、GCHQ の内部資料と解説報道[35]によれば次の通りである。

そもそもこのプログラムの背景には、2011 年の「アラブの春」があるとされる。「アラブの春」は、英国諜報諸機関にとっても、寝耳に水の出来事であって、その発生を予測することができなかった。これに対して、英国の諜報及び国家安全保障委員会は、その 2011 年度報告[36]で、「自然発生的な『アラブの春』の発生自体を予測することが出来なかったのは仕方がないとしても、発生後の展開、地域全体への急速な波及を理解していなかったのは、当該地域に対する理解力の欠如を示すものではないかとの疑念を生じさせる」と諜報諸機関に課題を提起していた。このような批判に対する GCHQ の一つの回答が本プログラムであろう。

2012 年 8 月の内部資料[37]（GCHQ 職員が NSA 職員に説明したプレゼン資料）によると、「スクーキー・ドルフィン」とは、社会事象の傾向を把握分析するために、インターネット上のオンライン活動を広汎にリアルタイムで監視するものである。監視対象としたのは、ユーチューブ（動画）の視聴、ブロッガー（グーグルのブログサービス）への訪問、フェイスブックでリンクされた URL（ウェブサイトなどのアドレス：統一資源位置指定子）である。インターネット回線上からこれらのデータをリアルタイムで検索抽出して、商業ソフトウェウアの SPLUNK を使用して自動的に類型に応じて検索、分析、可視化をする。それによって、ユーチューブのどの動画がどれ位見られているか、どのブログにどれだけのアクセスがあるか、フェイスブックでリンクされる人気のあるウェブサイトなどはどれか、などが図表によって分かり易く表示される。

この分析方法によって、例えば、ロンドン市内でクリケット関連のファン活動が何時何分頃盛り上がったかとか、ナイジェリアの首都ラゴスにおける特定職業の求人状況とかが分かると説明している。また、このビッグ・データ分析に加えて、特定の標的の通

---

[35] Richard Esposito, Matthew Cole and Marc Schone, “Sowden docs reveal British spies snooped on YouTube and Facebook,” *NBC News.*, 27 January 2014, accessed 28 January 2015,
http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook

[36] UK, *Intelligence and Security Committee of Parliament: Annual Report 2011-2012*(July 2013), 4-5, 13-14, accessed 24 February 2015,
http://isc.independent.gov.uk/committee-reports/annual-reports.

[37] ス資料、GCHQ, *Psychology: A New Kind of SIGDEV,* August 2012, accessed 24 February 2015,
http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/snowden_youtube_nbc_document.pdf

信内容をシギントにより検出分析することによって、分析を更に深めることができとしている。更に、GCHQ 内部資料は、2012 年 2 月 14 日のバハレーンに於ける反政府抗議行動に関して、前日の 13 日のインターネット上の活動に見られる特徴的動向を指摘して、その予測可能性を示している[38]。

2012 年 8 月の段階では、本プログラムは未だ試験段階のようであるが、今頃は更に精緻化して、抗議行動や大衆運動の発生規模や時刻に対する予測プログラムとしても完成しているのではないかと考えられる。

[38] 23 日のインターネットのオンライン活動から、24 日の抗議行動を実際に「事前」予測したのかどうかは、報道された内部資料からだけでは、不明である。

４　オンライン秘匿活動（Online Covert Action）

（１）「オンライン秘匿活動」とは何か

「オンライン秘匿活動」とは、GCHQ の定義によれば、「オンライン上の技術を使用して、現実世界或はサイバー世界で何かを起させること」、即ち、単なるサイバー空間からのデータや情報の収集ではなく、現実の効果を生じさせることとされる。これはヒューミントの世界で言えば、積極工作（Active Measures）である。（諜報機関の観点に立てば）サイバー空間の拡大、重要性の増大に伴い、サイバー空間においてもヒューミントの世界と同様に「積極工作」の可能性と必要性が増加しているということである。

GCHQ の本活動については、３件の内部資料（2012 年２件、2010 年１件）[39]が報道されており、また、これらを含む内部資料を元に分析した報道[40]がなされている。そこでこれらを総合的に分析して、GCHQ が現に行い、また、目指している「オンライン秘匿活動」の姿を記述する。

（２）「オンライン秘匿活動」への取組

GCHQ が何時頃から「オンライン秘匿活動」に取り組み始めたのかは、明確でない。2010 年の内部資料から判断して、活動自体は相当以前から行っていたと見られる。即

---

[39] ３件の内部資料（スノーデン資料）は次の通り。
--GCHQ, *SigDev Conference 2012: Cyber Integration "The art of the possible"*, (2012), accessed 24 February 2015, http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive1_nbc_document.pdf
--GCHQ, *Full-Spectrum Cyber Effects*, (2010), accessed 24 February 2015, http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive2_nbc_document.pdf
--GCHQ, *The Art of Deception: Training for a New Generation of Online Covert Operations,* (2012), accessed 24 February 2015, https://firstlook.org/theintercept/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/

[40] 本件に関する報道記事は次の通り。
--Matthew Cole, et. al., "Exclusive: Snowden Docs Show British Spies Used Sex and 'Dirty Tricks'," *NBC News*, accessed 24 February 2015, http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091
--Matthew Cole, et. al., "Exclusive: Snowden Docs Show UK Spies Attacked Anonymous, Hackers," *NBC News,* accessed 24 February 2015, http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361
--Glenn Greenwald, "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations, " *The Intercept*, 25 February 2014, accessed 5 September 2014, https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/

ち、「オンライン秘匿活動」は、2010 年時点で既に GCHQ の全作戦(operations)の５％を占めていたとされる。但し、2012 年の資料によれば、2011 年 9 月に「オンライン秘匿活動」についての資格制度と教育制度（Online Covert Action Accreditation program）を創設して、急速に要員養成を強化しており、更に近年 GCHQ が力を入れているのが伺われる。

GCHQ 内での担当部署は、合同脅威分析・諜報グループ JTRIG(Joint Threat Research and Intelligence Group)である。同グループの中に、人間科学作戦班(Human Science Operations Cell)という名称の中核担当部署がある。

2012 年の計画によれば、2013 年初めまでに 150 人以上の要員を養成し、また、基礎教育を 500 人以上の分析官に施す予定とされている。

なお、英国の諜報関係者によれば、この「オンライン秘匿活動」と呼ぶ積極工作の分野においては、英国は米国より少し先行しているという評価がされている[41]。

（３）「オンライン秘匿活動」の類型と活動の場

ア　「オンライン秘匿活動」の類型

「オンライン秘匿活動」の類型を分類するには幾つかの視点がある。

先ず、技術的な視点からの分類では、情報作戦と技術的妨害の二つに区分される。情報作戦(Information Operations)とは、サイバー空間において一定の情報を送達することにより、対象の行動に影響を与え、或は、対象の行動を妨害するものである。即ち、サイバー空間の（データや情報の遣取りという）本来の機能を利用するものである。これに対して、技術的妨害(Technical disruption)とは、CNA（コンピュータ・ネットワーク攻撃）であり、DOS 攻撃などにより標的のサーバーを通信不全に陥れるなど、サイバー空間での（データや情報の遣取りという）機能を技術的に妨害するものである。

次に、与える効果の観点からの分類では、妨害活動、影響力活動、オンライン・ヒューミントの三つに区分される。

① 妨害活動(Disruption)には、先に述べた技術的妨害と、情報作戦の中で対象の信用を失墜させるなど妨害の効果を生むものが含まれる。

② 影響力活動(Influence)には、情報作戦の内、オンライン世論調査の結果を操作したり、ユーチューブへのアクセス件数を水増しするなどして、世論形成に影響を与えたり、或は偽情報を流布させるなど欺瞞戦術を駆使して関係者の行動に一定の影響を与えようとするものである。

③ オンライン・ヒューミントとは、サイバー空間で展開するヒューミント活動であり、担当官がネット上で何者かに成り済まして、標的人物と交流をするなどして、一定の効果を生み出そうとするものである。具体例としては、GCHQ 担当官がハッカー仲

41 Cole, et. al., "….British Spies Used Sex and 'Dirty Tricks'," *NBC News*.

間を偽装して交流した上で、本物のハッカーの人定を特定して、検挙有罪に導いた例が挙げられている。

更に、「オンライン秘匿活動」は、効果の現れ方によって、即効型と隠密型に分けられる。即効型('Blitz' style approach)は、短期間に最大限可能な限りの妨害や効果の発現を狙うものであり、隠密型(more subtle approach)は、効果が探知され難いものであり、従って作戦の効果が長期に及び易いとしている。

イ　「オンライン秘匿活動」のための基礎知識

「オンライン秘匿活動」のためには、心理学、社会学、人類学、歴史学、経済学、政治学等の人間科学の成果が必要であるとされており、「オンライン秘匿活動」の教育では、サイバー活動における人間的側面、心理学とサイバー心理学、サイバー空間での行動癖、心理徴候、偽装欺瞞の方法、戦略的な影響力の行使方法などを学習し、その成果を活用するとしている。

但し、教育の時間配分から判断すると、偽装と欺瞞の手法に大きな力点が置かれているのが分かる[42]。

ウ　「オンライン秘匿活動」の場

サイバー空間の中で「オンライン秘匿活動」、特に情報作戦に於いて情報の送達の場として示されているものは次の通りであり、広汎な場が想定されている。

- フェイスブック
- ショート・メール・サービス
- ツイッター
- リンクトイン
- ウェブ・ペイジ
- ブログ
- Eメール
- ニュース・メディア
- インスタント・メッセージング／IRC(Internet Relay Chat チャット)
- 電話通話

ここで、ニュース・メディアも情報送達の場として想定されていることが注目される。

次に、「オンライン秘匿活動」について、活動の与える効果の観点からの分類に従い、その内容を見ていくこととする。

（4）妨害活動

---

[42] ス資料　GCHQ, *The Art of Deception: Training for a New Generation of Online Covert Operations.*

妨害活動の手法の全貌[43]は明確ではないが、判明している具体的手法は次の通り。

ア　通信妨害（技術的妨害の一つ）

- 対象の保有する端末、特に携帯電話に対して、大量のテキスト・メッセージを送付したり、或は大量の通話呼出を掛けて、事実上、利用不能にする。

  アフガニスタンでの実施例では、約１０秒毎にテキスト・メッセージを送付したり、継続的に通話呼出を掛けて、タリバンの作戦行動を大いに妨害したという。
- オンライン上での存在を消去する[44]。大変な困惑を惹起することができる。
- ファクスを通信不能にする。

イ　コンピュータを使用不能にする手法（技術的妨害の一つ）

- ウィルスを送付する。Ambassadors Reception というウィルスは、端末中の全メール削除、全ファイル暗号化（による閲読不能化）、スクリーン振動、ログイン拒否などの効果があり、端末が使用できなくなる。各種の分野で幅広く使用され、大変効果的であるとされる。
- DOS（サービス妨害）攻撃を掛ける。

  実施例としては、アノニマス・グループ（ハクティビスト集団の一つ）が使用するチャット・ルーム（複数）に DDOS 攻撃を掛け、８０％の利用者を追い払ったという。

ウ　個人の信用を毀損する手法（情報作戦の一つ）

- ハニー・トラップを仕掛ける。

  インターネットの特定サイトに誘い込む。或は、実際に「友好的な人物」に会える場所に誘い込む[45]。（ポルノサイトに誘い込んだり、物理的に売春地域に誘い込み、これを流布することにより、信用毀損を狙うものと考えられる。）
- ソーシャル・ネットワーク・サービス上の対象の写真の摩り替え
- 特定の者による被害者の一人と称してブログを掲載する。

  幾つかの作戦で成功した。イラン関係でも使用したという。

---

[43] 妨害活動の一覧として、次の手法が記載されているが、個々の手法の内容は明確ではない。Infiltration Operation, Ruse Operation, Set Piece Operation, False Flag Operation, False Rescue Operation, Disruption Operation, Sting Operation。この内、False Flag Operation とは、ウェブ空間に他人に成り済まして記事を掲載して、同人の信用を毀損する手法とされる。GCHQ, *The Art of Deception: Training for a New Generation of Online Covert Operations.*

[44] 具体的には、対象の携帯電話に対する通信を送達不能にすることと解釈できるが、技法の内容は不明である。

[45] このハニー・トラップといい、既述した「ロイヤル・コンシェルジェ」といい、GCHQ はオンライン上の活動と現場の物理的活動の両者を統合して運用する柔軟性を保持していると見られる。

- 対象の同僚、隣人、友人に対して、対象者に関する否定的なメールやメッセージを送付する。

（対象集団の内部通信に浸透して、内部不和を惹き起こすことにも使うようである。）

エ　会社の信用を毀損する手法（情報作戦の一つ）

- ブログその他を使用して、他の会社やマスメディアに秘密の情報を漏洩する。「漏洩情報」としては、現実には公開情報、或は開示しても支障のないシギント情報を使用する。必要な場合は、公衆にも知らせる。
- 否定的な情報を適宜な場に掲載する。

これらによって、対象会社の契約を妨害し、ビジネス関係を破壊する。

記述からも明らかなように、これらの手法の多くは現実に既に使用されているとみられる。なお、妨害活動の手法はこれらに限定されている訳ではない。

オ　対象組織の中に不和の種を蒔いて組織を崩壊させる手法（情報作戦の一つ）

各種の手法を総合的に使用すると見られるが、詳細は不明である。

カ　妨害活動の具体例：　ジンバブエ

GCHQ の内部資料によれば、2011 年 3 月現在 GCHQ は、アフリカのジンバブエの独裁で悪名高い体制（ムガベ大統領）への支持を低下させ、体制変換を目指した活動をしていた[46]。但し、ムガベ大統領は 2013 年に再選（６選）されており、明らかにこのオンライン秘匿活動は成功していない。

（５）影響力活動

影響力活動の具体的手法としては、宣伝、欺瞞、メーセージの大量送付、物語の流布、偽装（成り済まし）、心理学が提示されている[47]。それぞれの中身は必ずしも明確ではないものの、判明している具体的手法は次の通り。

なお、影響力活動にはこの他にも、オンライン世論調査の結果を操作したり、ユーチューブへのアクセス件数を水増しするなどして世論形成に影響を与えたり、多様な手法がある。

ア　他国に「秘密」を信じさせる（偽情報を信じさせる）手法

- 「秘密」情報を、対象国が浸透しているコンピュータに保管して盗ませる。

---

[46] ス資料、”Behavioural Science Support for JTRIG,” *The Intercept,* 2 April 2015, accessed 3 April 2015, https://firstlook.org/theintercept/document/2015/04/02/behavioural/

[47] 英文では、それぞれ Propaganda, Deception, Mass Messaging, Pushing Stories, Alias Development, Psychology と記載されている。GCHQ, *Full-Spectrum Cyber Effects* (2010).

（浸透されているコンピュータの特定などのために）コンピュータ・ネットワーク開拓（CNE）担当者と協同する。また、適切な場合には潜在的に「破滅的な」情報も対象国に提供するとしている（対象国がそれを信用した場合に、対象国に決定的に不利に作用する情報と考えられる）。

- 対象国のシギント機関が監視しているネットワークを経由して「秘密」情報を送付して傍受させる。
  使用する情報は、開示できるものを使用することとされている。
- オンライン上の代理人を使って「秘密」情報を提供する。
  代理人には偽装した者を充てるとしている。

イ　外国ニュース会社を利用して情報を流布させる手法

- 特定のジャーナリストを選定して特定の情報を提供することにより、当該情報を当人と接点のある標的者に流布させる。
  但し、関係筋によれば、この手法はまだ実行に移されていないとの由である[48]。

（6）オンライン・ヒューミント

オンライン・ヒューミントの実例として、次の事例がある。

ア　フォークランド諸島維持のためのオンライン・ヒューミント[49]

フォークランド諸島は、1982 年にその領有を巡り英国がアルゼンチンと戦争をして勝利した土地であるが、アルゼンチンはその領有権を諦めておらず、最近アルゼンチンは中南米諸国を味方につけるなど外交攻勢をかけているという。

そこで、英国 GCHQ は、2009 年以来英国の立場を強化するためのオンライン秘匿活動キト QUITO 作戦を立案した。GCHQ の内部資料[50]によれば、詳細は不明であるものの、2011 年 3 月現在アルゼンチンによるフォークランド奪取阻止のためのオンライン・ヒューミント作戦を実施中であるとされる。

イ　ハッカーの特定と逮捕[51]

2011 年夏からのオンライン・ヒューミントによって、ハッカーの人定を特定して、逮捕・有罪に持ち込んだ事例がある。GCHQ 担当官は、自分自身をハッカーに偽装して、ハッカーが頻繁に訪れるチャット・ルームに参入した。但し、チャットをするだけ

---

48 Cole, et. al., "….British Spies Used Sex and 'Dirty Tricks'," *NBC News*.

49 Andrew Fishman and Glenn Greenwald, "Britain Used Spy Team to Shape Latin American Public Opinion of Falklands," *The Intercept*, 2 April 2015, accessed 3 April 2015, https://firstlook.org/theintercept/2015/04/02/gchq-argentina-falklands/

50 ス資料、"Behavioural Science Support for JTRIG," *The Intercept.*

51 Cole, et. al., "….UK Spies Attacked Anonymous, Hackers," *NBC News.*

では、そこに集うハッカーの人定を特定することはできない。皆、仮名を使っており、またIPアドレス等も分からないからである。

そこで、ハッカー仲間と（DDOS 攻撃を掛けるため）攻撃中継機とする端末の獲得方法等について議論するなどして、信用を得た上で、ハッカーが関心を持つBBCのウェブニュース記事「誰がハクティビストを愛するか？」のリンクを送って紹介。ハッカーがそのリンクをクリックすることにより、ハッカーの使用していたVPN（仮想専用ネットワーク）のIPアドレスを探知して、それを端緒にハッカーを特定することに成功したという。こうして、最終的には、ハッカー４人の人定を特定して、その内英国内に居住する３人が2011年から2012年にかけて逮捕され有罪となった。（なお、１人はスカンジナビア諸国に在住するため、放置。）

但し、裁判所では、彼らの人定が何故判明したのかについての資料は提出されなかったという。

この事例は一例であり、他にもオンライン・ヒューミントは活用されていると見られる。また、この事例から分かるのは、英国ではシギント機関であるGCHQがハッカー捜査にも関与しているということである。英国ではGCHQや秘密諜報機関などインテリジェンス機関の活動目的に「重要犯罪の防止と探知についての支援」が含まれているが、ハッキング行為は重要犯罪とされているのであろう。何れにしても、サイバー犯罪の捜査に、サイバー空間のプロフェッショナルであるシギント機関の支援が得られるのは、捜査機関としては心強いことである[52]。

（７）JTRIGの道具と技術

「オンライン秘匿活動」の担当部署である統合脅威分析・諜報グループJTRIGでは、その活動のため、様々な道具や技術を開発しており、2012年７月現在でのその道具・技術一覧の内部資料[53]が報道[54]されている。

この道具・技術一覧表は全体が興味深いものであるが、その内の「効果(を生じさせる)能力」に分類されている道具・技術一覧は、正に、現実世界やサイバー世界で現実の「効果」を生じさせるという「オンライン秘匿活動」に対応するものである。

52　本作戦は、2011年夏ハクティビストに対して実施された「ウェルス」作戦の一環であり、捜査機関に対するインテリジェンス支援と位置付けられている。「ウェルス」作戦には先に述べたアノニマス・グループに対するDDOS攻撃も含まれている。
-- Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014), 193.

53　ス資料 GCHQ, *JTRIG tools and techniques*　in GCWiki (5 July 2012) , accessed 24 February 2015,
https://firstlook.org/theintercept/document/2014/07/14/jtrig-tools-techniques/

54 Glenn Greenwald, "Hacking Online Polls and Other Ways British Spies Seek to Control the Internet," *The Intercept,* 14 July 2014, accessed 29 July 2014,
https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/

「効果能力」分類には３７の道具・技術が掲載されているが、これらの道具・技術の多くは、当初特定の作戦のために必要とされて開発したもので、その後標準装備とするため改良を加えた（或は改良中の）ものであるとしている。そして掲載した道具・技術は直ちに使用できるか､或は開発中のものでも近日中に使用可能となる予定のものであるとしている。更に、この一覧表に記載が無いからといって、作れないということではないので、作戦に必要であれば、JTRIG 担当者に相談して欲しい、作戦立案当初からJTRIG 担当者を参加させれば、それだけ必要とする道具・技術を開発できる可能性が高まる、と JTRIG 担当者との連携を呼び掛けている。

この３７の道具･技術の内から幾つかを紹介することにより､「オンライン秘匿活動」の内容に対する理解を深める資としたい。

ア　主として妨害活動用

- 「アングリー・パイレイト」～コンピュータ上のアカウントを永久に使用不能とする。
- 「プレデター・フェイス」～ウェブサーバーに対する特定 DOS 攻撃の道具
  「ローリング・サンダー」～ピアツーピア通信を使った DDOS 工撃の道具
- 「スカーレット・エンペラー」～特定電話端末に継続的に掛け続ける DOS 攻撃の道具。
- 「シルバーロード」～過激派のビデオを掲示しているウェブサイトを発見し、その過激ビデオを除去する。
- 「キャノンボール」～特定端末に対してテキスト・メッセージを継続的に送り続ける。

イ　主として影響力活動とオンライン・ヒューミント用

- 「アンダーパス」～オンライン世論調査の結果に変更を加える。
- 「バジャー」～情報作戦を支援するためＥメールを大量送付する。
  「ワーパース」～情報作戦を支援するため SMS メッセージを大量送付する。
- 「ゲートウェイ」～特定のウェブサイトに対するアクセスを人為的に増加させる。
  「スリップストリーム」～特定のウェブサイトのペイジビュー件数を水増しする。
- 「ジェステーター」～ユーチューブ等の動画サイトの特定の動画を増幅させる。
- 「ボム・ベイ」～特定ウェブサイトのヒット件数や順位付けを上げる。
- 「チェンジリング」～如何なるＥメールアドレスをも偽装して、その偽装アドレスを使ってメールを送る。

- 「スカイスクレーパー」～情報作戦のため、動画や音楽を作成してウェブ空間で流布させる道具。
- 「インペリアル・バージ」～対象とする二つの電話を通話接続してしまう。
- 「ディア・ストーカー」～スマートフォンや第二世代携帯電話に対して信号を送付してその現在位置の探知を支援する。

JTRIG は、これらを含め、実に多彩な道具・技術を開発している。この事実は、これらの道具・技術を使用する GCHQ の「オンライン秘匿活動」自体も多彩で広汎に及んでいることを示唆している。

（8）「スポラ作戦」～NSA による「オンライン秘匿活動」の一例

NSA による「オンライン秘匿活動」については、現在迄のところ殆ど報道されていないので、第２部には記載しなかったが、１件だけ内部資料に基づいた報道があるので、ここで紹介する。NSA もオンライン秘匿活動に取り組んでおり、その一端が垣間見えるということである。

これは「スポラ作戦」といい、ソーシャル・メディアを利用した所謂「フラッシュモブ」や自然発生的な抗議運動を、主催者側に気付かれることなく、妨害する作戦である。

2012 年 12 月の NSA 内部資料[55]によれば、近年、ソーシャル・メディアを使って行う「フラッシュモブ」や自然発生的なデモが増加している。そこで、関連するソーシャル・メディアによる通信そのものを妨害するのではなく、通信内容を変化させる、即ち、デモの場所と時刻を変化させて通信することにより、関係者にはデモの場所と時刻について幾つかの異なる情報が通信される。その結果、参加者は各地各時刻に分散して、大きなデモの発生が防止されるというものである。

この作戦の実効性については、実際に小規模デモで試してみたところ、同一の場所と時刻には人が少ししか集まらなかったため、主催者や参加者は、デモの課題に対する人々の関心が低いと誤認して、その後のデモを止めてしまったという。

既に、Facebook、WhatsApp、Skype、Google Hangout、PalTalk については、プログラムが開発済であり、iMessage、Yahoo Messenger、ICQ は（2012 年時点では）開発継続中である。

なお、本作戦は、2011 年 11 月に行われた巨大抗議行動の「ウォール街を占拠せよ」に触発されて始まったようである。「オンライン秘匿活動」も多彩である。

---

[55] “NSA-Skandal: Facebook unterwandert Flashmob-Verabredungen,” *Heise Online*, 1 April 2015, accessed 3 April 2015, http://www.heise.de/newsticker/meldung/NSA-Skandal-Facebook-unterwandert-Flashmob-Verabredungen-2592853.html.

５　GCHQ の国際会議に対する取組

国際会議・交渉は、如何なるものであれ、参加各国の利害の違いが基底にあり、従って、一定程度ポーカー・ゲーム的色彩を有することになる。ポーカーでは、仮に、自分の手札を秘密にしたまま、他の参加者の手札を知ってゲームをすることが出来れば、圧倒的に有利である。そこで、インテリジェンス機関は、重要な国際交渉に際しては、当然相手の手札、手の内を探る活動をすることとなる。これに関して、二つの事例を紹介する。

（１）G20 ロンドン会合（2009 年）での取組

2008 年 9 月のレーマン・ショックを契機に世界的金融危機が発生した。これに対処すべく、同年 11 月に第 1 回 G20 サミットが米国で開催され、引き続いて、2009 年 4 月にロンドンで第 2 回 G20 サミットが開催された。また、同年 9 月には同じくロンドンで G20 の財務相・中央銀行総裁会議も開催された。

このロンドンにおける 2009 年 4 月の G20 サミットと 9 月の G20 財務相・中銀総裁会議において、GCHQ は各国代表団のコンピュータや携帯電話を監視して新しいシギント能力を開拓したと自己評価している。そこで、この取組に関して報道[56]と GCHQ 内部資料[57]を元に記述してみる。

ア　取組方針

４月のサミットを控えた 2009 年 1 月の内部資料によれば、ゴードン英首相（当時）は、サミット開催国として、国際的金融危機対策で進展を図る決意であったという。そこで、GCHQ としては、議長国として好ましい会議成果をもたらすために有益なインテリジェンスを適時に且つ利用し易い形で提供することを、その方針とした。

この方針の特徴は、情報の適時性（速報性）を重視していることで、実際、GCHQ はそのための取組を行った。それを新しい能力開拓と称していると見られる。

なお、この方針は政府高官の了承を受け、実際、インテリジェンスの成果は、関係大臣に提供されたという。

イ　全般的取組

---

[56] Ewen MacAskill, et. at.., “GCHQ intercepted foreign politicians’ communications at G20 summits,” *The Guardian,* 17 June 2013, accessed 18 September 2013, http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

[57] ス資料、GCHQ,　“GCHQ surveillance – the documents,” *The Guardian*, accessed 4 March 2015, http://www.theguardian.com/uk/interactive/2013/jun/16/gchq-surveillance-the-documents.

取組の全貌は不明であるが、幾つかの興味深い取組が報道されている。

○　インターネット・カフェの設置

秘密諜報機関（SIS）等と共に、各国代表団のためにインターネット・カフェを設置して、カフェで送受信されるＥメールを傍受した。加えて、利用者のオンラインでのログイン・パスワードなど必要データも収集して、会議後の情報収集に役立つデータを取得した。

○　携帯電話「ブラックベリー」スマートファンへの浸透

代表団員は、「ブラックベリー」等のスマートフォンを利用する者が多く、これに浸透することにより、良い情報成果を得ることが出来た。即ち、「ブラックベリー」による通信に関しては、ニア・リアルタイムで分析官にデータを提供し、これに基づき、適時に関係大臣に情報成果を報告することが出来たという。

加えて、将来の資料源開拓に役立つ 20 件のメールアドレス等の新規データを入手することが出来たという。

○　Ｅメール・アカウントへの侵入

詳細は不明であるが、関係者のＥメール・アカウントに侵入して、同人宛のメールを本人と同時、或は本人が読む前に入手することが出来たという。この手法は、最近の英国の国際会議では良く使用する手法であるという[58]。

○　会議期間中の電話通話の 24 時間監視

９月の財務相･中銀総裁会議では､各国代表の誰が誰と電話しているかについて、24 時間リアルタイムで監視し､その成果をリアルタイムでグラフ化して GCHQ の作戦センターの巨大スクリーンに表示すると共に、分析官 45 人にも提供。この情報は､英国代表団にも提供されたが､各国代表の活動水準を示す指標として有益な情報であったとの評価を得たという。即ち、会議中、或はその前後にどの国の代表団が活発に活動していたかを、英国代表団に知らせることができたのである。

内部資料では、GCHQ にとって、事後的な分析情報では十分ではなく、このようなリアルタイムでの兆候情報が極めて重要であると評価している。

なお、４月の G20 サミットに関連しても、同様の情報要求があったようであるが、その際は、このシステム開発が間に合わなかった様である[59]。

ウ　個別国への取組

---

[58] この手法のコード名や技術的詳細については､「ガーディアン」紙は報道を控えるとしている。仮に、代表団員がＧメールやヤフーメールの様なクラウド・サービスのＥメールア・カウントを使用していれば、GCHQ がこれらのＥメールを入手するのは容易である。しかし、多くの国の代表団がその様なセキュリティ度の低いメール・サービスを利用しているものか、不明である。

[59] 但し、会議の前には、どの国の代表がどの国の代表と連絡を取り合っていたかは、収集して報告した可能性が高いのではなかろうか。

個別の国を対象とした取組で興味深いものは次の通り。

○　露メドヴェージェフ大統領の電話傍受

４月のサミットでは、ロシアのメドヴェージェフ大統領や随員が、モスクワと秘匿電話で遣取りをしているのを、NSA が傍受解読して情報化したという。これは英国内メンウィズヒルの米国 NSA 施設にいる NSA 分析官によるもので、GCHQ はその情報報告を受領して、活用したということである。

○　南アのコンピュータへの浸透

南アフリカについては、その外務省ネットワークに侵入して、G20 会議への出席者に対する事前ブリーフィング資料を入手していたとされる。

（２）国連気候サミット（2010 年）での取組

2009 年デンマークでの気候サミットに対する米国 NSA による取組については、先に（第２部第 3 章４の（４））見たが、英国 GCHQ も気候問題には取り組んできた。気候問題は 2007 年頃から重要性が増し、GCHQ のインテリジェンスの対象事項となったという。

本件については、2010 年末のメキシコ・カンクンでの気候サミットに対する GCHQ 取組に関する内部資料が報道されている。本内部資料は、カンクン・サミットに派遣された GCHQ 職員の帰国体験報告（パワーポイント）であるが、本資料[60]と関連報道[61]を元に、GCHQ の取組を見てみよう。

ア　気候変動問題に対する GCHQ の取組

内部資料によれば、気候変動問題は、2007 年インドネシア・バリ島における第１３回気候サミットで、インテリジェンスの重要優先対象となったという。その後、2009 年 12 月のコペンハーゲン気候サミットが節目と意識され、これに向けて情報収集を強化した。

報道によれば、2009 年第２四半期には、英国のインターネットの光通信基幹回線から得たデータから情報報告書を 6 件作成し、また、UKUSA 諸国からの情報や衛星通信傍受データからも報告書を作成したという。更に、2009 年には、コンピュータ・ネ

---

60 ス資料　*Supporting HMG's Climate Change Ambitions (…or, "A GCO's tales from Cancun",* (February 2011), accessed 4 March 2015, http://www.documentcloud.org/documents/1350180-20110405-cancun-amp-reqs-redacted-small2.html#document/p1

61 Anton Geist, et. al., "Disguised as Climate Negotiators," *Information*, 1 November 2014, accessed 4 March 2015, http://www.information.dk/514369;
--Anton Geist, et. al., "Snowden documents reveal British climate espionage – Copenhagen climate summit targeted," *Information,* 1 November 2014, accessed 4 March 2015, http://www.information.dk/514368.

ットワーク開拓（CNE）により積極的且つ攻勢的なデータ収集にも取り組み、環境サミットへの参加国代表が発言する前にその発言内容を知っている態勢を構築すべく取り組んできたとされる。

こうして一定のデータ収集態勢が構築できると、次の課題は、それを適時適切な形で、情報を必要とする顧客、即ち、この場合はサミット代表に伝えるかであるが、英国内での会合と異なり、外国での会議にどう対処するかが課題となる。これに対する GCHQ の回答が、GCHQ 職員の国外サミット会場への派遣である。この派遣職員は、政府通信職員（Government Communications Officer：GCO）と呼ばれている。

気候変動問題で政府通信職員が初めて派遣されたのは、2009 年 5 月パリで開催されたエネルギー及び気候に関する主要経済国フォーラムであった。この時は初めてでもあり、課題が残されたという。次に派遣されたのが、2009 年 12 月デンマーク・コペンハーゲンで開催された国連気候サミットである。サミット交渉自体は失敗したが、政府通信職員の派遣は成功であり、成果が上がったとされる。そして、2010 年末メキシコ・カンクン開催の国連気候サミットにも、派遣された。

カンクン・サミットは、一見コペンハーゲン・サミットと比べて重要性が低下していたと見られるが、内部資料では、派遣の理由として、①顧客から派遣要請を受けたこと、②速報を要する関係情報入手の可能性が高かったこと、③新内閣[62]に GCHQ の能力を知らせる良い機会であったことが挙げられている。

イ　2010 年気候サミットへの政府通信職員の任務

メキシコ・カンクンに派遣された政府通信職員の任務は、GCHQ とサミット代表団のリエゾン（謂わばワンストップ・サービスの窓口）として機能し、代表団が他の参加国代表団の立場について正確に把握するための支援をすることである。そのためには、GCHQ の現地代表として本部からの最新の情報を提供すると共に、現地情勢を踏まえた情報要求を本部に対して発出することが必要となる。

一般に、サミット代表団が必要な情報は、各国政府の交渉方針や絶対的な交渉拒否事項、或はどの国がどの国に同調しているかなど多様であるが、この多くはサミット開始以前に既に形成されており、当然、GCHQ は事前にも収集し報告している筈である。

しかし、会議は始まれば状況は流動的となる。そこで、各国代表団が本国と連絡を取り新しい指示を受けているかどうか、受けているとすればその内容は何か、などが情報関心となり、この情報提供には、現地代表団を現地で支援するシギント機関職員が必要となるのである。

ウ　事前準備

政府通信職員の派遣に当たっては、次の様々な準備が必要であったという。

---

[62] 英国では 2010 年 5 月に労働党内閣から保守党内閣への政権交代が行われた。

- 英国代表団の中に適切な肩書きを設定して入ること。
- ロジ対策（通信設備、作業部屋、通行証、各国代表団リスト等の準備）
- 顧客（サミット代表団）との事前顔合せ
- 情報要求の調整
- GCHQ 本部での調整（他チームや秘密諜報機関、情報提供方式その他）

エ　まとめ

所謂、政府通信職員（GCO）の制度は、シギント機関 GCHQ とシギント・ユーザーを繋ぐ有効なインターフェイスである。シギントの専門家が（他の関係者や総合情報担当者を介在させずに）直接シギント・ユーザーの傍にいることによって、適時適切なシギント支援をすることができる。その実現のため、GCHQ も色々工夫をしているということであり、ここまで工夫が進んでいるのである。

なお、同様な枠組は、米国 NSA では 1961 年のキューバ危機でホワイトハウスに NSA 職員を常駐派遣することで実現した（第 1 部第 2 章 6 の（1）で既述）[63]。更に、NSA「60 年史」によれば、1960 年代のベトナム戦争では「シギント支援グループ(SSG)」が設置され、軍司令官に対するシギント情報支援のワンストップ・サービスを提供し、大いに成果が上がったという[64]。この SSG は、現在では、CSG(Cryptologic Support Group 乃至 Cryptologic Services Group)と呼称されているようである[65]。但し、米国 NSA が外国で開催される国際会議の代表団の中に NSA 職員を派遣しているかどうか、その実例に関する内部資料は現時点では報道されていない。常識的に考えれば、米国 NSA も既に実施に移していると考えるのが妥当であろう。

---

[63] US NSA, *NSA 60 Years of Defending Our Nation*, 32, accessed 1 September 2014, https://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf.

[64] US NSA, *NSA 60 Years,* 36.

[65] "The National Security Agency in 2002," *Top Level Telecommunications*, 3 July 2014, accessed 5 March 2015, http://electrospaces.blogspot.jp/2014/07/the-national-security-agency-in-2002.html

６　カナダ CSE の特徴ある活動

（１）通信保全局 CSE 概観

主として CSE のウェブサイト[66]の情報を基に、通信保全局 CSE を概観してみたい。

ア　沿革・予算・人員

第二次世界大戦中、カナダにはシビリアンのシギント組織[67]と軍のシギント組織とがあったが、これら組織が協力して効果的に機能した。そこで、戦後の 1946 年、その人員（分析官約 180 人）を継承して、カナダのシギント機関が秘密裡に発足した。組織の名称は CBNRC であるが、これはカナダの国立調査研究機関である National Research Council（NRC：国立調査審議会）の中の通信部（CB: Communications Branch）として秘匿して設置されたためである。

組織は長年秘匿されてきたが、1974 年にテレビで暴露報道されたことを契機に、その存在が明るみになり、1975 年に通信保全局（Communications Security Establishment: CSE）として組織が改編された。

更に、2001 年の米国９/１１のテロ事件を契機に、同年 12 月にテロ対策法が制定され、これに伴い国防法（National Defence Act）が改正されて、その任務権限が国防法で明確に規定された。同法施行後の１２年間で、CSE の人員は２倍以上に増加したという。

現在の予算人員は公表されていないが、報道[68]によれば、人員は約 2000 人、2013 会計年度の推定予算は４億６千万ドルとされる。

イ　任務・権限

通信保全局 CSE は国防大臣が所管し、その任務は、国防法によれば次の三つである。

①　シギント

②　カナダ政府にとって重要な電子情報及びコンピュータ・ネットワーク保護の支援

③　連邦法執行機関とセキュリティ機関の支援

①のシギント任務に関しては、対外諜報のために国防大臣の承認を得て通信傍受が出来るが、この傍受は外国にある外国機関を標的にするものであって、カナダ人やカナダ

---

66 CSE ウェブサイト、”About Us,” Communications Security Establishment, accessed 9 February 2015, https://www.cse-cst.gc.ca/en/about-apropos.

67　連合国の要請で、ドイツ占領下フランスのビシー政権の通信暗号解読を担当するため、カナダのシビリアンの組織が設置されたと見られる。カナダのフランス語能力が期待されたものであろう。

68 “CSE: What do we know about Canada’s eavesdropping agency?” *CBC News*, 27 January 2015, accessed 26 February 2015, http://www.cbc.ca/news/canada/cse-what-do-we-know-about-canada-s-eavesdropping-agency-1.1400396.

在住者を標的にすることは許されていない[69]。但し、外国標的の収集の過程では、外国標的とカナダ人との間の通信も収集可能であり、このデータの取扱に関してはカナダ人のプライバシーを保護するための手続が定められているとされる。

次に、③の連邦法執行機関やセキュリティ機関の支援に関しては、支援対象は主として、連邦警察、セキュリティ諜報サービス(CSIS)、国境管理庁である。且つ、その支援のための通信傍受やデータ収集は、それら支援対象の諸機関が法律に基づいて与えられた権限を、専門能力を有する CSE が執行するものであり、CSE の独自の権限に基づくものではないとされる。従って、その執行に際しては、令状の取得など諸機関が必要な法的手続きを履行するとしている。これら諸機関に対するシギント情報の提供が、この支援によるものに限定されるとすれば、米国 NSA や英国 GCHQ と比べると、治安面における活動は限定されていると言えよう。

最後に、②の政府にとって重要な電子情報とコンピュータ・ネットワークの保護に関しては、その業務が具体的に列挙されている。それは次の通りであるが、これはカナダに於けるシギント機関とサイバー・セキュリティの関係を理解する一助となると考える。

- 共通政府サービス機構（Shared Services Canada: 政府諸機関に対してコンピュータ・ネットワーク・サービスを提供する政府組織）と協力して、政府ネットワークに対する侵入を探知し、阻止し、損害を修復する。
- シギントの能力と UKUSA 協力からの情報を活用して、サイバー脅威の実態とその探知と防止に関する知見を得る。この知見により、実際の侵入や攻撃の前に防止するため有利な位置を占めている。
- 暗号に関する政府責任部署(the lead agency)として、政府の秘密通信に対して機材や知識を提供する。
- IT セキュリティ技術に関する政府責任部署（the lead technical agency）として、IT セキュリティの基準を定める。
- 政府調達機材に関する IT セキュリティの技術評価を行う。
- IT セキュリティ研修センターを設置して、政府の IT セキュリティ専門家の訓練を行う。
- 官民の最重要コンピュータ・ネットワーク保護に貢献する。

ところで、注目すべきは、この②の任務に関する通信傍受・データ収集は、国防大臣の承認を得れば、その対象は外国人に限定されず、カナダ人及びカナダ国内に及ぶことである[70]。この点においては、CSE の権限は相当に広いと言えるであろう。

ウ　余話

---

[69] National Defense Act, Sec.273.65(1)参照。
[70] National Defense Act, Sec.273.65(3)参照。

カナダのインテリジェンス諸機関を見ると、その際立った特徴は、ヒューミントを主体とする対外諜報機関が存在しないことである。カナダのインテリジェンスとしては、シギント機関である通信保全局 CSE の他に、セキュリティ諜報サービス（Canadian Security Intelligence Service: CSIS）が存在するが、これは、英国セキュリティ・サービス、ドイツ連邦憲法擁護庁、フランス対内安全保障総局などと同様の、セキュリティ・サービス（対内治安諜報機関）であり、対外諜報機関ではない。英国秘密諜報サービス、ドイツ連邦諜報庁、フランス対外安全保障総局、或は米国の CIA の様な対外諜報機関が存在しないのである。

その背景として考えられる事情は、先ず、カナダを取り巻く国際環境が安定的であり、対外諜報機関の必要性を強く感じなくて済んできた事情があると見られる。しかし、それ以上に大きな要因は、UKUSA 諸国との協力関係を持つ通信保全局 CSE の存在によって、カナダ政府による人員予算面での投資額を遥かに超える豊富なシギント情報を得ているからではないかと考える。対外ヒューミントまで手を出さなくても、カナダの情報需要を満足させる十分なシギント情報が入手出来ているということではなかろうか。

カナダの対外諜報機関の不在は、シギントの侮れない価値を示すものであろう。

（2）NSA と CSE の協力関係の概観

NSA と CSE の協力関係については、NSA 渉外部の 2013 年 4 月付内部資料[71]が報道されている。但し、報道からは資料全４頁中の半分以上の機微な部分が削除されており、協力関係の表層しか知ることができない。しかし、それでも有益であるので、その概要を紹介する。

ア　協力の沿革

米加のシギント協力は、第二次世界大戦中の同盟に起源を有するが、正式な協力関係の開始は 1949 年の米加合意（CANUSA　agreement）の締結による。協力関係の基本原則は、何れかの国の国益に反する場合を除き、シギント全分野に於ける協力である。

情報保証分野の正式な協力関係は、1986 年の合意覚書締結に始まる。

イ　CSE の評価

CSE は貴重なセカンド･パーティの協力機関である。協力関係は、北米大陸全体の防衛に関する共通利益に基づいている。協力のため、渉外担当者及び職員（integrees）を交換し、また、共同プロジェクトや共同活動を行っている。更に、サイバー防衛分野でのより緊密な協力についての強い要望がある。カナダは、シギント関連機器の生産能力が限定されているので、情報保証関連の米国製品の大きな購入者である。

ウ　両機関の緊密な協力分野

---

71 ス資料、*NSA Information Paper : NSA Intelligence Relationship with CSE*、*(April 2013)*、accessed 24 March 2015,
http://s3.documentcloud.org/documents/1691676/odni3april2013-canada-v1-0.pdf

- 多様な対外諜報標的に関するコンピュータ・ネットワークへのアクセス及び資源開拓。標的には、テロ対策、中東、北米、欧州、メキシコを含む。
- 情報保証及び重要インフラ防衛
- サイバー能力及びネットワーク・セキュリティ基準の発展

エ　NSA から CSE への提供の一部[72]

両機関は約２０ヶ国の優先対象国に対する収集で協力をしているが、NSA は、技術開発、シギント能力、芸術の域にある収集・処理・分析のためのソフトウェアや資源、情報保証能力を分け与えている。CSE とのインテリジェンス交換は全世界の標的に及んでいる。現在、NSA が資金援助をしている事業はないが、時々、共同プロジェクトにおける研究開発や技術面で NSA が費用負担をしている。

オ　CSE から NSA への提供の一部[73]

CSE は、高度な収集・処理・分析のための資源を提供し、また、NSA の要請に応じて秘匿の収集施設を開設している。CSE は米国では不可能な地域に対して類のないアクセスを NSA と共有している。また、シギント成果物、分析力、技術及びソフトウェアを提供している。CSE は相互利益となる複数の開発プロジェクトに投資している。

（３）カナダ政府のサイバー・セキュリティ対策

ア　初めに

CSE はカナダにおける IT セキュリティの責任部署であり、カナダ政府の通信情報ネットワークのセキュリティ保持を任務の一つとしている。ネットワーク・セキュリティのために CSE が構築運用しているシステムについて、2010 年時点の内部資料[74]及びこれらを含む内部資料に基づく報道[75]がなされている。このシステムは、米国の連邦政府一般官庁の防禦システム Einstein３（第２部第４章１の（３）で既述）と類似のシス

---

[72] NSA 内部文書では、本文に記載した１項目以外に２項目の記載があるが、削除されている。

[73] 上記註同様、NSA 内部文書では、本文に記載した１項目以外に２項目の記載があるが、削除されている。

[74] ス資料、SCE, *Cyber Network Defense R&D Activities,* 2010, accessed 26 February 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/1676540/5iiarc-conference-september-2010-csec-briefing.pdf;
--ス資料、SCE, *Cyber Threat Discovery,* 2010, accessed 26 February 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/1676153/csec-its-dsco-2010-20101026-final.pdf

[75] Amber Hildebrandt, Michael Pereira and Dave Seglins, “CSE monitors millions of Canadian emails to government,” *CBC News,* 25 February 2015, accessed 26 February 2015, accessed 26 February 2015；
--Ryan Gallagher and Glenn Greenwald, “Canadian Spies Collect Domestic Emails in Secret Security Sweep,” *The Intercept*, 25 February 2015, 26 February 2015, https://firstlook.org/theintercept/2015/02/25/canada-cse-pony-express-email-surveillance/

テムのようであるが、より詳しい資料が報道されている。そこで、これらの報道を基に、カナダ政府の政府ネットワーク・セキュリティの取組について見てみたい。

先ず、CSE の公式資料[76]は次のように述べている。即ち、カナダ政府のネットワークは、5 万 7000 台以上のサーバーを使用しインターネット網との接続点は約 9000 に及ぶ。このネットワークに対する脅威は大きく四つの集団、即ちハクティビスト、犯罪者、テロ組織、諸国家からもたらされている。そして、現在 100 以上の国家が恒常的にサイバー作戦を敢行する能力を有すると見積もっている。CSE はシギントの経験と知見により外国からのサイバー脅威の性質と手法をより良く理解しており、そのため、政府ネットワークのセキュリティについては、民間が提供できるものを越えて、より広い防護措置を提供できる。また、UKUSA の協力関係から得たインテリジェンスは、カナダのサイバー・セキュリティを大いに増進している。

イ　ネットワーク・セキュリティの全体

2010 年時点の内部資料によれば、政府ネットワークのセキュリティは、次の三つの手法で行っている。

① CSE による「フォトニック・プリズム」計画
② それぞれのネットワーク管理主体による侵入検知
③ CSE の「コッツ」ハードウェア・プラットフォーム（近々、設置予定）

この内、③は、米国 NSA との緊密な協力の下に展開する積極的な防禦であるとされ、「コッツ」という名称のハードウェアを使用するシステムであるが、その内容は不明である。また、②は通常のスパムメール対策やウィルス対策のセキュリティ措置であろう。そこで、ここでは①の「フォトニック・プリズム」計画について見てみよう。

なお、CSE には、サイバー・セキュリティのため、被害対処チームやマルウェア発見チームなど幾つかの担当部署があるようである。

ウ　「フォトニック・プリズム」計画

CSE は、政府ネットワークに対する侵入を阻止するため、カナダ政府機関が受信或は発信する全てのＥメールを収集分析しているという。そのデータ量は、Ｅメールのコンテンツ・データで、毎日 1～10 テラバイトのデータを収集しており、日または月単位で保管できるという[77]。また、メタデータは、毎日 10～100 ギガバイトを収集しており、月または年単位で保管できるという。このデータ保管により事後的な分析や捜査が可能となる。

---

[76] CSE, *CSE Response to CBC's Questions*, February 2015, accessed 26 February 2015, http://www.documentcloud.org/documents/1676089-cseresponsesto2setsofquestions.html#document/p1

[77] システム全体の能力は、「毎月」400 テラバイトとされているが、全体で 400 テラバイトの記憶容量を持ち、その容量の中で新規データを上書きしているということではないかと考える。

現在、収集しているＥメールの量は、毎日平均４０万件に達しているが、これらのメールにマルウェアが添付されていないか、マルウェア添付容疑メールを発見抽出するシステムが「ポニーエクスプレス」と呼ばれている。この「ポニーエクスプレス」の運用により、毎日、攻撃容疑メール約 400 件を自動検出して、これをセキュリティ担当官に送付し、担当官は分析の上その中の１％、毎日平均４件のマルウェア付きメールを検出して、メール送付先の政府機関に通報しているという。「ポニーエクスプレス」の開発には英国 GCHQ の協力も得たという。

一方、現在は、添付資料に直接マルウェアを仕込む方法よりも、メールに特定 URL へのリンクを貼ってそこを訪問するように仕向け、そこでマルウェアを挿入する手法が増加している。そして、メール添付の URL は極めて多く、容疑 URL の検知抽出のためのプログラム開発に力を入れているという[78]。

また、Ｅメールの他に、政府機関のウェブサイトへの訪問アクセスに関するメタデータも収集保管しているという。

なお、この「フォトニック・プリズム」計画では、そもそもデータを何処から収集しているのか、明確でない。但し、少なくともその一部は、インターネット回線から取得していると報道されている。

エ　2011 年時点の将来構想「カスケード」

2011 年の CSE 内部資料[79]によると、ネットワーク・セキュリティ対策は既述した「フォトニック・プリズム」計画等だけでは十分でないとして、「カスケード」構想を提案していた。これは、2015 年までにシギントと IT セキュリティの両者の目的を統合した巨大センサー・システムを構築しようとするものである。具体的には、インターネット通信でカナダ国内と国外を接続する基幹回線の通り口（gateway）の全て[80]に、通信事業者の協力を得てセンサーを設置して、全ての国際通信をモニターできるようにする。

---

78 文章中に設定したハイパーリンクを利用する手法が多いため、ハイパーリンクとＥメールの相関関係やメール受領者がハイパーリンクをクリックしたか否かなどのデータを総合して、容疑 URL として検出するプログラムを開発しているようである。

79 ス資料、CSE, *CASCADE: Joint Cyber Sensor Architecture*, circa 2011, accessed 24 March 2015,
https://s3.amazonaws.com/s3.documentcloud.org/documents/1690204/cascade-2011.pdf
--ス資料、*CSEC Cyber Threat Capabilities*, circa 2011, accessed 24 March 2015,
https://s3.amazonaws.com/s3.documentcloud.org/documents/1690224/doc-6-cyber-threat-capabilities.pdf

80 現在センサーとデータ収集装置が設置されているのは、通り口（gateway）の一部であると見られるが、その割合は不明である。なお、CSE のシギント・データ収集源としては、この他に外国衛星通信の傍受とマイクロ波通信の傍受が存在することが、内部資料から読み取れる。
--ス資料、CSE, *CASCADE: Joint Cyber Sensor Architecture*.

これにより全ての国際通信のデータ収集が可能となり、収集データは、シギント目的にもITセキュリティ目的にも使えるようにするものである。

この構想の背景にある考え方は、ダイナミックな防衛であり、国内インターネット・ネットワーク全体とシギント能力を活用してネットワーク・セキュリティを確保しようというものである。このため次の諸点を達成目標としている。即ち、

① 侵入・攻撃が標的に到達する前に探知する。シギント、即ちUKUSA諸国と協力したCNE（コンピュータ・ネットワーク開拓）対策（Counter - CNE）により、敵のCNEを解明して侵入・攻撃が何時国内ネットワークに入ってくるかを事前に把握する。

② 仮に標的端末・ネットワークに敵の侵入を許した場合には、攻撃者端末と標的端末間の指令通信やデータ送信を探知する。

③ 侵入・攻撃を、通信途上で消去したり、或は攻撃者端末に対して反撃を加えたりする。

なお、2015年3月CSEは、報道機関からの照会に対して、スノーデン資料は既に過去のものであり可能なアイデアを述べたものに過ぎず、必ずしも現在の実態やプログラムを反映したものではない旨述べている[81]。

何れにしても、ネットワーク・セキュリティへの取組も相当に幅広いものであることが伺われる。

（4）「レヴィテーション」計画：テロリスト発見プロジェクト

ア 初めに

現在、過激派はインターネットを活用してテロ活動を行っている。その一例は2008年のムンバイ・テロ事件で既述（第2部第3章2の（1）XKeyscore）した。これはテロリストがテロの実行に当たってインターネットを情報収集や通信に活用した事例である。しかし、過激派は、更に、インターネットを使って、若者を誘引し過激化させテロ実施マニュアルを拡散させてテロに至らせるという、ローンウルフ型のテロリスト育成もしている。

CSEは、このようなテロの拡散を防止するために、「レヴィテーション」計画というテロリスト発見プロジェクトを実施している。そこで2012年時点での内部資料[82]とこれら内部資料を基にした分析報道[83]から、その姿を見てみたい。

---

[81] "An excerpt of CSE's response to CBC's questions," CBC News, 23 March 2015, accessed 24 March 2015, http://s3.documentcloud.org/documents/1690243/csestatements.pdf

[82] ス情報 CSE, *Levitation and the FFU Hypothesis*, 2012, accessed 29 January 2015, https://s3.amazonaws.com/s3.documentcloud.org/documents/1510163/cse-presentation-on-the-levitation-project.pdf

[83] Ryan Gallagher and Glenn Greenwald, "Canada Casts Global Surveillance Dragnet Over File Downloads," *The Intercept,* 28 January 2015, accessed 29 January 2015,

何れにしろ、テロリストがテロの宣伝普及活動をインターネット空間を利用して行う時代には、テロ対策はインターネット空間でも行う必要が生じてくるということである。

イ　無料ファイル共有サイトの監視と容疑 IP アドレスの取得

過激派は、無料ファイル共有サイト（Free File Upload sites）を利用して、ビデオや文書で過激思想の宣伝を行い、更に、爆弾製造教本などテロ訓練実施のマニュアルを拡散させている。そこで、CSE は、無料ファイル共有サイトを監視することによって、そこから潜在的なテロリストを発見するプロジェクトを開始した。

対象とする無料ファイル共有サイトは世界の 102 のサイトであるが、CSE には「アトミック・バンジョー」というプログラムがあり、これらのサイトへのアクセスについてはメタデータを収集管理しているという。但し、この 102 のサイトのファイル全てに関心がある訳ではなく、その内の過激ビデオや過激文書を掲示する特定場所（URLs 統一資源位置指定子）2200 箇所を監視対象としている。そこで、これらのファイル共有サイトからのデータ・ダウンロードを毎日 1000 万件から 1500 万件を把握分析しており、その結果、月に 350 件程度の「興味深い」ダウンロードを抽出し、その IP アドレスを取得しているという。

ウ　個人の特定とその後

過激ファイルをダウンロードした容疑 IP アドレスを把握すると、これに基づき、この IP アドレスから、フェイスブックのアカウントやグーグルのアカウントへのアクセス、或はクッキー情報等を割り出して、それらからデータを抽出して、ファイルをダウンロードした者の特定に至るという。

この特定のためには、英国 GCHQ が開発した「Mutant Broth」や米国 NSA の「Marina」というデータベースを使用するという。前者では、データをダウンロードした前後併せて１０時間の当該 IP アドレスからのインターネット活動を検索できるという。また、後者はインターネット通信のメタデータのデータベースで１年分が保管されているので、矢張り IP アドレスから様々なオンライン活動の情報が収集できる。これらにより、例えば、アクセスしているフェイスブックのアカウントが判明すれば、そこから当該人物の個人情報が取得できることとなる。

---

https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/
--Amber Hildebrandt, Michael Pereira and Dave Seglins, “CSE taracks millions of downloads daily: Snowden documents,” *CBC News,* 27 January 2015, updated 28 January 2015, accessed 29 January 2015, http://www.cbc.ca/news/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120

このようにして人物を特定した上で、当人のオンライン活動の全体を把握して、テロ実行の可能性が一定の高さと評価されれば、次にはテロ担当に通報して更に調査を深めることとなる。

エ　適用範囲

このプログラムの適用範囲が、世界中のどの地域に及んでいるかは、不明である。報道[84]によれば、欧州、中近東、北アフリカ、北アメリカの幾つかの諸国を対象としているとされる。また、他方、「興味深い」ファイルのダウンロードをした者の所在地として、カナダ、米国、英国、ドイツ、スペイン、ポルトガル、ブラジルが挙げられている。

[84] Gallagher and Greenwald, "Canada Casts Global Surveillance Dragnet Over File Downloads," *The Intercept.*

第２章　サード・パーティ関係、スウェーデン、フランス

サード・パーティは、NSA が個別に協力関係を持っている諸国である。2013 年時点においては、３３ヶ国がサード・パーティに位置付けられているが、その協力関係の内容や親密度はそれぞれの国によって異なっている。

本章では、サード・パーティ関係の一般論を NSA の内部資料で見た後に、サード・パーティ諸国の中からスウェーデンとフランスを取り上げ、次章ではドイツを取り上げて詳しく分析することにより、サード・パーティ関係の全体像に迫ることとする。なお、NSA にとって三ヶ国の特徴を一言で言えば、スウェーデンはサード・パーティの優等生、フランスは普通のサード・パーティ、ドイツは重要特異なサード・パーティと言えよう。

１　サード・パーティ関係とは

サード・パーティの協力関係を一般的に言えば、NSA にとっては、標的にアクセスするための地理的な利点、当該国に特有な地理的分析力・言語的分析力などを入手することができ、他方、サード・パーティ諸国にとっては、米国 NSA の技術力或いは自国では入手できないシギント情報に価値があると見られる。その基本的な考え方については、2009 年 9 月付の NSA の内部文書[1]に記載されているので、これを元に NSA の基本対処方針を見てみたい。

（１）サード・パーティ関係を開始する条件

第三国で米国諜報コミュニティを代表するのは CIA 代表であるので、短期間の特定目的のシギント協力であれば、公式のシギント協力関係を樹立していない国に於いては、CIA 代表を通じた協力で十分であるとしている。それは、公式のシギント協力関係を維持するには相当の資源の投入を必要とするので、CIA を通じた協力で目的が達成されるのであれば、そのままで良いということである。

これに対し、NSA が第三国のシギント機関と直接協力関係を開始するのは、次の二つの場合であるとしている。即ち、

① 両国間のシギント情報交換が量的に増大し、或は質的に複雑化して、直接の協力関係が必要となった場合、或は

② 迅速且つ直接の情報伝達を必要とする兆候・警告情報の交換のために、直接の協力関係が必要となった場合

---

[1] ス資料、NSA, Foreign Affairs Directorate, *What Are We After with Our Third Party Relationship? – And What Do They Want from Us, Generally Speaking?* （15 September 2009）, accessed 4 December 2014, https://firstlook.org/theintercept/document/2014/03/13/third-party-relationships/?Edi

これらの場合には、国家諜報長官の承認を得て、NSA が公式のシギント協力関係を開始するとしている。

NSA にとって現在のサード・パーティの協力関係の多くは数十年に及ぶものであり、その中で相互の信頼関係が強化されて来ている。そして、信頼関係が強固になれば、NSA としてもより進んだ技術を提供できるとしている。

（２）サード・パーティとのギブ＆テイク関係

ア　サード・パーティに求めるもの

①　地理的特性からする重要標的通信へのアクセス

②　地理的分析能力、特殊言語能力

③　兆候・警告情報の収集に関する協力支援

イ　サード・パーティが欲するもの

①　シギント技術（ハードウェア、ソフトウェア、関連技術）

②　地域全体、全世界についてのシギント情報

ウ　協力関係の進展は、あくまで米国の国家諜報要求が、サード・パーティ国の国家諜報要求と交叉する場合に限られる[2]。但し、例外として、危機的状況に於いては、米国が相手国に支援をすることがあるとしている。

（３）渉外態勢

NSA でサード・パーティ関係を管理する担当部署は、渉外部（Foreign Affairs Directorate）であり、本部に、それぞれの国の担当デスク Country Desk と全体を統括する渉外担当官（これには、外国機関との協力関係の戦略担当者 Foreign Partner Strategist も含まれている）がいる。また、それぞれのサード・パーティ国にはシギント渉外担当を配置するのが基本のようである。

---

[2] ここで筆者の解釈を述べると、「米国と相手国の国家諜報要求が交叉する場合」とは、シギント協力がそれぞれの国の国家諜報要求の充足に貢献する場合ということである。即ち、シギントに関する国家諜報要求の充足という面においてギブ・アンド・テイクの関係が成り立つ場合にのみ協力するし、シギント協力関係が進展するということである。

なお、危機的状況に於いては一方的なシギント支援があり得るとしている。これは、危機的状況にある国を支援することに米国の国益が合致する場合は、シギント面だけを見ればギブ・アンド・テイクの関係は成り立たないが、国益全体の立場からシギント支援をすることがあり得るということである。

何れにしろ、ここには、博愛主義もなければ、一方的なインテリジェンスやサービスの提供も存在しない。インテリジェンス活動が、国民からの付託を受けて且つ国民の負担の上に成り立っている以上（そして場合によっては構成員の人命の犠牲の上に成り立っている以上）、これは当然のことであり、世界のインテリジェンス業界の常識を述べたものである。インテリジェンスとは、「教えて下さい」と言って只で貰えるものではないのである。

２　スウェーデン FRA と NSA との協力関係

スウェーデンは注目に値する。一方で、政治的中立を標榜しながら、他方で、英米と密接なシギント協力関係を保持してきたからである。

スウェーデンは政治的中立を標榜してきた。第一次、第二次の二つの世界大戦にも参戦せず中立を維持した。第二次世界大戦後の東西冷戦下において、NATO 北大西洋条約機構にも加盟しなかった。そこで、シギント面でも、スウェーデンは東西両陣営のどちらとも中立関係にあったのではないか、と考えがちであろう。

ところが、実は、秘密裡に UKUSA 諸国と緊密なシギント協力関係を有していたのである。つまり、スウェーデンの政治的中立政策は、それ自体が目的ではなく国益を守るための手段であって、これは、インテリジェンス面での米英との協力を妨げるものではなかったということである。そして、インテリジェンス協力も国益を守るための手段、国益を賭けた闘いであることを示すものであろう。NSA と FRA のシギント協力について、主として NSA の内部資料に基づき見てみたい。

（１）国防無線通信局(Foersvarets Radioanstalt: FRA)概観

主としてその公式ウェブサイト[3]の情報を基に、スウェーデンのシギント機関である国防無線通信局 FRA を概観する。

ア　沿革・予算・人員

スウェーデンは、第一次世界大戦の前からシギントに力を入れてきたと言われる。そして、第二次世界大戦中の 1942 年には、既に国防無線通信局が発足している。二度の大戦で中立を堅持するためにも、インテリジェンスが強く必要とされたものと考えられる。

現在の FRA の予算は、2015 年予算では、8 億 6400 万クローネで、１クローネ 15 円換算では、約 130 億円である[4]。人員は 2009 年時点で 700 人弱とされている[5]。現在では人員は増強されている可能性が高いが、比較的小さな組織である。

なお、FRA と並ぶスウェーデンのインテリジェンス組織に、SAPO（Saekerhetspolisen, Security Police）がある。SAPO は所謂セキュリティ・サービスであり、従来司法省に属する国家警察の一部局であったが、2015 年１月に国家警察

---

[3] FRA の公式ウェブサイト http://www.fra.se/hem.11.html、accessed 9 April 2015.

[4] Sverigs Riksdag, *Statens Budget foer 2015,* accessed 10 April 2015, http://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-dokument/Betankanden/201415Statens-budget-for-2015_H201FiU10/?html=true

[5] "Öppen version av Försvarets radioanstalts årsredovisning 2009" （国防無線通信局年報 2009 年公開版). *FRA.*, accessed 10 April 2015, http://www.fra.se/download/18.6bc8a61512cc555baf580004532/arsredovisning-2009.pdf

から完全に分離され、司法省で国家警察と並立する組織となった。人員は約 1000 人[6]、2015 年予算は 11 億 4200 万クローネ[7]（約 170 億円）である。

イ　組織

国防無線通信局 FRA は、長官、副長官の下に４つの部で構成されている。４部とは、シギント担当、サイバー作戦担当、技術支援担当、管理担当の四つである。

収集手段としては、国内の各地の施設のほか、空軍のシギント機（ガルフストリームⅣ型）や海軍のシギント船（オリオン）を使用している。

この点では、NSA の内部資料[8]でも、FRA は多くの収集施設を持ち、幅広い通信の収集に熟達していると評価されている。

ウ　任務・権限

FRA の任務は、シギントと情報セキュリティの二つである。

シギントでは、外交、安全保障、国防の各政策のために活動し、インテリジェンスの提供先は政府（内閣及び政府諸機関）、国防軍、SAPO、国家警察となっている。現在のシギントに関する法律が 2009 年に施行された際には、SAPO を含む国家警察はシギントの提供先から除外されていたが、不都合であるとして法律が改正され、SAPO と国家警察は 2013 年 1 月からシギントの提供先に含まれるようになった。

情報セキュリティでは、FRA は特定の政府機関や国営企業に情報セキュティのサービスを提供している。また、政府機関に暗号を提供している。

更に、重要インフラの情報ネットワークに対する攻撃を防止するため、所謂「技術的探知及び警告システム」（TDV システム）[9]についての政府からの提案要請を受けて、2011 年、2012 年の２回に亘って報告書を提出した。FRA は本件についてウェブサイトに掲載すると共に、FRA は世界中での IT 脅威の進化を監視するシギント能力を有しており、この任務に適任である旨述べている。

エ　法律制定と監督

従来、FRA は無線通信に関しては、携帯電話やインターネット通信を含め自由に収

---

6 SAPO の公式ウェブサイト　http://www.sakerhetspolisen.se/, accessed 10 April 2015.

7 Sverigs Riksdag, *Statens Budget foer 2015.*

8　ス資料、NSA,　Information Paper, *NSA Intelligence　Relationship with Swede*n, 18 April 2013, accessed 8 April 2015,
https://www.documentcloud.org/documents/894384-nsa-internal-pm-on-fra-and-sweden-relations.html

9 FRA が提案した TDV システムとは、米 NSA やカナダ CSE の例を見ても分かるように、端末や個別ネットワークのセキュリティ対策ではなく、インターネット基幹回線を含めたスウェーデン全体の通信回線網にマルウェア等による IT 攻撃を検知するシステムを構築するものと考えて間違いないであろう。

集できると解されてきたが、有線回線からの収集に関してはこれを認める法律が無かった。そこで、シギントに関する法律が制定され、2009 年から施行されたが、これにより、インターネット基幹回線を含む有線回線からのデータ収集が認められ、通信事業会社にはこれに協力する義務が課された。

この権限を行使するための組織として国防諜報裁判所が設置され、有線回線からのデータ収集は同裁判所の令状を得て行うこととされた。

また、FRA の業務全般の監督のためには国防諜報委員会が設置された。

なお、FRA が収集できる通信は、所謂外国通信であり、通信当事者が全て国内にいる場合には収集を許されず、国境を越える、或は国境外から来るインターネット通信に限定されている。

（2）NSA との協力の沿革

協力関係の沿革や現状について、2013 年 4 月付の NSA 渉外部の内部資料[10]を基に見てみると、次の通り。

ア　協力関係の沿革

FRA は、1954 年以来 UKUSA 諸国と協力関係を保持してきた。

協力関係開始の際は、UKUSA 協定に基づく米 NSA と英 GCHQ の合意により、FRA とのコミント面での協力は GCHQ が担当し、エリント面では NSA が担当とすることとされた。後に、コミント面も含めて技術的な問題については、NSA が担当することとなった。

ところが、それが情勢にそぐわなくなり、NSA、GCHQ、FRA の三者合意によって、2004 年 4 月から、コミント全般についても、FRA は NSA と直接の協力関係を持つこととなった。即ち、NSA は GCHQ と事前調整無しに FRA と協力関係を進めることが可能となったのである。これにより、コミント面で FRA と NSA 間の協力関係が急成長したという。

要するに、米国 NSA としては、スウェーデン FRA との協力関係では、主としてエリント面を中心に置いていたところ、情勢の変化によりコミント面でのスウェーデンとの協力の価値が高まり、コミント面でも FRA との直接の協力関係に乗り出したということと考えられる。

イ　協力関係はトップ・シークレット

スウェーデンは、政治的中立を標榜してきた国であるので、他のサード・パーティ諸

---

10 主な出典資料は次の通り。

--ス資料、NSA,　Information Paper, *NSA Intelligence Relationship with Swede*n.

--ス資料、“2004 – the SE NEUTRAL agreement,” *SVT,* 11 December 2013, accessed 8 April 2015, https://www.documentcloud.org/documents/894388-2004-avtalet-se-neutral.html

国と比べて米国等とのシギント協力は秘匿しておきたい動機が強い。従って、NSA にとってサード･パーティ諸国とのシギント協力関係の存在自体は、通常はシークレットであるが、スウェーデンとの関係は、トップ・シークレットに指定されている。

なお、スウェーデンは、欧州に於けるシギントの多国間協力枠組である SSEUR 欧州シギント首脳会議にも参加している。SSEUR 参加１４ヶ国の中で NATO 非加盟国は、(欧州域外のセカンド・パーティ国オーストラリアとニュージーランドを除くと) スウェーデンだけである。

（３）NSA と FRA の相互関係の基本

NSA は、その内部資料[11]で、FRA を極めて有能で且つ技術的にも革新的な信頼できるサード・パーティであると高く評価している。NSA と FRA の基本的ギブ・アンド・テイク関係は次の通りである。

ア　NSA から FRA への提供

- 技術的支援、収集処理の機器や訓練の提供
  （XKeyscore ソフトウェアの提供も含まれている[12]。）
- FRA からのデータ収集要求を受けて、特定の NSA 収集施設に対して収集任務の付与をしている。
  （これは、セレクターによるデータ要求を受け、要求に応じて収集した素データを提供していると解釈できるが、後述する独 BND との関係にも記載のない事項であり、FRA との協力関係の深さが伺われる。）
- （内容不明の協力）[13]
- 機器購入に於ける便宜供与（NSA が米国企業から購入しているシギント関連機器について、FRA に対してその輸出を許可し購入を支援しているものと見られる。）
- 多国間協力枠組への参加組織であること（NATO 構成員でないにも拘わらず、上記 SSEUR のメンバーになっていることを指すものと考えられる。）

イ　FRA から NSA への提供

- ロシア、バルト地方、中東、テロ対策に於ける類のないインテリジェンス
  （地理的特性からの分析能力を含めてのものと考える。）
- 傑出し且つ類のないエリント信号収集[14]

11　ス資料、NSA,　Information Paper, *NSA Intelligence Relationship with Swede*n.

12　ス資料、“X-Keyscore slide with Swedish example,” *SVT,* 11 December 2013, accessed 8 April 2015,
https://www.documentcloud.org/documents/894389-xkeyscore-slide-with-swedish-example.html

13 この部分は、内部資料を報道した SVT によって削除されている。

- 特別な収集イニシアチブへのアクセス
  （インターネット基幹回線から収集したデータの提供を指すものと見られる。）
- 暗号解読面での協力

（4）協力関係での具体的課題

2013 年 4 月には、NSA と FRA の戦略計画協議が開かれたと見られるが、その準備のための NSA 内部資料[15]によれば、両組織の協力関係に於ける最近の課題としては次のようなものがあった。

なお、FRA はこの戦略計画協議のため毎年、FRA 長官を初めとする幹部が訪米しているようである。

ア　インターネット基幹回線からのデータ収集

2011 年以来、FRA はスウェーデン国内でインターネット基幹回線からデータを収集してこれを NSA に提供している。NSA は、これをロシアの指導部、国内政治、エネルギー問題等の優先度の高い課題について類のないデータ収集の場を提供していると評価している。そして、2013 会計年度（2012 年 10 月から）では同データ源からの情報報告が 123 件に及んでいる。FRA はデータを収集する通信事業者を拡大する予定であり、地理的にロシアを越えた遠方の標的についてもデータ収集源として期待できるとしている。

インターネットの基幹回線が、ストックホルムから海底ケーブルでバルト海を渡ってロシアに向け敷設されており、この回線からデータを収集しているものと見られる。

なお、FRA は、本件に関する取材に対して、FRA は他国機関に基幹通信回線への直接のアクセスを認めたことはなく、また、他国機関に FRA のデータへの直接のアクセスを認めたこともない。他国機関に適用するデータは、FRA が収集したものの中から FRA 選択した一定のものであると述べているという[16]。

イ　テロ対策

欧州に於いてテロ対策で協力している。FRA は、ドイツ国内にある NSA の欧州大

---

14 現在までに報道された NSA 内部資料にはエリント関係のものが殆ど見られないが、ここに記載がある事実が、エリント関係でのスウェーデンの貢献の大きさ、重要性を示していると考えられる。なお、1952 年にはスウェーデン空軍のエリント信号収集機が、ソ連軍によって撃墜されている。

15 ス資料、NSA, *Visit Precis: SWEDUSA 2013 Strategic Planning Conference (SPC)*, circa April 2013, accessed 8 April 2015, https://www.documentcloud.org/documents/894387-se-xkeyscore-ingvar-akesson-dirnsa-meeting-2013.html

16 Gunnar Rensfeldt, "NSA 'asking for' specific exchanges from FRA – Secret treaty since 1954," *SVT,* 8 December 2013, accessed 8 April 2015, http://www.svt.se/ug/nsafra4

陸最大の分析センター・欧州シギント・センター（ECC：後述）に、数回に亘り分析官を派遣して協議を行い、テロ対策でのスウェーデン語支援を行っている。2013 年 1 月には、ストックホルムに NSA のテロ対策部門の分析官を常駐させることを始めた。

また、2013 年 1 月には、SAPO（Security Police スウェーデンのセキュリティ・サービス）に対し FRA からのシギント提供が可能となった。これは、2009 年施行のシギント法のため不可能となっていた[17]ものが、4 年間振りに可能となったもので、NSA はこれをテロ対策上評価している。

ウ　サイバー防衛

NSA の NTOC、即ち NSA/CSS 脅威作戦センターは、サイバー防衛に関して FRA と真剣に協力する用意があり、2013 年 4 月の戦略計画協議の際にそのための了解覚書を署名する予定である。

FRA は、サイバー防衛に関する所管庁となるべく運営をしており、近くスウェーデン政府の承認を得られることを期待している、と NSA は評価している。

なお、2012 年 11 月にスウェーデンのイスラエル大使館が関係するコンピュータ・システムへの侵入事件[18]があった。これについては、2013 年 2 月に FRA から NTOC に照会があり、NTOC でも分析をしたが、結論は FRA と同じであったとされる。この案件を見て分かるのは、過去の個別ハッキング事案の調査についても、FRA は NSA と協力できる関係を構築しているという事実である。

エ　「ウィンターライト」作戦～コンピュータ･ネットワーク開拓（CNE）での協力

第 2 部第 2 章 7 の CNE で述べたところであるが、NSA には TAO グループという謂わばハッキングの専門部隊があり、コンピュータ・ネットワーク開拓 CNE に従事しているが、そのための有力な手法が「クオンタム」計画である。

スウェーデン FRA は、この「クオンタム」計画への参加協力も始めている。当面は、スウェーデン FRA 参加による「クオンタム」計画が機能するかどうかの実証試験を、FRA と GCHQ の両者で行ったが、機能することが立証されたとしている[19]。そこで、

---

17 但し、この 4 年間 FRA から SAPO へのシギント提供が完全に遮断されていた訳ではなく、一定の提供ルートは非公式に保持されていたと見られる。
--Julian Borger, “GCHQ and European spy agencies worked together on mass surveillance,” *The Guardian*, 1 November 2013, accessed 6 November 2013, http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

18 これは、イスラエル大使館によるシステム侵入事件か、イスラエル大使館のシステムに対する侵入事件かの何れかであるが、それは不明である。

19 報道された内部資料を分析すると、この実証試験の状態は次のようなものであったと推定できる。即ち、先ず、スウェーデン国内のインターネット回線に設置した装置でインターネット通信をコピーして、近辺に設置してある「ターモイル」システムに取り込み、「ターモイル」が

2013 年夏までには、FRA と NSA の両者による実施に移行したいと考えているようである。

これを見ても分かるのは、FRA と NSA の協力関係は、共同してハッキング行うところまで進展しているということである。

標的通信（標的端末から特定ウェブサイトへの接続を要求する通信）と認識すると、これを GCHQ にある「タービン」システムに向け送信する①。次に「タービン」システムは標的通信の発信元、即ち標的端末に対して、特定ウェブサイトの偽装サイト（「フォックスアシッド」サーバー）に呼び込むための信号を送信する②。標的端末がこの信号を迅速に受信して偽装サイトへの接続・誘い込みに成功すると③、マルウェアを感染させることができるというものである。実証試験では、②１００件に対し③５件が成功したとしている。第２部第２章７CNE（１）遠隔侵入・ア「クオンタム」計画と読み比べていただきたい。

３　フランス DGSE と NSA との関係

フランスは、米国にとって普通のサード・パーティと見られる。「普通」という意味は、米国は協力もすれば、インテリジェンスの標的ともし、他方、米国自らもインテリジェンスの標的とされているということである。つまり、シギント部門でも、国益が一致する範囲では協力し、一致しない範囲では互いに競い争う関係である。

その両者の関係を、フランスのシギント機関 DGSE を概観した後に、米国（英国を含む）とフランスの協力面、米国がフランスを標的としている面、フランスが米国を標的としている面の三つの側面から見てみたい。但し、残念ながら、フランスについては、報道されている内部資料や報道自体が少ないので、断片的にしか見られない。しかし、断片からでも概ねの姿は知ることができよう。

（１）対外安全保障総局（la Direction générale de la sécurité extérieure : DGSE）概観

主として、DGSE の公式ウェブサイト（英語版）[20]の情報を基に、対外安全保障総局 DGSE を概観してみたい。

ア　沿革・予算・人員

フランスの対外安全保障総局の起源は、第二次世界大戦中の 1940 年、ドゴール将軍が設立した「自由フランス」諜報組織に遡る。同諜報組織は、1942 年に BCRA(諜報及び作戦中央局)に改組されたが、大戦中はフランス国内の対独抵抗運動の支援調整に当たった。

戦後の 1945 年諜報組織は SDECE（外国資料・防諜総局）に発展したが、1982 年に再度改組されて現在の DGSE となった。

仏紙ル・モンド[21]によれば、現在の人員は 4991 人（内軍人は 28%）である。予算は正規予算が約 6 億ユーロであるが、他に首相府が管理する機密費から特別資金という形で約 4000 万ユーロが支出されている。

イ　組織・任務・権限

DGSE は、対外諜報機関であるが、その情報源として、公式ウェブサイトにヒューミント、シギント、イミント（衛星画像）、オシントを挙げており、総合諜報機関であ

---

[20] DGSE の公式ウェブサイト http://www.defense.gouv.fr/english/dgse、accessed 13 April 2015.

[21] Jacques Follorou and Johannes Franck, “Révélations sur le Big Brother français,” *Le Monde,* 4 July 2013, updated 7 July 2013, accessed 13 April 2015, http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html. ル・モンド紙は数値の出典は示していないが、他の過去の数値と対比しても、実態と大きく外れることはないと考える。

る。

組織は、長官の下に５つの局がある。管理局、戦略局、情報局、作戦局、技術局であり、シギントは技術局が担当している[22]。

DGSE は国防相の指揮下にあるが、2009 年大統領令によれば、インテリジェンスの方針の決定権は国家元首（大統領）が持っている。

（２）DGSE のシギント力

ア　フランス・テレコムとの特殊関係

DGSE は、米英などと比べれば人員・予算共に小さな組織であり、特にシギント面では弱体と見られる。その DGSE の力となっているのが旧国営企業のフランス･テレコムとされる。

英 GCHQ の 2010 年時点の内部資料[23]では、DGSE は某フランス通信事業者と長期に亘って協力関係を持っているとのみ記載され、会社名までは記載されていない。

報道[24]によれば、その某通信事業者とは、フランス･テレコムであり、同社は DGSE に対して全面的に協力しているとされる。フランス・テレコムは世界的な民間大企業であるが、そもそもその起源は、フランス政府の郵政電信電話省の中の電信電話総局であった。それが、1988 年分離されて国営のフランス・テレコム社となり、更に 1996 年に株式会社化された。政府の持株比率は、当初１００％であったが、徐々に株を放出して 2004 年には持株比率が５０％以下（現在は２７％）となり、完全民営化がなされたものである。

そのフランス・テレコムと DGSE の密接な関係は、実は民営化前の国家組織であった 1981 年以来のものであり、アンリ・セレスという技術者が中心になって構築したものとされる。つまり、法律に基づく契約的な関係というよりは、人的関係に基づく事実上の協力関係とされる。それが民営化後の現在でも継続しているのである。この協力関

---

22 小谷賢（編）『世界のインテリジェンス』（PHP、2007 年）、211 頁。

23 Jacques Follorou , “Les services secrets britanniques ont accès aux données des clients français d'Orange,” *Le Monde*, 20 March 2014, updated 26 March 2014, accessed 13 April 2015,
http://www.lemonde.fr/international/article/2014/03/20/les-services-secrets-britanniques-ont-acces-aux-donnees-des-clients-francais-d-orange_4386266_3210.html.

24 上記の他、次の記事が出典資料である。

-- Jacques Follorou , “Espionnage：comment Orange et les services secrets coopèrent,” *Le Monde,* 20 March 2014, updated 13 May 2014, accessed 13 April 2015,
http://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html.

-- Jacques Follorou , “Les X-Télécoms, maîtres d’œuvre du renseignement,” *Le Monde,* 20 March 2014, updated 26 March 2014, accessed 13 April 2015,
http://www.lemonde.fr/international/article/2014/03/20/les-x-telecoms-maitres-d-uvre-du-renseignement_4386654_3210.html.

係では、DGSE はフランス・テレコムの通信ネットワークとデータフローに自由且つ完全なアクセスを与えられているとされる。また、DGSE がフランス･テレコムから入手したデータは、独り DGSE だけではなく、フランスの諜報コミュニティの各組織が利用できるものであるという。更に、フランス･テレコムはデータ収集で協力しているだけでなく、暗号解読などの IT 技術でも DGSE に協力しているという。技術的支援を含め IT 企業自体の協力が得られるのであれば、確かにシギント機関としてはそれ程人員が多くなくても有効に機能できるであろう[25]。

イ　メタデータ・データベース

報道[26]によれば、2013 年 4 月に出された国民議会のインテリジェンスの報告書は、2008 年以来、特に DGSE のシギントについては全諜報コミュニティのための保持能力（pooling capabilities）に進展があったと評価している。そして、同委員会は、更に、その保持能力の向上と他の諜報機関によるアクセス向上を求めている。

その諜報コミュニティ全体のために DGSE が構築しているものに、メタデータのデータベースがある。メタデータは、フランス･テレコムの全面協力を得て収集していると見られるが、電話、E メール、ショート・メッセージ・サービス（SMS）、ファックス、その他のインターネット活動である。

このメタデータのデータベースは、DGSE の他、６つの諜報機関が利用可能であるとされている。６つの諜報機関とは、DGSI（対内安全保障総局：内務省傘下の所謂セキュリティ･サービス）、DRM（軍諜報局）、DPSD(軍保全局)、DNRED(国家関税諜報・調査局)、Tracfin（資金洗浄対策課）、パリ警視庁諜報サービスである。

なお、DGSE のシギント担当の技術局長は、DGSE は欧州のシギント機関では、英国の次に大きいデータ・センターを持っていると公開の場で豪語している。その DGSE のデータ･センターは本部地下の３フロアを占めており、その発生する熱量で DGSE 本部の暖房は不要である程であるとされる。

（３）米国 NSA（英 GCHQ を含む）との協力関係

ア　協力関係の進展

両者の協力関係についても断片的な報道資料しか得られていないが、それによれば[27]、

---

[25] Follorou , “Les X-Télécoms, maîtres d’œuvre du renseignement,” *Le Monde.* 本記事によれば、スウェーデンではエリクソン社、オランダではフィリップス社がシギント当局に協力しており、ネットワーク通信に詳しい企業の協力がなければ、普通のシギント機関が一流の技術力を持つのは難しいとしている。

[26] Follorou and Franck, “Révélations sur le Big Brother français,” *Le Monde.*

[27] 主として次の報道による。

--Follorou , “Les services secrets britanniques ont accès aux données des clients français d'Orange,” *Le Monde.*

米国 NSA とフランス DGSE の協力関係は、2006 年以降進展したという。

NSA との協力関係の進展では、英国の GCHQ が同じ欧州連合の国として積極的に参画し、或は仲介の労を取ったようである。GCHQ は、この頃、フランスのみならず、独、西、伊、蘭、スウェーデンに対しても、各国機関によるインターネット回線からのデータ収集について実情調査を行うと共に、当該分野での協力関係の構築・強化に向けて働掛けを行っている。

フランスとの関係では、2009 年にはインターネット回線からのデータ収集での協力について、DGSE と GCHQ 担当者が数回に亘り協議会合を持っている。また、協議の過程では、フランス・テレコム社の技術者までもが直接 GCHQ 担当官と協議しており、フランスのシギントにおけるフランス・テレコム社への依存との密接な関係が現れている。

イ　「Lustre」（シャンデリア）計画

ル・モンド紙が仏諜報コミュニティ高官から匿名で取材したとして報道[28]したところによれば、協力関係の進展が「Lustre」計画という米仏共同事業に結実したようである。

即ち、同計画は、DGSE と NSA が 2011 年末から 2012 年初にかけて締結した協力合意であり、仏 DGSE は、DGSE が収集しているインターネットのデータを提供し、他方、米 NSA はフランスがインテリジェンス網を持っていない地域の情報を提供する合意となっている。

アフリカやアフガニスタンと欧州を結ぶ海底ケーブルは、フランスではマルセイユとブルターニュ地方のパンマールで上陸している。DGSE はフランス・テレコムの全面的な協力を得てここからデータを収集しているとみられるが、そのデータを DGSE が NSA に提供するものである。提供データは DGSE 側で選別はしておらず、フランス国民と海外との通信も含まれるという。但し、提供データはメタデータに限定されるのか、コンテンツデータも含まれるのか、については不明である。

（4）諜報対象としてのフランス

このようなフランスとのインテリジェンス協力は、当然の事ながら、フランスを標的とするインテリジェンス活動を何ら妨げるものではない。フランスは、2013 年現在の NSA 内部資料では、諜報対象優先順位上、ドイツと並ぶ中位に位置付けられていると

--Borger, "GCHQ and European spy agencies worked together on mass surveillance," *The Guardian.*

[28] Jacques Follorou, "Surveillance : la DGSE a transmis des données à la NSA américaine," *Le Monde*, 30 October 2013, accessed 13 April 2015, http://www.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html

される[29]。そこで、フランスを標的とした NSA によるシギント活動の断片を見てみたい。

ア　特別収集サービス（SCS）

既述（第 2 部第 2 章 6）の通り、フランスの首都パリの米国大使館には特別収集サービス（SCS）の拠点が置かれており、フランスの政治外交情報を初め各種の情報を収集している。

イ　在米のフランス大使館、国連代表部からのデータ収集[30]

既述（第 2 部第 2 章 7 （３））の通り、NSA は各国の在米大使館と国連代表部 38 公館から、TAO グループを使用してデータを収集している。フランスの大使館と国連代表部はその対象とされている。

大使館に対する収集方法は、「ハイランズ」と「PBX」という二つの手法である。「ハイランズ」は、大使館内の端末或はシステムに何らかのインプラントを設置してデータを取得するものであり、「PBX」とは電話の交換機に何らかの工作をするものと考えられる。

国連代表部に対する収集方法は、「ハイランズ」と「バクラント」という二つの手法であり、後者の「バクラント」は、コンピュータ・スクリーンのデータを読み取り収集するものである。

ウ　フランス外務省の VPN（仮想専用ネットワーク）攻略

現在多くの事業体は VPN（仮想専用ネットワーク）を使用して、その構成組織内通信の秘密保全と効率を実現している。政府機関も例外ではなく、フランスの外務本省と在外公館は VPN で結ばれている。

ところが、NSA の 2010 年の内部資料によれば、米 NSA はこの VPN 回線に繋った暗号を解読してそのシステムへの侵入に成功しているとされる[31]。フランス外務省内の連絡通信は、全て NSA が読んでいる可能性があったということである。

---

[29] Laura Poitras, Marcel Rosenbach and Holger Stark, “Ally and Target: US Intelligence Watches Germany Closely,” *Spiegel Online*, 12 August 2013, accessed 15 August 2013, http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html

[30] Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014), 145-147.

[31] “Success Story: NSA Targeted French Foreign Ministry,” *Spiegel Online*, 1 September 2013, accessed 27 October 2013, http://www.spiegel.de/international/world/nsa-targeted-french-foreign-ministry-a-919693.html

エ　仏系企業を標的

NSA の内部資料を分析すると、フランス系の通信関係企業が NSA の諜報対象になっていることが分かるとされる[32]。

即ち、NSA の内部資料に、wanadoo.fr と alcatel-lucent.fr のメールアドレスが多く表示されており、NSA はこの 2 社を標的としてデータ収集をしていると推定される。Wanadoo は、フランス・テレコムの子会社（現在は本社に再統合）でインターネット事業者であり、Alcatel-Lucent は、仏アルカテルと米ルーセント・テクノロジーの合併会社で、インターネット関連の海底光ケーブルやルータを扱っている。インターネット通信関連企業を標的にすることは、インターネット空間の支配を目指す NSA としては当然の行為であろう。

なお、既述（第 2 部第 3 章４（３）経済産業情報・科学技術情報の収集）したように、NSA はフランスの経済産業情報について幅広い情報関心を設定している。

オ　大統領など政府幹部の電話通話の傍受

2015 年 6 月の報道[33]及びそこで引用された NSA 内部資料[34]によれば、NSA は過去

---

[32] Jacques Follorou, “France in the NSA's crosshair：Wanadoo and Alcatel targeted,” *Le Monde*, 21 October 2013, accessed 22 October 2013, http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-wanadoo-and-alcatel-targeted_3499739_651865.html

[33] “ Espionnage Élysée,” *Wikileaks*, 23 June 2015, accessed June 2015, https://wikileaks.org/nsa-france/

--Fabrice Arfiet, Jerome Hourdraux and Julian Assange, “2006-2012: Hollande, Sarkozy et Chirac écoutés,” *Mediapart*, 23 June 2015, accessed 24 June 2015, http://www.mediapart.fr/journal/international/230615/2006-2012-hollande-sarkozy-et-chirac-ecoutes

--Fabrice Arfiet, Jerome Hourdraux and Julian Assange, “Revealed: how US tapped phones of three French presidents ,” *Mediapart*, 23 June 2015, accessed 24 June 2015, http://www.mediapart.fr/journal/france/230615/revealed-how-us-tapped-phones-three-french-presidents

--Martin Untersinger, “Comment la NSA a-t-elle pu surveiller des conversations au plus haut niveau de l'Etat ?” *Le Monde,* 23 June 2015, accessed 24 June 2015, http://www.lemonde.fr/pixels/article/2015/06/24/comment-la-nsa-a-t-elle-pu-surveiller-des-conversations-au-plus-haut-niveau-de-l-etat_4660318_4408996.html

--Martin Untersinger, “Trois présidents français espionnés par les Etats-Unis,” *Le Monde*, 23 June 2015, accessed 24 June 2015, http://www.lemonde.fr/pixels/article/2015/06/23/trois-presidents-francais-espionnes-par-les-etats-unis_4660295_4408996.html

[34] この内部資料は、その情報内容から判断して、スノーデン資料ではなく、他の情報漏洩者からのものであると指摘されている。この漏洩者は、愉快犯的反体制派の可能性もあれば、或は他国諜報機関のスパイである可能性もあるとされる。

--“Wikileaks published some of the most secret NSA reports so far,” *Top Level Telecommunications,* 26 June 2015, accessed 29 June 2015,

10 年以上に亘って、フランスの大統領や政府幹部の通信を傍受してきたことが明らかになった。

報道された NSA 内部資料[35]は、毎日の「世界シギント・ハイライト」（Global SIGINT Highlights）の幹部版（Executive Edition）であるが、フランスに関して幹部間の通信の傍受を基とした情報が含まれており、その中には、明らかに資料源がフランス大統領と閣僚の会話傍受と認められる次の情報が含まれている。即ち、

- 2012 年 5 月 22 日付ハイライト～ホランド大統領とエロー首相の会話
- 2010 年 6 月 10 日付ハイライト～サルコジ大統領とジュペ外相の会話
- 2006 年 12 月 28 日付ハイライト～シラク大統領とドスト＝ブラジ外相の会話

また同時に、2010 年時点の NSA の電話傍受標的データベースからフランスの政治関係標的が抜粋報道[36]されているが、それには、大統領の他、大統領府長官、大統領外交顧問、主要閣僚や外務省幹部などの固定電話と携帯電話 15 個が含まれている。これらから判断して、NSA はフランスの大統領、主要閣僚他政府の主要幹部の電話を長期に亘って傍受してきたものと見られる[37]。なお、これら電話傍受の手段については、今までのところ資料や報道が見られないが、上記ア、イ、ウの手段を含め、NSA の収集態勢全体を活用しているものと考えられる。

なお、本件報道に対応して、2015 年 6 月 24 日オバマ米大統領とオランド仏大統領は電話会談を行い、オバマ大統領は、「インテリジェンスと安全保障分野に於ける緊密な協力を含む二国間関係の堅持を約束すると共に、2013 年末の当局間の約束、即ちホランド大統領の通信は（その時点で）標的としていないし今後も標的としないことを再確認した。」[38]

カ　余話～大統領官邸へのハッキング

2012 年 5 月に大統領官邸であるエリゼ宮のネットワークに対するハッキングがあり、極秘メモなどの内容が窃取された。フランス当局はこれを NSA によるものではないかと疑い、NSA と DGSE との間に興味深い遣取りがあったので、NSA の内部資料とこ

---

http://electrospaces.blogspot.jp/2015/06/wikileaks-publishes-some-of-most-secret.html

[35] NSA 内部資料、NSA, “Global SIGINT Highlights,” *Wikileaks*, 23 June 2015, accessed 24 June 2015, https://wikileaks.org/nsa-france/intercepts/

[36] NSA 内部資料、”Top French NSA Targets,” *Wikileaks,* 23 June 2015, accessed 24 June 2015, https://wikileaks.org/nsa-france/selectors.html

[37] NSA 内部資料、NSA, “Global SIGINT Highlights,” *Wikileaks*, 23 June 2015, updated 29 June 2015, accessed 30 June 2015, https://wikileaks.org/nsa-france/intercepts/
29 日に追加掲載された資料には、局長クラスを標的とした通話傍受に基づく情報も含まれている。

[38] US,　The White House, Chief of Press Secretary, “Readout of the President’s Call with French President Hollande,” 24 June 2015, accessed 26 June 2015, https://www.whitehouse.gov/the-press-office/2015/06/24/readout-president%E2%80%99s-call-french-president-hollande

れに基づく報道[39]を中心に見てみたい。

2013 年 1 月 NSA のアレクサンダー長官はフランスを訪問したが、その際、DGSE と ANSSI(国家情報システム保全庁、サイバーセキュリティ担当官庁)との会談では、DGSE と ANSSI のそれぞれの長官から、突然、本件ハッキング行為について詰問され、米国が関与していないか質問されたという。これに対し NSA 長官は、その場で、NSA の関与を否定して、真犯人究明のための技術支援を申し出た。

NSA 長官の発言に沿って、NSA は NTOC（脅威作戦センター）の分析官 2 人を同年 3 月パリに派遣することとなったが、フランス側は、訪問直前になって訪問を断ると共に、DGSE 技術局長（シギント責任者）と ANSSI 長官の NSA 訪問を要求してきた。この訪問について、フランス側は、ハッキングについての技術的詳細を提示し、真犯人究明への協力を要請するとしていた。

そこで、訪問日が 4 月 12 日に設定されたが、NSA は事前準備のため、先ず組織内の責任部署である TAO グループに確認したところ、関与を否定したという。そこで、更にファースト・パーティとセカンド・パーティの諸機関に問い合わせたが、何れの機関も関与を否定したという。ここでファースト・パーティとは米国自身の諜報諸機関であり、関与の可能性があるのは CIA、またセカンド・パーティでは英 GCHQ と加 SCE に関与の可能性があると見られた[40]が、何れも否定したという訳である。

但し、本件について、NSA は、イスラエルのモサッドとシギント国家部隊 ISNU には照会しなかったという。

ところで、そもそも、フランス当局が NSA の仕業ではないかと疑った理由は、ハッキングの技術が極めて高度であり世界でも一部の国家機関しか行なえないものであること、そして、使用されたマルウェアが NSA が開発に関わった Flame と同様の特徴を有することにあるとされる[41]。NSA 長官の訪仏前の 2012 年 11 月には、これがリークされてフランス国内で大々的に報道され、NSA に批判が向けられていたのである。Flame はイランの核燃料施設の攻撃にも使われたマルウェアで、その開発には NSA、

米国の緊密な同盟諸国首脳の電話傍受は、メルケル独首相の通話傍受が 2013 年秋に大きく取り上げられ、数十人(dozens)の同盟国首脳が傍受対象から除外されたとされている。第 2 部第 2 章 6（4）及び第 3 部第 3 章 5（2）ウ参照。

[39] Jacques Follorou and Glenn Greenwald, "The NSA's intern inquiry about the Elysee hacking revealed," *Le Monde,* 25 October 2013, accessed 14 April 2015, http://www.lemonde.fr/technologies/article/2013/10/25/the-nsa-s-intern-inquiry-about-the-elysee-hacking-revealed_3502734_651865.html

[40] 英加二つの機関が関与の可能性ありとされる理由としては、英国 GCHQ はその力量及び地理的条件のため関与の可能性があり、カナダ CSE はそのフランス語能力のため UKUSA 諸国の中でフランスを担当しているのではないかと推定される。

[41] "French weekly reports on alleged US cyber espionage attack on president's office," *BBC Monitoring European,* 23 November 2012, accessed 14 April 2015, http://www.biyokulule.com/view_content.php?articleid=5429

CIA、そしてイスラエルが関与したと言われている。そこで、ファースト･パーティとセカンド･パーティの諸機関が関与していないのであれば、残る可能性はイスラエルということになる。

2008 年の NSA 内部文書では、イスラエルは、米国に対して攻撃的な諜報機関として、世界中で第 3 位と評価されていたという[42]。フランス大統領府を標的にする可能性も十分にあるということであろう。

なお、NSA がイスラエルに照会しなかった組織上の理由は、「フランスは、イスラエルとの共同の議論[43]の対象となる標的ではないため」という。この表現から示唆されるのは、ファースト・パーティとセカンド･パーティ諸機関とは、フランスに対するハッキング作戦について共同の議論を行っているという事であり、また、ハッキング作戦についてのイスラエルとの共同の議論は、フランスに対しては行っていないが、他の何れかの国に対しては行っているという事である。正に、サイバー空間における「ハッキング」（NSA の用語ではコンピュータ･ネットワーク資源開拓 CNE）においても、世界のプレーヤーの間では合従連衡の世界が展開されているのである。

（５）諜報主体としてのフランス

上記の様にフランスは米国初め UKUSA 諸国の諜報対象となっているが、フランスが普通の国である以上、一方的に諜報の標的になっている訳ではなく、当然、自らも米国初め UKUSA 諸国に対してシギントを含む諜報活動を行っている筈である。

しかし、残念ながら、この面での資料は極めて少なく、断片的である。その断片的資料を見て行きたい。

ア　米国の 2007 年シギント「戦略的任務リスト」の記載

第 2 部第 1 章２「戦略的任務リスト」で既述したところであるが、米国シギントの収集任務分野の一つに外国諜報機関からの対米諜報活動があり、中国初め 10 ヶ国が特記されているが、その中にフランスが含まれている。

この対米諜報活動はシギント活動に限定されないが、フランスが対米諜報活動に従事しており、機会と能力があれば当然シギント面でも諜報活動を行っていると推定できるであろう。

イ　フランスによるコンピュータ･ネットワーク開拓（CNE）活動

カナダ CSE の 2010 年と 2011 年の内部資料[44]は、カナダ CSE による CNE 対策

---

[42] Follorou and Greenwald, “The NSA’s intern inquiry about the Elysee hacking revealed,” *Le Monde.*

[43] 「共同の議論」とは要するに共同して了解した上でのハッキング作戦ということであろう。

[44] 次の二つのスノーデン資料である。

（Counter-Computer Network Exploitation）、つまり他国シギント機関その他による CNE・ハッキング行為への対策について記述しているが、そこでフランス諜報機関による可能性が高いマルウェアを発見したとしている。

即ち、カナダ CSE は、2009 年 11 月に Snowball と名付けたマルウェアを発見。それ以来このマルウェアの追跡究明を続けてきたが、マルウェアはその後 SnowballⅡ、Snowman と進化しているため、全体を Snowglobe と名付けた。このマルウェアの追跡究明では、シギント・プラットフォームの中の特別資料源や外国衛星通信収集などで収集したデータを活用して追跡を続け、一定の解明が出来たという。

それによれば、マルウェアを使用して侵入したネットワークを運用するインフラ（所謂、作戦中継機）としては、カナダ、米国と英国に多くが設定されており、フランス語サイトの利用が多いという。更に究明したところ、当該マルウェアに運用者が付けた名称は Barbar（フランスの子供向けの人気番組名）であり、また、開発者は Titi とフランス語[45]で記載されていることが判明した。そして、その他の特徴をも総合的に検討して、この Snowglobe マルウェアはフランスの諜報機関のものである可能性が高いと判断している。

このマルウェアの標的としている組織は、UKUSA 諸国の中では、カナダのフランス語報道機関がある。但し、最重点の標的は、イランの外務省及び核開発に関係する大学や研究機関である[46]。この他、欧州ではギリシャ、フランス、ノルウェー、スペインでマルウェアが発見されているが、標的は欧州金融協会（European Financial Association）である可能性があるとされ、また、旧フランス植民地のアルジェリアや象牙海岸も標的とされている。

この一例によって、フランスにとって UKUSA 諸国が最重要な標的ではないものの、

--CSE, *Snowglobe: From Discovery to Attribution,* (2011), accessed 15 April 2015, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH68ea.dir/doc.pdf

--CSE, *Pay attention to that man behind the curtain: Discovering aliens on CNE infrastructure*, (June 2010), accessed 15 April 2015, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0142/416fcbbf.dir/doc.pdf

[45] Titi は、フランスの人名ティエリの略称、或はフランス口語で小人のことを言うとされる。

[46] フランス諜報コミュニティを情報源とする下記の報道によれば、イランについて、嘗ては米国やイスラエルからの情報提供に依存していたが、2006 年から 2010 年の間に DGSE の能力が向上して、単独での対イラン CNE を実施できるようになったという。そして、自分で機微な情報を収集できるようになって初めて、米、英、独、イスラエルと情報交換を進展させることができるようになったとしている。情報の世界の協力は常に情報のギブ&テイクが基本であるという事である。Jacques Follorou and Martin Untersinger, "La France suspectée de cyberespionage," *Le Monde,* 21 March 2014, updated 19 May 2014, accessed 15 April 2015, http://www.lemonde.fr/international/article/2014/03/21/la-france-suspectee-de-cyberattaque_4387232_3210.html

UKUSA 諸国も対象として諜報活動を行っているのは明白であろう。

ウ　フランス国内での対米、対 UKUSA 諸国のシギント活動

　フランス国内での対米等のシギント活動に関する資料は得られていない。しかしながら、DGSE に対してフランス・テレコム社が積極的に協力しているという前提に立てば、フランス国内の米国大使館、領事館は言うに及ばず、米国系企業なども含めて、フランス・テレコム社の協力を得て、米国権益に対してシギント活動を行っていると推定して誤りではないであろう。

第３章　サード・パーティ・ドイツとの独特な関係

サード・パーティ諸国の中でも、ドイツはNSAにとって重要特異な国である。ドイツは現在NSAにとって欧州大陸に於ける最重要拠点であるが、また同時に、ドイツは第二次世界大戦での旧敵国であり、東西冷戦では冷戦の前線国家であったという歴史的経緯も関係していると考えられる。米国NSAとの密接且つ微妙で独特な協力関係を見ていくこととする。

１　連邦諜報庁BND(Bundesnachrichtendienst)概観

ドイツのシギント機関は、対外諜報機関である連邦諜報庁が所管している。そこで、連邦諜報庁とそのシギント部門について、公式ウェブサイト情報[1]を中心に概観してみたい。

（１）沿革

連邦諜報庁の前身は、有名なゲーレン機関である。

ゲーレン機関は、1946年7月旧ドイツ軍のゲーレン少将が、米軍と合意の下その支援を受けて設立した私設諜報機関である。ゲーレン少将は、ドイツ参謀本部の対ソ連諜報部門である東方外国軍課の責任者であったが、大戦末期にドイツの敗戦と大戦後の米ソ冷戦を見通していた。そこで、東方外国軍課の諜報資産を秘密裡に保全した上で、大戦後に米軍の支援と資金を得て、米軍占領下のバイエルン州内に私設の諜報機関を設置したのである[2]。

その後、1949年米英仏の占領地区にドイツ連邦政府（西ドイツ）が成立し、更に1955年に主権回復宣言を行なって再軍備を開始するなど、西ドイツは独立主権国家としての形態を整えた。これに伴い、1956年ゲーレン機関は連邦政府に移管され、連邦諜報庁が設立された。組織は、連邦の行政機関として首相府に併置されている。

（２）人員・予算・組織

連邦諜報庁は、対外諜報機関であるが、その諜報源として、公式ウェブサイトではヒューミント、シギント、イミント、オシントを挙げており、総合諜報機関である。シギントは、既にゲーレンの私設機関時代に開始したという[3]。

連邦諜報庁の現在の人員は、約6500人であり、内約750人が軍人である。2015年度予算は、6億1557万ユーロである[4]。その規模は、ヒューミントその他を含む全体で

---

[1] BNDウェブサイト、Bundesnachrichtendienst, accessed 27 March 2015, http://www.bnd.bund.de/DE/_Home/home_node.html

[2] この経緯は、『諜報・工作―ラインハルト・ゲーレン回顧録』（1973年）に詳しく記載されている。

[3] 小谷賢（編）『世界のインテリジェンス』（ＰＨＰ、2007年）、165頁。

[4] 独財務省ウェブサイト、*Bundeshaushalt 2015,* accessed 27 March,

も、英国のシギント専門機関 GCHQ と比べると、人員は同程度、予算は半額以下であり、シギント機関としては、それ程強大ではないことが推定される。

組織は、１４の局から構成されており、ヒューミント担当局、シギント担当局の他、地域分析担当局２局、テロ担当局、大量破壊兵器拡散担当局、状況監視センター、防諜保安局、情報技術局等がある。また、長官の下に３人の副長官がおり、それぞれ担当を決めて分担しているが、必ずしも、全ての局を局割りで分担しているようではないようである。

- 副長官（長官代理）～分析、ヒューミント、大量破壊兵器拡散、テロ担当
- 副長官（軍事担当）～状況監視センター、シギント局、
  涉外、オシント・イミント担当
- 副長官（管理担当）～防諜保安、情報技術支援、技術研究開発、管理担当[5]

（３）BND のシギント組織

BND のシギント担当局は、技術偵察局（Technische Aufklaerung : TA 局）と呼ばれている。NSA の内部資料[6]によれば、シギント局は収集部、分析部、暗号解析部、サイバーインテリジェンス部の４部で構成されている。

収集部には、固定収集施設（sites）、移動収集（mobile collection）、戦略的収集（strategic collection）、令状傍受（warranted interception）の四つの収集部署がある。

固定収集施設は、衛星通信と無線通信の傍受施設であり、次の施設が判明している[7]。これらの幾つかは、冷戦終結後米国から引き継いだ施設である[8]。

- シェーニンゲン（ニーダーザクセン州）　＜衛星通信＞
- ラインハウゼン（同上）

---

http://www.bundeshaushalt-info.de/startseite/#/a/a/ausgaben/einzelplan.html

[5] ス資料 NSA, “Internal NSA presentation on the BND's organization,” *Spiegel Online,* 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/media/media-34050.pdf

[6] 同上。

[7] “NSA-Skandal: BND greift täglich 220 Millionen Verbindungsdaten ab,” *Heise Online*, 30 January 2015, accessed 27 March 2015, http://www.heise.de/newsticker/meldung/NSA-Skandal-BND-greift-taeglich-220-Millionen-Verbindungsdaten-ab-2533630.html

[8] 次の施設も米軍から引き継いで運用しているとみられる。

- トーデンドルフ（シュレスウィッヒ・ホルスタイン州）　旧米海軍施設
- フレンスブルグ（同上）　旧米陸軍施設　（無線通信）
- ホーフ（バイエルン州）　旧米空軍施設　（エリント）

--Matthew Aid, “Strange Deletions from the NSA Documents Published Online by Der Spiegel,” *Matthewaid.com*, 18 June 2014, accessed 3 April 2015, http://www.matthewaid.com/post/89206344456/strange-deletions-from-the-nsa-documents-published.

○　アウグスブルグ・ガブリンゲン（バイエルン州）　旧米陸軍施設
○　バード･アイブリング（同上）　旧 NSA 施設　＜衛星通信＞、＜無線通信＞

戦略的収集は、インターネット通信基幹回線からの（大量且つ不特定の通信）収集である。外国通信であれば、BND は一定量の傍受、データ収集が認められており[9]、国内数ヶ所で通信事業者の協力を得て実施している。これによりアクセスを認められた回線容量は膨大なものである[10]。

サイバーインテリジェンス部は、2011 年頃に新設された部署であり、サイバー生産、サイバー技術、サイバー作戦の三つの課から構成されている[11]。

（４）BND の任務規定

1990 年制定された連邦諜報庁法第１条[12]により、連邦諜報庁は内閣官房長官の管轄下にあり、連邦共和国の外交及び安全保障政策にとって重要な情報を収集することが任務とされている。

また、同法第９条により、連邦諜報庁の任務遂行のため必要な場合、又は公共の安全（oeffentliche Sicherheit）のため必要な場合は、国内の公共諸機関に対して情報を提供することができることとされている。更に、同法１２条により、その活動について内閣官房長官に報告すると共に、連邦各省大臣に対してその所掌事務に関して直接報告することとされている。

（５）連邦議会監視委員会

諜報諸機関の活動を監視するため、連邦の諜報活動に関する議会監視に関する法律[13]によって、連邦議会に監視委員会（Parliamentalische Kontrollgremium）が置かれている。委員は連邦議会が議員任期の初めに議員の中から選出するとされる。

監視対象となっている諜報機関は、連邦諜報庁、連邦憲法擁護庁、軍事保安局の三機関である。

なお、連邦憲法擁護庁(Bundesamt fuer Verfassungsschutz)とは、ドイツのセキュ

---

9 Christiane Schulzki-Haddouti, “Mit dem Staubsauger durch den Telekommunikationsverkehr,” *Heise Online*, 16 February 2001, accessed 6 April 2015, http://www.heise.de/tp/artikel/4/4941/1.html

10 Julian Borger, “GCHQ and European spy agencies worked together on mass surveillance,” *The Guardian*, 1 November 2013, accessed 6 November 2013, http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

11 ス情報、NSA, *Talking Point Topics Proposal,* (circa April 2013), accessed 20 June 2014, http://www.spiegel.de/media/media-34119.pdf

12 ドイツ、Gesetz ueber den Bundesnachdienstdienst.

13 ドイツ、Gesetz ueber die parliamentalische Kontrolle nachrichtendienstlicher Taetigkeit des Bundes.

リティ・サービスであり、内務省に属する。人員は、2500～3000 人で、2015 年度予算は 2 億 3077 万ユーロである[14]。なお、連邦制を採るドイツは１６の州で構成され、各州にはそれぞれ州憲法擁護庁がある。連邦と各州の憲法擁護庁は連携して活動しているため、セキュリティ・サービス機能は連邦憲法擁護庁と各州憲法擁護庁が協力して荷っていると見られる。また、軍保安局は、連邦軍の防諜・保安を担当している。

14　独財務省ウェブサイト、*Bundeshaushalt 2015.*

２　在独 NSA 組織と米独関係の基本

（１）現在のドイツ内での組織、施設

NSA は現在でも、ドイツ国内に相当数の施設を維持しているとされるが、その全貌は必ずしも明らかではない。2007 年時点でも、１ダース以上の収集拠点を保持していたとされる[15]。

各種資料から、現在その存在が判明しているドイツ国内に於ける NSA 組織は次の通りである。

ア　欧州シギント・センター（European Cryptologic Center: ECC）

ダルムシュタット近郊のグリースハイム米陸軍基地内に所在

欧州大陸に於ける NSA 最大の分析センターであり、2011 年現在の人員は約 240 人である。NSA は、米国領土内にはミニ NSA とも呼べる地方本部が４つあるが、ECC は、それに次ぐレベルの組織であり、謂わば、NSA の欧州前進基地である[16]。

ECC の前身組織 ESOC(European Security Operation Center) は 2000 年代初めに設置されたが、それが発展して、2011 年 5 月に ECC に改組された。約 240 人の人員は、NSA 本部からの派遣職員、各軍シギント組織からの派遣軍人、民間契約職員など多様である。

その任務は、先ず、米国の欧州軍とアフリカ軍に対する支援である。両軍の司令部は近くのシュトゥッツガルトに所在しており、両軍司令部に対するインテリジェンス支援と両軍に所属するシギント部隊に対する教育訓練なども担当している。また、NSA 前進分析基地として、戦域レベルや戦闘レベルでの任務の他、国家的諜報任務も果たしている。即ち、特定の課題について地の利を生かした分析報告を行い、大統領デーリーブリーフィングや域内各大使に対する情報支援でも使用されるなど活躍しているという。地の利とは、諜報対象地域のアフリカ、中近東近くに所在して、地域の CIA、特別収集サービス SCS、欧州軍・アフリカ軍合同分析センターなど各種の米国インテリジェンス組織、或はインテリジェンス顧客との交流・相互刺激、更に、セカンド・パーティ、サード・パーティとの協力を通じて、より良い情報分析報告ができるということである。特にアフリカ諸国についての分析では優れているようである[17]。

---

[15] Sven Becker, et. al., “New NSA Revelations: Inside Snowden’s Germany File,” *Spiegel Online,* 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

[16] ス資料、NSA, *The ECC—NSA’s Newest Cryptologic Center*, 10 June 2011, updated 13 June 2011, accessed 1 April 2015, http://www.spiegel.de/media/media-34076.pdf

[17] 主な出典資料は、上記資料の他、次のスノーデン資料である。
--NSA, *The European Security Center to Become the ‘ESOC’*, 11 September 2006, accessed

イ　欧州技術センター（European Technical Center: ETC）

ヴィースバーデンの米陸軍基地内に所在

欧州大陸での NSA の通信技術センターである。ヴィースバーデン地域は、欧州に於ける NSA の情報通信網のハブであり、ここでは、NSA の通信技術者が相当数常駐して、NSA の通信網、シギント収集やデータフローの技術的管理を行っている。対象とする通信網は、NSA と各軍シギント組織だけではなく、サード・パーティ諸国との通信網も含まれている。本センターが担当しているサード・パーティ諸国は、2011 年現在で欧州、アフリカ、中近東の２７ヶ国に及んでいるとされる。即ち、NSA が協力関係を有するサード・パーティ諸国の内、アジアを除く殆どの組織との通信網の維持管理に当たっている組織でもある[18]。

ウ　NSA 欧州事務所(NSA/CSS Europe: NCEUR)

シュトゥッツガルト市ファイヒンゲン地区

（米国欧州軍司令部・アフリカ軍司令部と同一地）

NSA の欧州地区の事務所が所在する。欧州地区内の NSA の諸組織の統括調整を行う事務所である。欧州軍司令部やアフリカ軍司令部関係の業務量が多いことなどのため、同一場所に設置されていると考えられる[19]。

エ　在独特別渉外活動（Special US Liaison Activity Germany: SUSLAG）

バード・アイブリング所在

独 BND との渉外調整組織。嘗てバード・アイブリングには NSA の衛星通信の傍受拠点があったが、2004 年に NSA はその独自運用を停止して、BND に移譲した。その後、衛星通信の分析処理を米独共同して行ってきた（後述）。

オ　特別収集サービス(SCS)の拠点

---

1 April 2015, http://www.spiegel.de/media/media-34072.pdf

--NSA, *Forward Production at NCEUR—Inside the Customer's Decision Space,* 14 January 2005, accessed 1 April 2015, https://edwardsnowden.com/2014/06/18/forward-production-at-nceur-inside-the-customers-decision-space/

--NSA, *European Security Center to Begin Operations,* 29 March 2004, accessed 1 April 2015, http://www.spiegel.de/media/media-34070.pdf

[18] ス資料、NSA, *NSA Communications Hub in Europe Is Modernized*, 20 October 2011, accessed 1 April 2015, http://www.spiegel.de/media/media-34083.pdf

--ス資料、NSA, *SID Around the World: The Rheinland*, 16 September 2003, accessed 1 April 2015, http://www.spiegel.de/media/media-34080.pdf

[19] Becker, et. al., "…: Inside Snowden's Germany File," *Spiegel Online.*

特別収集サービスは、CIA と NSA の共同事業であり、大使館等の在外公館を活用して行う収集分析活動である。ドイツには在ベルリン大使館と在フランフルト領事館の二つの拠点で活動してきた。これらの諜報対象は当然ドイツである。

但し、既述（第２部第２章の６）したように、在ベルリン大使館での活動は、2013 年末に停止された可能性が高い。在フランクフルト領事館における活動については停止されたか否か不明である。

カ　その他の収集拠点

上記の他にも、ドイツ国内には NSA の拠点が相当数存在すると見られる。

（２）諜報対象としてのドイツ

ア　友好国にして諜報対象

ドイツは、米国 NSA にとってサード・パーティの協力国であるが、協力国であるということと諜報対象とすることとは矛盾しない。実際、米国 NSA が原則的に諜報対象としないのはセカンド・パーティの UKUSA 諸国（英加豪 NZ）４ヶ国だけである。その他の国々は、米国の国益に基づく情報要求に従い諜報対象となる。従って、友好国であろうとも、米国の国益に重要な影響を与え得る国々は、当然諜報対象としての優先順位も高く評価されることになる。

イ　諜報の優先順位

そこで、諜報対象としてのドイツの位置付けを見ると、既述した 2007 年「戦略的任務リスト」（第２部第１章の２）によれば、分野別では、１６分野の内の２分野、戦略的科学技術と外交政策において、日本と並んで記載されている。

最近の諜報対象優先順位リストでは、2013 年 4 月現在の NSA 内部資料があり、資料自体は報道されていないが、資料に基づく報道[20]によれば、総体としては、NSA にとって優先順位最高の諜報対象は中国、ロシア、イラン、パキスタン、アフガニスタンであるが、ドイツは、フランスや日本と並んで中位に位置付けられているという。優先順位は５段階（１が最高、５が最低）で位置付けられており、分野毎のドイツの位置付けは、次の通りである。

３：　外交政策、経済的安定、金融システム

４：　武器輸出、新技術、高度通常兵器、国際貿易

５：　防諜、米国重要インフラに対するサイバー攻撃

---

[20] Laura Poitras, Marcel Rosenbach and Holger Stark, “Ally and Target: US Intelligence Watches Germany Closely,” *Spiegel Online*, 12 August 2013, accessed 15 August 2013, http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html

ウ　標的の実例

ドイツを標的とする具体的な諜報活動としては、既述（第 2 部第 2 章 6 特別収集サービス（4））したメルケル首相に対する情報収集がある。2015 年 7 月にウィキリークスが報道した NSA 内部資料の NSA「世界シギント・ハイライト」幹部版[21]には、2009 年や 2011 年中のメルケル首相の電話通話傍受に基づく各種情報が掲載されている。また、2010 年時点の NSA の電話傍受標的データベースには、メルケル首相を含むドイツ政府幹部の固定電話番号と携帯電話番号が 140 個以上掲載されており[22]、これらの電話通話が傍受対象となっていたことが伺われる。

その他には、ドイツの衛星通信企業に対する攻撃が報道されている[23]。

それによれば、英国 GCHQ は、ドイツの企業を標的として、英国バッドの施設から CNE（コンピュータ・ネットワーク資源開拓）をしているという。標的となったのは、STELLER、 CETel、 IABG などのドイツの衛星通信事業者であり、それぞれ、衛星通信の地上局を運営して、主として（石油掘削基地、ダイヤモンド鉱山、難民キャンプ、多国籍企業の支店等）地上回線が十分でない遠隔地への衛星通信サービスを提供している。STELLER のケルン近郊ヒュルトの地上局には 7 5 個ものパラボラ・アンテナが設置されており、特に有名であるという。また、衛星通信の利用者には北欧の某国外務省も含まれるという。

GCHQ は、これら企業のシステム・エンジニアを狙って彼らの端末をハッキングして侵入してから、これを踏み台にして企業のコンピュータ・ネットワークに侵入しており、重要顧客リストや衛星通信の技術提供企業、そして将来の技術動向についてデータを収集していたという。なお、IABG のネットワークについては、「NSA のネットワーク分析センターが既に見ているかも知れない」との GCHQ 担当者のコメントが付されていたという。

---

[21] NSA 内部資料、"Top German NSA Intercepts," *Wikileaks,* 1 July 2015, updated through 20 July 2015, accessed 21 July 2015, https://www.wikileaks.org/nsa-germany/intercepts/

[22] NSA 内部資料、"Top German NSA Targets," *Wikileaks,* 1 July 2015, updated through 20 July 2015, accessed 21 July 2015, https://www.wikileaks.org/nsa-germany/selectors.html --Von John Goetz, Hans Leyendecker and Georg Mascolo, "Was die Wilileaks-Dokumente zeigen," Sueddeutscher Zeitung, 2 July 2015, accessed 2 July 2015, http://www.sueddeutsche.de/politik/selektorenliste-der-nsa-was-die-wikileaks-dokumente-zeigen-1.2547250

[23] Laura Poitras, Marcel Rosenbach and Holger Stark, "'A' for Angela Merkel: GCHQ and NSA Targeted Private German Companies," *Spiegel Online,* 29 March 2014, accessed 31 March 2014, http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html

何れにしろ、これは氷山の一角であり、その他にも、色々諜報対象としているのは間違いない。

（3）協力相手としてのドイツ

サード・パーティとしてのドイツとの協力関係は、サード・パーティ諸国との協力関係の一般論の通りであり、米国が主としてシギント技術を提供し、他方、ドイツは地理的特性からする重要標的通信へのアクセス、データを提供している関係と見られる。

協力関係の現状については、2013 年 1 月付の NSA 渉外部の内部資料[24]がある。この資料はサード・パーティ国との協力関係を年毎に総括した資料のようであるので、これを元に NSA と BND の関係を見てみると次の通り。

ア　NSA から BND への提供

① BND が独力でその外国衛星通信関連の（傍受処理分析）能力を維持できるように、相当量のハードウェアとソフトウェアを BND の費用で提供し、また、関連分析技術を提供した。（これは、主として BND に移管したバード・アイブリングの衛星通信傍受施設についての言及と見られるが、シェーニンゲンの BND 衛星通信傍受施設の運用でも裨益するところがあろう。）

② 軍事・非軍事のインテリジェンス報告を提供した。（通信素データではなく、エンド・プロダクトとしてのシギント報告書を提供していると考えられる。）

イ　BND から NSA への提供

① 外国衛星通信へのアクセスを提供した。（素データを提供していると見られる）

② 高価値のデータについてイグボ語(ナイジェリアの言語)の言語支援を提供した。

③ その他、ドイツは独特なアクセスを提供した。

③の詳細は不明である。欧州域外に於いて、BND は NSA と通信データ取得のための共同事業を行っていると見られる。また、現在まで十分明らかになっていないが、他にも、NSA が BND の協力を得て、ドイツ国内で秘密裡に収集している通信データが存在するようである。例えば、Glotaic 計画というものがあり、ノルトライン・ヴェストファーレン州内の通信基幹回線からデータを秘密裡に取得しているのではないかと、2015 年 2 月現在、連邦議会 NSA 調査委員会で問題となっている[25]。

---

[24] ス資料、NSA, Information Paper, *NSA Intelligence Relationship with Germany - Bundesnachrichtendienst,* 17 January 2013, accessed 20 June 2014, http://www.spiegel.de/media/media-34053.pdf

[25] “NSA-Ausschuss will Kooperation des BND mit Tarnfirmen aufklären,” *Heise Online*, 26 Feburary 2015, accessed 2 April 2015, http://www.heise.de/newsticker/meldung/NSA-Ausschuss-will-Kooperation-des-BND-mit-Tarnfirmen-aufklaeren-2560617.html

ウ　その他の特徴的動向

①　情報関心分野として継続すべくNSAとBNDが同意したのは、次の分野である。

～～テロ対策、国際組織犯罪、（不明）[26]、（不明）、薬物対策、特定国からの人の密輸（Special Interest Alien Smuggling）、アフガン・シギント連合

②　BND長官が2012年に、アフリカ地域、（不明）、大量破壊兵器拡散問題について協力を強化したいと提案したとされ、NSAはこれに前向きに対応することとしている。

③　テロ対策の面で、BNDは、NSAとBfVの協力関係強化の支援をしている。

2007年のドイツでのイスラム過激派の逮捕（後述）以来、NSAとBfVは徐々に協力関係を強化しており、情報分析協議を定例化し、ドイツ人・非ドイツ人の過激派の追跡でもより緊密に協力するようになった。また、BfVが国内でアクセスする通信データの収集処理を改善するため、NSAはシギントを探索し分析する支援を行っている。NSAは、XKeyscoreのソフトウェアをBfVに提供し、BNDはその活用についてBfVを支援している（後述）。

④　NSAの情報保証総局は、ドイツの連邦情報セキュリティ庁BSIと情報保証の分野で長期に亘って協力関係を持ってきた。この度、ドイツ政府がサイバーセキュリティ戦略を策定してBSIをその責任部署と定めたため、独BSIはCND（コンピュータ・ネットワーク防禦）を含めて情報保証分野での協力強化を望んでいる。CNDも協力範囲に含めるということであるので、NSAとしては、情報保証総局の他、シギント総局、ドイツのBfV，BNDを含む協力関係の強化の機会と考えている。なお、CND協力のため、情報保証及びCNDに関する了解覚書をNSAとBSI，BNDの間で締結すべく作業中である。

⑤　ドイツ政府は、個人情報保護法の解釈に変更を行い、BNDと外国機関とのインテリジェンス共有に関して柔軟性を拡大した。BNDは、インテリジェンス共有を拡大するため、長期に亘り、ドイツ政府に対して個人情報保護法の柔軟な解釈について働き掛けてきた。（具体的な解釈変更の内容は不明。）

⑥　ドイツは、アフガン・シギント連合（AFSC）への積極的な参加国であり、特定分野を分担して、当該分野についての分析報告と収集メタデータを共有している。

---

[26] （不明）とは、NSA内部資料の報道に当たって、特に機微な記述があり、報道メディアによって黒塗りにされた部分である。以下同じ。

３　在独 NSA の活動と米独関係の沿革

ドイツに於ける NSA の活動と米独関係の沿革については、現在までに報道されている NSA 内部資料は断片的であり、大戦後の全体像は分からない。そこで、その断片的な資料に加えて、戦後史の展開と西ドイツと統一ドイツが置かれた地政学的位置を考慮して、ドイツに於ける NSA の活動と米独シギント関係の推移を推定してみることとする。

（１）第二次世界大戦終結から冷戦終結まで

先ず、ヒットラー・ドイツ帝国が崩壊消滅して大戦が終結した後、占領国としての米国の関心は、ヒットラー・ドイツの残党を完全に排除してドイツを民主化することであり、従って、占領当局のシギント機関の任務も、ドイツ人の通信を監視することであったと考えられる。

しかし、直ぐに東西の冷戦が始まり、西ドイツは正にソ連を筆頭とする共産主義諸国との冷戦の主正面となった。従って、西ドイツ内にはソ連圏に備えて米軍の軍事基地が多数置かれ、また、米国シギント機関の関心も当然、対ソ連圏の収集が主体となったと考えられる。

対ソ連圏の収集に於いての米国 NSA と独 BND の関係を推定すると、独 BND はあくまで補助的役割であって、米国 NSA は基本的に、独力で（但し、UKUSA 諸国との協力を含む）強大な収集態勢を構築していたものと見られる[27]。先ず、東西冷戦に於ける最重要前線のインテリジェンスを、UKUSA 諸国以外の国と分担することは、容易なことではないと考えられる。また、西ドイツについて見れば、1955 年に主権回復宣言をしたとは言え旧敵国であり、完全な同盟国になった訳ではなく、依然として米国の監視対象でもあった[28]。そして、米国が西ドイツ内に構築した膨大なシギントシステムと

---

[27] 2007 年の NSA 内部資料によれば、NSA が戦後西ドイツ内で開設し或は廃止したシギント活動施設は、累計で 150 ヶ所にも及ぶという。
Becker, et. al., "…: Inside Snowden's Germany File," *Spiegel Online.*

[28] 西ドイツが米英仏の占領下にあった 1955 年までは、三ヶ国とも占領地内のドイツ人を監視していたが、英仏は、西ドイツの主権回復宣言後西ドイツに対する監視は削減したとされる。これに対し、米国は監視を続け、西ドイツ国内及び西ドイツと他の西欧諸国間の電話や通信を傍受し続け、1950 年代半ばでも、年間約 500 万件の電話通話を傍受していたとされる。
--Becker, et. al., "…: Inside Snowden's Germany File," *Spiegel Online.*

また、1975 年には、米大統領のボン訪問の先遣隊として来訪した米インテリジェンス機関員２人が、セキュリティ・チェック名目で首相府宮殿に入って、実際は電話回線に工作していたのが発覚した事実がある。
--Melanie Amann, et. at., "The German Prism: Berlin Wants to Spy too," *Spiegel Online,* 17 June 2013, 6 August 2014,
http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html

対比すれば、西ドイツ BND は、技術的にも資金的にも人員的にも、シギント任務を分担する程の信頼できる組織とは看做されていなかったのではないだろうか[29]。

（２）東独スパイが見た米独関係

東西冷戦時代には、東ドイツは NSA と BND のシギント部門にスパイを獲得し運営しており、それによって、当時の西ドイツに於ける NSA の活動や米独シギント関係を把握していた。そこで、そのスパイとスパイの見た米独関係について触れておきたい。

旧東ドイツの国家保安省の対外諜報局の担当官クラウス・アイヒナーによれば、次の通りである[30]。

ア　NSA 内の東独スパイ

旧東ドイツは、その崩壊前、NSA 内にスパイを２人持っていたという。

一人は、ジェームス・ホールで、1984 年に西ベルリンで勤務している際にスパイとして獲得され、後にフランクフルトに転勤になった。西ベルリンではトイフェルスベルク（悪魔の山）という地名の丘にある収集施設で勤務し、フランクフルトでは第 533 陸軍情報大隊に所属していた[31]。同人の直接の接触者は、東独のために働くトルコ人であった。同人からの情報は、NSA の各種指令・指示文書等の重要文書１万３千頁以上に及んだが、その中には国家シギント要求リスト（National Sigint Requirement List）約 4200 頁が含まれていた。同リストは国別にシギント要求項目の詳細が記載され（西独の場合約 30 頁に及ぶ）、項目毎に入手可能、近く可能、入手不可能の別が記載されている極めて重要な文書であったとされる[32]。なおこのような文書の持出し複写が可能

---

[29] NSA が BND のシギント部署 TA 局と公式な協力関係を開始したのは 1962 年である。そもそも BND の前身組織は 1946 年に発足して以来、米軍と（これを継承した）CIA の支援と資金を元に運営されてきた組織であるから、米国 NSA が BND のシギント部門と任務分担を図ろうと考えれば何時でも協力は開始できる状況にあった筈である。NSA の公式な協力開始が BND の前身組織発足１６年後であったということは、BND の TA 局がその程度にしか評価されていなかったということではないだろうか。
--ス資料、NSA, Information Paper, *NSA Intelligence Relationship with Germany - Bundesnachrichtendienst(BND)*, (17 January 2013), accessed 20 June 2014, http://www.spiegel.de/media/media-34053.pdf

[30] Michael Sontheimer and Andy Mueller-Maghun, “Interview with Ex-Stasi Agent: ‘The Scope of NSA Surveillance Surprised Me’,” S*piegel Online*, 18 June 2014, accessed 20 March 2015, http://www.spiegel.de/international/germany/interview-with-former-stasi-agent-about-the-nsa-a-975010.html

[31] 経歴からすると、ホールは NSA 本体の職員というよりは、中央安全保障サービス（CSS）傘下の陸軍シギント部隊に所属していたと見られる。

[32] Georg Von Mascolo, “GEHEIMDIENSTE: Spurenvernichtung im Amt,” *Spiegel*, 26 July 1999, accessed 1 July 2015, http://www.spiegel.de/spiegel/print/d-14010746.html
なお、ジェームス・ホールは、東独の対外諜報局からの亡命者の情報により、1989 年に逮捕

であったのは、フランクフルトの部隊の保全措置が弱体であったためであったという。

また、二人目は、ジェフリー・カーニーで、西ベルリンのマリーエンフェルデ米空軍基地内の施設で勤務していたという。

両者を運営していたのは、東ドイツの国家保安省の対外諜報局である。

1989 年 11 月ベルリンの壁が崩壊し、東独国家の消滅が見通された 1990 年初め、東ドイツの対外諜報局の担当官（クラウス・アイヒナー）は、この二人のスパイから入手した NSA 関連資料約４０冊を国家保安省の中央資料館に移管した。移管は、貴重な資料を将来の歴史資料として保存したかったためであるとされる[33]。

米国は、後にこの文書の存在を知り、その提供を執拗に要求したという。その結果、資料の大部分が 1992 年 7 月に米国に引き渡された。その後、ドイツ国内の当該資料は、ドイツ連邦政府によって秘密指定され、現在では殆ど非開示になっているという[34]。

イ　BND 内の東独スパイ

また、旧東ドイツは、BND のシギント部門にも 1972 年以来スパイを運営していた。同スパイは米国との渉外事項に詳しい地位にいたため、シギントに関する米独協力の実態も掌握していたという。

ウ　スパイ情報から分かる米独関係

BND 内のスパイ情報に拠れば、東西冷戦時代、ソ連圏に対するシギント収集については、米国 NSA は西ドイツに依存することはなく、全て独力で強大な収集態勢を構築していたという[35]。そして、米独関係は一方的なもので、西独 BND が米国 NSA に対して、東独に関するシギントの提供を要請しても度々拒否されたという。例えば、BND の指導部は、西ベルリンの「悪魔の山」から NSA が収集している東ベルリンの通信素データの提供を何度も要求したが、これに対して NSA は情報報告書を提供することはあったが、シギント素データを提供することはなかったという[36]。そのため、BND は

され、懲役 40 年の有罪判決を受けた。

[33] Becker, et. al., "…: Inside Snowden's Germany File," *Spiegel Online.*

[34] 1992 年にドイツ内務省が資料を米国に引き渡した際は、コピーを取らずに原資料を引き渡したため、現在ドイツ連邦政府には資料自体が殆ど存在しないという説もある。
--Von Mascolo, "GEHEIMDIENSTE : Spurenvernichtung im Amt," *Spiegel.*

[35] インテリジェンスこそが、東西冷戦の勝敗を決する最重要事項であり、シギントに於いて米国が真に任務分担をして相互依存関係にあったのは、UKUSA 諸国だけであったということであろう。

[36] インテリジェンスにおいて素データは極めて重要である。先ず、情報報告書（エンド・プロダクト）（通常諜報源について一定のサニタイズ措置が採られている）の信頼性や正確性を評価するためには素データが不可欠である。エンド・プロダクト交換だけであれば、友好機関といえども情報操作をされる可能性が残る。また、素データの提供があれば、自ら収集した素データと総合分析することにより、より正確に或は広範囲に分析を行い、独自のエンド・プロダ

フランスに支援を求め、仏独共同で西ベルリンのテーゲル空港内に（「悪魔の山」と同一の通信網に対する）収集拠点を建設したという。

また、NSA 内のスパイ情報に拠れば、NSA の標的は全方位であり、東独や共産圏だけではなく、西ベルリンや西ドイツにも向いていたという。即ち、西ドイツの主要な政治家やビジネスマンの情報ファイルも作成されていたという。

これらの情報は、上記（１）で述べた米独関係の推定を裏付けるものであろう[37]。

（３）冷戦終結後

1989 年にベルリンの壁が崩壊したのを契機にソ連圏は崩壊し、冷戦は米国とその同盟国が勝利して終結した。そして、1990 年には、ドイツ最終規定条約が米英仏ソ・東独･西独の６ヶ国間で調印され､西ドイツが東ドイツを併合して完全に主権を回復して、統一ドイツが成立した。

冷戦終結により、米国は「平和の配当」を求めて、大幅な軍備削減を行い、また、シギントを含むインテリジェンス予算算も削減を行った。そして、ドイツが東西冷戦の前線国家でなくなった以上､ドイツ国内の米国シギント施設や活動も大幅に削減されたと考えられる。

（４） 9/１１後

クトを作成することができる。

[37] 余話～スパイの存在の意味する所

NSA 内部や BND 内部に東独のスパイが居た、それも、長期間に亘り発覚しなかったという事実は、注目に値する。過去にもあった事は、現在でもあり得るのである。現在でも、NSA の中に外国機関のスパイがいる可能性は否定できない。或は退職後の職員が工作を受けて現職中の知識を提供しているかも知れない。NSA の基本的なシギント収集態勢やシギントの技法の多くは既に、スノーデン告発がなくとも外国ヒューミント機関に知られていた可能性があるという事である。

なお、第 2 部第 2 章 7 CNE の最後の脚注に記載したように、米国人事管理局（Office of Personnel Management）は、2015 年 6 月 4 日、人事管理局の情報システムが侵入を受け 400 万人に及ぶ連邦職員の人事管理データが窃取された旨公表し、更に 7 月 9 日には、これに加えて個人背景調査（background investigation）記録から 2150 万人分の個人情報が窃取された旨公表した。

既述したように、個人背景調査とは連邦職員に採用されるため必要な調査であるが、その前提として申請者は相当の個人情報を提供する必要がある。特に（インテリジェンス関連を含む）高度なセキュリティ・クリアランスを必要とする国家安全保障関連職務（national security positions）に就くには、様式 86 に従い詳細な個人情報を提供する必要がある。今回はその様式 86 のデータも窃取されたのであり、且つ攻撃は中国からなされているという。中国のハッカーはスパイ工作に使用するため膨大な個人情報のデータベースを構築しているとされるが、様式 86 には詳細な経歴データ、健康状態の他、親族、友人関係、交友のある外国人、国外活動等のデータが含まれており、中国政府がそれを入手したとすれば、米国諜報機関職員に対してスパイ工作を仕掛けるための最高の基礎資料を得たことになると指摘されている。

ところが、9/１１の米国同時多発テロ事件によって、情勢は大きく変化する。先ず、米国では「世界中でのテロとの戦い」（global war against terrorism）が大きな政治課題となり、シギントを含むインテリジェンス予算が増額された。そして、アフガニスタン戦争（2001 年～）や第二次湾岸戦争（2003 年）を通じて、これらの地域諸国に対するシギント需要が高まった。また、同事件にはドイツ・ハンブルグにあったアル・カイダの細胞が深く関与（パイロット３人はハンブルグ在住）しており、米国にとってドイツを初めとする欧州諸国内のイスラム過激派の発見と監視が大きな課題となり、ここでもシギント需要が高まった。

こうして、ドイツは、テロとの戦いに於いて米国がシギント部門でも協力を強化するべき国となった。具体的には、ドイツ国内、そして欧州内のイスラム過激派に対する情報収集での協力であり、同時に、アフガニスタンその他の中東地域に対する情報収集での協力である。ドイツ国内のイスラム過激派の情報収集について言えば、米国当局にとっては、先ずドイツ当局、即ち BND や BfV との協力によることが望ましいと考えられるが、それが不十分であれば一方的にでも実行すべき任務ということになる。

この状況について、元 NSA 長官のマイケル・ヘイデン氏は、「9/１１後、NSA は BND との強固な協力関係を発展させるように尽力してきた。占領者として行動するのを避け、我々の協力を拡大提供したのである。」旨を述べている[38]が、米国 NSA の立場を実に微妙に表現したものと言えよう。また、NSA の元契約職員トーマス・ドレークは、「9/１１後、ドイツは NSA にとって海外で最重要な監視プラットフォームとなった。NSA と BND の関係は強化された。」旨を述べている[39]

---

[38] Poitras, Rosenbach and Stark, “Ally and Target: US Intelligence Watches Germany Closely,” *Spiegel Online*.

[39] Thomas Drake and Jesselyn Radack, interview by Sven Becker, Marcel Rosenbach and Joerg Schindler in circa July 2014, accessed 11 July 2014, http://www.spiegel.de/international/world/interview-with-nsa-experts-on-us-spying-in-germany-a-979215.html

４　9/１１以後の米独シギント協力の強化

9/１１後のシギントに関連する米独関係について、協力の具体例を幾つか見てみたい。なお、この間の両国関係は、テロ対策が中心であるので、時期は相前後するが、初めにテロ対策関連事項から述べる。

（1）ドイツ国内テロ対策での米国の貢献[40]

過去１０年以上、ドイツ国内でのテロ事件の殆どで、その防止や捜査に、NSA からの情報が貢献して来たと言う。その顕著な例が、2007 年 9 月のイスラム過激派ザウアーラント・グループによる大規模テロの防止である。

ザウアーラント・グループの中心は、イスラム教に改宗したドイツ人２人で、彼らはパキスタンのイスラム聖戦同盟（Islamic Jihad Union）の訓練キャンプに参加してテロの技術を学んだ。ドイツに帰国後、自動車爆弾による大規模テロを計画して、アメリカ人の集まるディスコ、ラムシュタイン米空軍基地、フランクルト空港などを標的にして、爆薬や信管その他爆弾の材料を入手して準備を進めていたところを検挙され、大規模テロが未然に防止された。

このテロ・グループの発見の端緒は、前年の 2006 年に NSA がパキスタンとドイツ間のＥメール通信を傍受したことであったとされる。

（2）「プロジェクト６」～CIA、BfV、BND の協力[41]

ザウアーラント・グループの検挙の前、欧州は、2004 年のマドリッド列車爆破事件、2005 年のロンドン地下鉄・バス爆破事件と、テロが相次いで騒然としていた。そのような情勢下の 2005 年に、テロ対策の「プロジェクト６」は開始された。NSA は直接の当事者ではないが、間接的に関与しているので紹介する。

報道によれば、「プロジェクト６」とはイスラム過激派の関係者データベースで、CIA、BfV、BND 三者の共同事業である。CIA が、他の国々でも成果が挙がっているとして導入を提案したもので、CIA がコンピュータとソフトウェアを提供したという。米国がシギントにより入手した中近東の過激派と連絡があるドイツ国内の電話番号等を提供し、ドイツ側はこれに基づいてドイツ国内の関連情報を収集してデータベースを

---

[40] Malanie Amann, et. al., “The German Prism: Berlin Wants to Spy Too,” *Spiegel Online*, 17 June 2013, accessed 6 August 2014, http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html

[41] Matthias Gebauer, et. al., “‘Project 6’: CIA Spies Operating in the Heart of Germany,” *Spiegel Online,* 9 September 2013, accessed 22 October 2013, http://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html

構築したものである。これによって、ドイツ国内のイスラム過激派容疑者とその関係者の解明が進められたものと見られる。ザウアーラント・グループの検挙にも貢献したと推定できよう。

このプロジェクトは2010年に終了したが、2012年にはNadis NWと呼ばれるBfVのシステムが稼働を開始し、「プロジェクト６」の機能はこちらに引き継がれたとされる。Nadis NWはBfVの他、１６の州憲法擁護庁もアクセスできるとされる。

なお、2012年中にBfVがテロ関係でCIA、NSA初め米国諜報諸機関に送付した情報件数は864件あり、他方米国から受領した情報件数は1830件であるという。

（３）テロ対策におけるNSAとBfV、BNDの協力強化[42]

ドイツ国内でのテロ防止の責務を第一次的に荷う組織は、所謂セキュリティ・サービス機能を果たす連邦憲法擁護庁BfVである。そのBfVとNSAとの協力関係強化の契機となったのが、先に述べたザウアーラント・グループの検挙である。

これを契機に、NSAとBfVは、BNDの協力も得て、徐々に協力関係を強化しており、情報分析協議を定例化し、ドイツ人・非ドイツ人の過激派の発見・追跡でもより緊密に協力するようになった。

また、BfVが国内で収集する通信データの検索分析処理を改善するため、NSAは支援を行っている。その一例が、XKeyscoreのソフトウェアの提供である。

2011年10月に、BfVが国内インターネット通信網から収集したデータを基に、国内のテロ容疑者をXKeyscoreソフトウェアで検索分析する実演を行った。XKeyscoreソフトウェアの特色は、メールアドレスやIPアドレス、或は対象者が不明でも、インターネット空間に於ける行動の特徴を分析することにより、未把握の過激派を発見することができるところにある[43]。BfVもその性能には魅力を感じたものと思われる。その後、BfV副長官からの正式な提供要請を受けて、NSAでは2013年3月に提供が正式

---

[42] 主な出典は、次のスノーデン資料である.
-- NSA, Information Paper, *NSA Intelligence Relationship with Germany – Bundesnachrichtendienst.*
--"Secret Documents on the cooperation between the NSA, BND and BfV in the fight against terrorism," *Spiegel Online*, 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/media/media-34046.pdf

[43] その方法は、行動探知技術（behavior detection techniques）と呼ばれている。これは、ネット上の特定の過激なウェブサイトに頻繁にアクセスしたり、爆弾の製造方法を教えている特定サイトの特定ファイルをダウンロードしたりするなど、特徴的な行動を行った者を検索抽出して、未把握の過激派を発見するものと考えられる。このような技法を使用するには、サイバー空間に於ける不特定の通信データを大量に取得保持していることが前提となる。最低でも、多数の特定サイトへのアクセス記録を取得保持していることが前提である。詳細は不明であるが、ドイツでもそのような収集をしているということであろう。なお、類似の発想のものに、第３部第１章の６カナダの項で見た「レビテーション」計画がある。

に決定された。なお、XKeyscore ソフトウェアの運用については、既に以前から提供を受けて取扱に習熟している BND が BfV を支援している。

また、これらの展開もあり、NSA は、2013 年 3 月にテロ対策で BfV との公式協力関係の樹立を決定した。テロ対策では、NSA と BND, BfV との三者の協力関係を更に強化していくこととしている。そのため、ドイツ側が NSA と BND、BfV の間の通信回線を改善して情報交換の迅速性を高めたとされる。また、NSA はテロ対策の分野で、BND と BfV と３ヶ月毎に協議会合を開催している。なお、欧州では他に、欧州シギント首脳会議 SSEUR の下にテロ対策連合（CT coalition）というテロ対策の下部組織が設置され、半年毎に協議会合を開催しているが、これにはドイツから BND が参加している。

（４）バード･アイブリング衛星通信傍受施設の移管と共同運用[44]

ア　バード・アイブリング施設の移管

バード･アイブリング施設は、元来ドイツ国内最大の NSA 施設で最盛期には 1800 人が働いていたという。任務は衛星通信の傍受で、そのため巨大なパラボラ・アンテナを９基運用していた。しかし、その重要性が相対的に低下したためか、2002 年には閉鎖の予定であった。ところが、9/1 1 事件の結果、閉鎖が 2004 年に延期され、更に 2004 年には NSA からドイツ BND に移管された。

現在、同施設で収集している衛星通信は、その傍受回線の性質から基本的に外国通信と看做されている。勤務している BND 職員は約 120 人で、技術、分析、管理の三部で構成されている。

イ　米独の共同運用

施設のドイツ移管後は、共同運用となった。移管の合意覚書が 2002 年 4 月に結ばれ、それによれば、主たる関心は、テロ対策、組織犯罪対策、大量破壊兵器拡散問題等である。また、ドイツ国民と米国民及び両国の法人は、収集対象にしないこととされている

---

[44] 主要な出典資料は次の通り。
--Hubert Gude, et. al., “Spying Together: Germany’s Deep Cooperation with the NSA,” *Spiegel Online,* 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html
--“German investigation of the cooperation between NSA and BND (Ⅱ),” *Top Level Telecommunications*, 16 December 2014, accessed 6 April 2015, http://electrospaces.blogspot.jp/2014/12/german-investigation-of-cooperation.html
--“German investigation of the cooperation between NSA and BND (Ⅲ),” *Top Level Telecommunications*, 13 January 2014, accessed 6 April 2015, http://electrospaces.blogspot.jp/2015/01/german-investigation-of-cooperation.html

が、例外として、テロ対策上必要で両国の合意がある場合、通信の一方当事者が国外にいる場合は収集できることとされていた[45]。

その結果、メタデータに関しては収集データの全件が NSA に提供され、コンテンツデータについては、2012 年、2013 年には、毎月約 300 万件が NSA に提供されたとされる[46・47]。

NSA は、2002 年の合意覚書に基づき、在独特別渉外活動（SUSLAG）を置き、この下部組織として、合同シギント活動（Joint Sigint Activity）と合同分析センター（Joint Analysis Center）を設置した。

後述する連邦議会 NSA 調査委員会に於ける証言によれば、合同シギント活動では、設備の多くは NSA が提供し、BND はそれを運用すると共に、取得データを米国に提供したという。データの流れは、BND 側から NSA 側への一方通行である。

但し、BND の公式の立場は、あくまで運用主体は BND であり、ドイツ法上問題の無いデータのみを米 NSA に提供したとしている。即ち、NSA の提示する電話番号やＥメールアドレスなどによるデータ要求に対して、BND 本部でその中にドイツ国民やドイツ企業が含まれていないかを確認し、もしこれらがあれば削除した上で、該当データを提供していると主張している。しかし、BND 本部による確認と統制は不十分なものであったという[48]。

---

[45] これは、スノーデン資料ではなく、シュピーゲル誌が独自に入手した資料によるとされる。Gude, et. al., “Spying Together: …,” *Spiegel Online.*

[46] 同上。

[47] BND の解釈では、バード･アイブリングに於ける衛星通信の収集は、国外に於ける収集と同様であり、国内法の規制は及ばない。但し、収集したデータがデータベースに保管されると個人情報保護法の適用対象になるというものとされている。“German investigation of the cooperation between NSA and BND (Ⅲ),” *Top Level Telecommunications.* この解釈によれば、データベースに保管前のデータの扱いは規制外であるので、米国 NSA にも制約無しに提供できると解釈できることとなるのではないかと考えられる。

[48] 2005 年、BND 職員が NSA からのデータ要求（所謂セレクター）の中に、ドイツも出資している欧州企業の EADS やユーロコプター、フランス政府職員が含まれているのを発見した。そのため、遅くとも 2008 年以降、NSA が提供するセレクターはそれを収集対象とする可否を BND 本部で点検するようになり、そこでドイツ関連のセレクターと認定して排除したものは、累計４万件に及ぶという。そして、スノーデン告発後の 2013 年 8 月、BND 本部で収集している NSA のデータ要求（所謂セレクター）を再点検したところ、2002 年合意覚書に違反する可能性のあるデータ要求約 2000 件が見過ごされていたことが判明したという。これらのデータ要求には、フランス政府職員や EU 機関や欧州各国政府に対するものがあった。そこで、BND 長官は 2013 年 11 月に新規則を定めて、BND のデータ要求には EU や欧州諸国関連のものを含めてはならない旨定めたとされる。なお、2015 年初め時点で、バード・アイブリング施設に対する NSA からのデータ要求は 460 万件であるとされる。
-- Von Maik Baumgärtner, et. al., “Überwachung: Neue Spionageaffäre erschüttert BND,” *Spiegel Online,* 23 April 2015, accessed 24 April 2015, http://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html

なお、この協力の一環で、2007 年以来 BND は、NSA の分析ツールである XKeyscore ソフトウェアの提供を受けている[49]。

合同シギント活動は 2012 年、合同分析センターも 2011 年に終了しているが、BND から NSA への衛星通信データの提供は、現在も継続している。

（５）「アイコナル Eikonal」作戦[50]

アイコナル作戦とは、米独協力による通信基幹回線からのデータ収集と分析事業である。NSA 側の位置付けは、「ランパート A」というサード・パーティと共同して行う事業（第２部第２章３の（４））に分類されている。ドイツ側の位置付けは、BND による一般の通信基幹回線からの国際通信データ収集（後述する「戦略的収集」）である。2004 年に開始されたが、2008 年 6 月に終了した。

データ収集は、ドイツ・テレコム社の協力を得て、フランクフルト近郊ニードの同社通信センター（switching center）で行われた。主たる情報関心はアフガニスタンとテロ対策である。そこで、ドイツ・テレコム社の通信センターにおいて、情報価値のありそうな国際通信回線を選択して、これに分配器（splitter）を設置してデータを取得し、更に「セレクター」によって必要データを選択する。この「セレクター」として登録された件数は数十万件とされるが、ドイツ側では法律で禁止されているドイツ国民のデータを収集しないように DAFIS というシステムを導入して、「セレクター」を点検して

-- Maik Baumgärtner, et. al., “America’s Willing Helper: Intelligence Scandal Puts Merkel in Tight Place,” *Spiegel Online,* 4 May 2015, accessed 14 May 2015, http://www.spiegel.de/international/germany/bnd-intelligence-scandal-puts-merkel-in-tight-place-a-1031944.html

--“German BND didn’t care much about foreign NSA selectors,” *Top Level Telecommunications,* 12 May 2015, updated 13 May 2015, accessed 14 May 2015, http://electrospaces.blogspot.jp/2015/05/german-bnd-didnt-care-much-about.html

[49] XKeyscore は、Ｅメールアドレスなどのストロングセレクターが無い場合でも、データの検索抽出に有効なソフトウェアである。その XKeyscore が能力を発揮するには、不特定且つ大量の通信データを取得保持していることが前提となる。従って、BND はそのようなデータを衛星通信傍受から得ているのは間違いがないと考えられる。

[50] “German investigation of the cooperation between NSA and BND (Ⅲ),” *Top Level Telecommunications*.

--Von Georg Mascolo, Hans Leyendecker and John Goetz, “Codewort Eikonal – der Albtraum der Bundesregierung,” *Sueddeutsche Zeitung*, 4 October 2014, accessed 30 March 2015, http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432

--“New details about the joint NSA-BND operation Eikonal,” *Top Level Telecommunications*, 28 May 2015, accessed 1 June 2015, http://electrospaces.blogspot.jp/2015/05/new-details-about-joint-nsa-bnd.html

問題のあるものは排除していた。「セレクター」により選択された収集データは、バード・アイブリングの合同シギント活動に送信された。

この共同事業によって、ドイツ側には、アフガニスタンでのドイツ軍防護やテロ対策のインテリジェンスで成果があり、また、NSA から進んだ装置や技術を得ることができたという。これに対し NSA 側では、取得した有効なデータ（国際電話、E メール、ファックス等）件数は年間 500～700 件に過ぎず、NSA は大いに失望したという。更に、システム上ドイツ国民の通信が確実に除去される確証が無かったので、BND はこのアイコナル作戦を 2008 年に終了させたという。

アイコナル作戦の終了に際しては、怒った NSA 副長官がベルリンに来訪して代償措置を要求したため、BND は NSA に対して欧州外でのデータ収集の共同事業を提案したという。

（６）ドイツによるサイバー諜報の強化と米独関係の緊密化

米独間では、今まで見てきたように、インターネット空間におけるインテリジェンス協力が進展していたが、当然、その背景には、ドイツ自身によるサイバー空間におけるシギント強化の動きが見られる。

ア　戦略的収集（strategic collection）[51]

インターネット通信については、フランクフルトには DE－CIX という世界最大のインターネット相互接続点ＩＸが存在しており、そこには欧州各地の通信が集中して経由するだけではなく、ロシアや東欧、中近東や南アジア、更にはアフリカとのインターネット通信も経由している。

ドイツでは、この様に欧州大陸に於ける国際的なインターネット通信の中枢であることを活用して、BND がインターネット通信からのデータ収集、所謂、戦略的収集（strategic collection）を行っている。そして、BND は、法令によりドイツを経由する外国間のインターネット通信の２０％を取得することが認めら、通信事業者にはこれに協力する義務が課されている。

具体的なデータ収集の方法は、NSA や UKUSA 諸国が包括的な取得を基本とするのに対して、選択的である。先ず、データの収集対象とする回線は、アフガニスタンとかパキスタンとか出発地や経由地、行き先地から判断して対象を定め、更にその中でも情

---

[51] Melanie Amann, et. at., “The German Prism: Berlin Wants to Spy too,” *Spiegel Online,* 17 June 2013, 6 August 2014,
http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html
--“German investigation of the cooperation between NSA and BND (Ⅲ),” *Top Level Telecommunications*.

報価値のありそうな特定回線を選んで収集している。収集では運営会社とも協議しているという。

次に、特定回線からのデータ取得の方法についても、米国 NSA など UKUSA 諸国のシステムは、先ず大量に取得して、記憶装置に記録した上で XKeyscore などの種々の検索分析ツールを使って必要な通信を検索抽出する方式をとっているが、ドイツでは、当初からセレクターに合致したもののみを選択的に抽出しているという。例えば、2011 年には BND は１万６千件以上のセレクターを使用したとされるが、その内９０％以上は所謂ストロングセレクターであり、電話番号や携帯端末識別番号、Ｅメールアドレス、IP アドレス、MAC アドレス等である。ドイツ国民の通信は取得してはいけないことになっているので、ドイツを示す国際電話番号やメールアドレス等を持つ通信は、抽出対象から自動的に除外されるという。

これに加えて、最近は通信内容に対するキーワード検索も可能となってきており、基幹回線からの抽出検索の仕方が、より情報価値のある可能性のある通信に絞り込めるようになってきたという。その結果、BND が分析対象として検索抽出したＥメールの数は、2010 年が 3700 万件であり、到底処理できない分量であったものが、2011 年 290 万件、2012 年 90 万件と減少してきているとされる[52]。

これらのデータを分析して作成する情報報告書は、現在、一日平均約２０件であるとされる。

なお、2012 年では、BND が検索抽出対象とした通信量は、法令で認められた２０％に及ばず、全通信の５％以下であるという。

イ　予算の増額要求[53]

2012 年連邦議会の秘密委員会で、BND 長官は、１億ユーロと 100 人の人員を要する５ヵ年計画を説明して予算要求をしたという。但し、その詳細は不明である。

ウ　サイバーインテリジェンス部の新設

BND の中でシギント担当の技術偵察局（TA 局）は、従来、収集部、分析部、暗号解析部の３部で構成されていたが、これに最近[54]、サイバーインテリジェンス部が新設された。同部は、サイバー生産、サイバー技術、サイバー作戦の三つの課で構成されている。課の細部構成の中には、コンピュータ・ネットワーク開拓（CNE）だけでなく、コンピュータ・ネットワーク防禦（CND）部署もあり、サイバーインテリジェンスに関

[52] 抽出件数の推移から判断して、この収集方法が開始されたのは近年のことと考えられる。
[53] Amann, et. at., “The German Prism: Berlin Wants to Spy too,” *Spiegel Online.*
[54] 部の新設時期は明確でないが、2011 年頃ではないかと推定される。

して幅広い任務が与えられているのではないかと推定できる[55]。定数 150 人のところ 2013 年 4 月時点で 130 人以上が充足され、残すところは所謂「ハッカー」であるが、これはまだ募集中であったという[56]。

エ　米独関係の緊密化

2013 年 4 月末には、米独のシギントに関する戦略計画協議があり、NSA 内部資料[57]によれば、そこでは両組織間の幅広い問題の議論が予定されていた。これは第 3 回目の協議であり、2011 年に開始されたと見られるが、斯かる協議の定例化が進むなど、協力関係の深化が伺われる。

なお、ドイツでは、BND がサイバー防衛センターを設置したり、連邦情報セキュリティ庁 BSI がボンに国家サイバー防衛センターを設置したりするなど、関心が高まっており、そこで、NSA としては、この会合ではコンピュータ・ネットワーク防禦（CND）へのシギントの関与について、NSA の技術[58]を含めて提示する用意があるとしている。このように、コンピュータ・ネットワーク防禦（CND）が重要議題となってきているのは、他のサード・パーティ諸国の場合と同様である。

また、シギントに関する米独協力では、閣僚級でも関係が緊密化し、これより 1 年前の 2012 年 1 月にはドイツのフリッチェ内務大臣が NSA 長官と会談し、スカイプ通信の傍受への協力要請をしている。更に、2013 年 6 月にはアレクサンダーNSA 長官（当時）が訪独して、政府要人とシギント協力について協議するなど、協力の緊密化が進んでいた。

ところが正に、アレクサンダー長官が訪独している最中に、スノーデンによる告発と内部資料の漏洩が始まり、この後、両国関係は波乱含みとなって行くのである。

55　ス資料、NSA, “Internal NSA presentation on the BND's organization,” *Spiegel Online,* 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/media/media-34050.pdf

56 ス資料、NSA, *Talking Point Topics Proposal,* (circa April 2013), accessed 20 June 2014, http://www.spiegel.de/media/media-34119.pdf

57　ス資料、”Briefing on the visit to the NSA of a high-ranking BND official,” *Spiegel Online,* 18 June 2014, accessed 20 June 2014, http://www.spiegel.de/media/media-34117.pdf
--ス資料、NSA, *Talking Point Topics Proposal.*

58　米国の CND では、NSA の TUTELAGE というシステムが重要な役割を果たしており、上記内部資料では、これについてドイツ側に説明することとなっていた。

５　スノーデン告発後の米独関係

2013 年 6 月のスノーデン告発を契機として、ドイツでは NSA によるシギント活動更には米国によるインテリジェンス活動に対して、世界の諸国の中でも世論の関心が大きく盛り上がった。その要因は、第１に、ドイツでは過去にヒットラー・ドイツと東ドイツという二つの体制において、国民が極めて強力な秘密警察・諜報機関の監視下に置かれた経験があり、国民がプライバシーや個人情報の保護について強い関心を持っていること挙げられる。第２に、スノーデンが NSA 内部資料を提供した１人にローラ・ポイトラスという米国人がいるが、彼女はドイツ・ベルリンに居住しており、彼女がシュピーゲル誌と共同して報道キャンペーンを展開してきたため、ドイツでは本件に関する報道量が極めて多いことが挙げられる。シュピーゲル誌による報道量は、ガーディアン、ワシントンポスト、ニューヨークタイムズの各紙を遥かに凌駕している。

これらの要因が相俟って、NSA の諜報活動に関する国民の関心が高いものと見られるが、米国では、ドイツに於けるこれらの事情が十分理解されていない嫌いがあり、それがスノーデン報道後の両国関係に軋轢を齎している。この米独関係について見てみたい。

（１）「ノー・スパイ合意」への取組

2013 年 6 月のスノーデンによる NSA 告発と内部資料漏洩を受けて、ドイツではシュピーゲル誌を中心に多量の報道がなされ、ドイツの歴史的経験も相俟って、NSA による対独諜報活動が政治問題化した。そして、同年９月末の総選挙を控え、この問題がメルケル政権への攻撃材料となることが危惧されたのである。

斯かる状況下、メルケル首相は、米国との間でノー・スパイ合意（相互スパイ禁止合意）締結に向けて取り組むと表明して、ドイツ国民の個人情報保護のため全力を尽くす姿勢を見せ、本問題が総選挙の争点となることを回避した[59]。

そして、これと相前後して、ドイツの内務省と司法省は、米国政府に対して、ドイツ国内に於ける米国の諜報活動に関する詳細な質問表を送付したが、法的規制や手続に関して機密指定を解除された大量の資料を得ただけで、内容のある回答は何も得られなかったという。

また、ノー・スパイ合意に関しても、全く進展はなかったという。ノー・スパイ合意に対する米国の拒否姿勢は明確であり、オランド仏大統領が、2014 年 2 月上旬米国を

---

[59] Veit Medick and Annett Meiritz, "'The Americans Lied': Trans-Atlantic 'No-Spy' Deal on the Rocks," *Spiegel Online*, 15 January 2014, accessed 23 March 2015, http://www.spiegel.de/international/germany/us-german-no-spy-deal-in-danger-of-failure-a-943614.html

国賓として訪問した際にもオバマ大統領はこれを拒否したと報道されている[60]。オバマ大統領は、その際の共同記者会見でも「米国がノー・スパイ合意を結んでいる国は存在しない」と発言している[61]。こうして、2014 年に至っても、ノー・スパイ合意に関しては何の進展もみられなかったが、その間の 2013 年 10 月には、次に記載する二つの件での軋轢が生じた。

（２）メルケル首相の電話盗聴と在独米英大使館のシギント活動の問題

ア　メルケル首相の電話盗聴問題

メルケル首相は「携帯首相」と渾名される程、携帯電話を多用する政治家であるが、独誌シュピーゲルが、NSA 内部資料を分析して、メルケル女史の携帯電話番号が収集標的として記載され、且つその任務が特別収集サービス（SCS）に付与されているのを発見した。同誌は 2013 年 10 月 10 日これを首相府に通告した。独政府は、連邦諜報庁 BND と連邦情報セキュリティ庁 BSI による調査を行い、これを真実であると判断した。そこで、独首相府は米ホワイトハウスと遣取りをしたが、必ずしも満足いく結果を得られなかったという。

そのため、メルケル首相は 10 月 23 日にオバマ大統領に直接電話をし、信頼関係の大きな侵害であると抗議し、且つ、諜報機関の活動と協力関係について明確な相互取決（ノー・スパイ合意）を定めるよう要求した。これに対し、オバマ大統領は、「メルケル氏の携帯電話傍受は知らなかった。知っていればさせなかった。現在、メルケル氏の電話は傍受されていないし、将来も傍受することはない。」旨応えたと報道されている[62]。

イ　在独・米英大使館からのシギント活動問題

ドイツ誌シュピーゲルは、続いて、NSA による米国大使館からのシギント活動、特

---

60 Hubert Gude, et. al., “Striking Back: Germany Considers Counterespionage Against US,” *Spiegel Online,* 18 February 2014, accessed 21 February 2014, http://www.spiegel.de/international/germany/germany-considers-counterespionage-measures-against-united-states-a-953985.html

61 US, Office of the Press Secretary of the White House, *Press Conference by President Obama and President Hollande of France,* (11 February 2014), accessed 25 March 2015, https://www.whitehouse.gov/the-press-office/2014/02/11/press-conference-president-obama-and-president-hollande-france

62 Jacob Appelbaum, et. al., “Berlin Complains: Did US Tap Chancellor Merkel’s Mobile Phone?” *Spiegel Online,* 23 October 2013 accessed 24 October 2014, http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html

--Ian Traynor, Philip Oltermann and Paul Lewis, “Angela Merkel’s call to Obama: are you bugging my mobile phone?” *The Guardian*, 24 October 2013, accessed 24 October 2013, http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german

別収集サービス（SCS）について関連報道を開始した[63]。報道では、（収集用の受信装置を格納したと見られる）大使館屋上の構造物の写真も添付されていた。更に、11 月に入り、大使館からの情報収集には、英国大使館も参加しているとの報道が続いた[64]。これも屋上構造物の写真付であった。

これらに関して、ドイツ政府は、外交関係に関するジュネーブ条約違反であるとして抗議したと報道されている[65]。

その結果かどうかは明確ではないが、2013 年 11 月中には、米大使館屋上の構造物の表面温度が大幅に低下しており、構造物内部での活動が停止されたと見られる[66]。また、英国大使館屋上の構造物は、2014 年 7 月までに撤去されたという[67]。

ウ　2014 年 1 月の大統領政策指令発出

これらの米独関係や、米国内での議論を背景に、2014 年 1 月 17 日、オバマ大統領は、シギント活動の見直しに関して演説[68]を行った。同大統領は、連邦議会に対してシギント活動に関する法制度について改革案を提示すると共に、同日シギント活動に関する新たな大統領政策指令[69]を発しシギント活動に一定の制約を課した旨表明した。

---

[63] Jacob Appelbaum, et. al., "The NSA's Secret Spy Hub in Berlin," *Spiegel Online,* 27 October 2013, accessed 28 October 2013,
http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html
--Von Konrad Lischka and Matthias Kremp, "NSA-Spaehskandal: So funktionieren die Abhoeranlagen in US-Botschaften," *Spiegel Online,* 28 October 2013, accessed 12 Novenber 2013,
http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaehskandal-so-funktionieren-die-abhoeranlagen-in-us-botschaften-a-930392.html

[64] "Et Tu, UK? Anger Grows over British Spying in Berlin," *Spiegel Online,* 5 November 2013, accessed 6 November 2014,
http://www.spiegel.de/international/europe/revelation-of-spy-nest-in-british-berlin-embassy-angers-germans-a-931868.html

[65] Medick and Meiritz, "'The Americans Lied':...," *Spiegel Online.*

[66] Duncan Campbell, "British embassy spying," *Duncan Campbell. Org,* undated, accessed 27 October 2014, http://www.duncancampbell.org/british-embassy-spying

[67] Melanie Amann, et. al., "Keeping Spies Out: German Ratchets Up Counterintelligence Measures," *Spiegel Online*, 22 July 2014, accessed 23 July 2014,
http://www.spiegel.de/international/world/germany-increases-counterintelligence-in-response-to-us-spying-a-982135.html

[68] US President Obama, *Remarks on Review of Signals Intelligence,* 17 January 2014, accessed 16 January 2015,
http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[69] US Presidential Policy Directive/PPD-28(Signal Intelligence Activities), 17 January 2014, accessed 16 January 2015,

同大統領政策指令によれば、対外関係では、今後は「説得力ある国家安全保障上の必要が無い限り、米国の親密な友人や同盟国の政府首脳の通信は傍受しない」こととされた。これに関連して、NSA 広報官は、数十人（dozens）の外国首脳は対象から除外されたと述べたという[70]。

更に、同演説と同指令では、外国関係では次の内容が定められている。

- 米国は、正当な国家安全保障の目的のみにシギントを使用する。
- 米国は、批判や反対を抑圧するためにシギント活動をしない。民族、人種、性別、宗教等に基づいて不利益を及ぼすようなシギント活動をしない。米国企業や米国の商業部門に対して競争力を付加するようなシギント活動をしない。
- 米国は、米国の国家安全保障を脅かさない一般人の情報を収集しない。
- 司法長官と国家諜報長官に対して、国外の人々にも一定の保護を与えるべく、情報の保管期間や情報配布の制限などの保護措置を定めるように指示した。

米国としては、これらの措置によって、ドイツを含む友好国や同盟国を納得させる積りであったのであろうが、明らかにドイツは納得しなかったようである。それは次の事件となって表面化する。

（3）CIA のスパイ摘発と在独 CIA 代表の追放

ア　BND 内スパイの摘発

2014 年 7 月 2 日 BND 職員マルクス・R（31 才）が CIA のため情報を提供していたとして逮捕され、7 月 4 日に公表された。

報道[71]によれば、摘発の端緒は、同人の不用意な行動である。同人は、同年 5 月 28 日にミュンヘン所在のロシア領事館に情報協力をしたいとＥメールを送付したが、これ

---

http://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

[70] Ellen Nakashima and Barton Gellman, “Court gave NSA broad leeway in surveillance, documents show,” *The Washington Post,* 30 June 2014, accessed 3 July 2014, http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html

[71] Nikolaus Blome, et. al., “Hunting American Spooks: Germany Prepares Further Spying Clampdown,” *Spiegel Online,* 14 July 2014, accessed 15 July 2015, http://article.wn.com/view/2014/07/14/Hunting_American_Spooks_Germany_Prepares_Further_Spying_Clam/

--Maik Baumgaertner, et. al., “Spiraling Spying: Suspected Double Agent Further Strains German-US Ties,” *Spiegel Online*, 9 July 2014, accessed 11 July 2014 http://www.spiegel.de/international/germany/arrest-of-bnd-employee-strains-ties-between-germany-and-us-a-979738.html

--Dan Roberts, Spencer Ackerman and Philip Oltermann, “White House on the back foot over CIA role in German spying scandal,” *The Guardian,* 7 July 2014, accessed 8 July 2014, http://www.theguardian.com/world/2014/jul/07/white-house-response-german-spying-scandal

が同領事館を監視していた連邦憲法擁護庁 BfV の傍受するところとなった[72]。そこで、BfV から通報を受けた BND の内部監査部署が追及し、更に連邦検察庁と連邦刑事庁による捜査に発展して検挙に至った。ところが、調査の過程で、同人が使用するＧメール・アカウントについて、独インテリジェンス機関が米国インテリジェンス機関に照会をした[73]ところ、回答が無いばかりか同メール・アカウントの使用が停止され、不審を招いたという。そして、実際、７月２日に同人の居宅等を捜索したところ、そのパソコンには秘密通信用の暗号ソフトが搭載され、且つ BND の機密文書 218 件入りの USB メモリーも押収された。

本人の供述によれば、同人は、２年程前から CIA の情報協力者となっており、切掛けは（ロシア領事館に対すると同様に）同人がベルリン所在の米国大使館にＥメールで協力を申し出たことである[74]。その後 CIA 職員２人と接触し、この間情報提供の見返りに約２万５千ユーロの報酬を得ていたという。CIA 職員は、在オーストリアの米国大使館に勤務しており、オーストリアからマルクスを運営していたのである。

なお、マルクスは、BND の EA 局（在外 BND 機関員との連絡及び渉外担当部署）に勤務しており、BND の活動全般に関する機密文書にアクセスできる地位にいたとされる。マルクスによる漏洩資料には、連邦議会に設置された NSA 委員会関係資料も含まれていたという。

イ　国防省内スパイ容疑者の摘発

続いて 2014 年 7 月 9 日には、国防省職員レオニド・K（37 才）が、CIA のために情報を漏洩していた容疑で、家宅捜索を受けると共に、取調べを受けた。

報道[75]によれば、同人は国際安全保障関係の専門家であるが、2010 年頃から、米国インテリジェンス機関への協力が疑われており、連邦憲法擁護庁 BfV と軍保安局 MAD の監視対象になっていたという。この間、同人は、米国インテリジェンス関係者と見られる者と会うため数回に亘りトルコ・イスタンブールに渡航したり、同米国人から２千

---

72 ドイツでは、ロシア等の大使館や領事館が防諜或は対外諜報目的で連邦憲法擁護庁の監視対象となっており、大使館へのＥメールも常時監視されているということである。セキュリティ・サービスを有する国の標準的なインテリジェンス活動である。なお、ドイツに於ける外国公館監視の一般的手法としては、電話とＥメールの傍受、大使館職員のリクルート、航空写真を含む観察が挙げられている。
--Baumgaertner, et. al., “Spiraling Spying…,” *Spiegel Online*.

73 マルクスがＧメールで遣り取りした履歴・内容は、グーグルのデータセンターに記録されているため、ドイツ当局は米国当局に対してそのメールの履歴・内容データの提供を要請したのではないかと考えられる。

74 米国大使館が連邦憲法擁護庁の監視対象ではなかったので、米国大使館宛のＥメールは監視されておらず、そのため、マルクスによる米国大使館に対する接近が把握できなかったということである。

75 Blome, et. al., “Hunting American Spooks: …,” *Spiegel Online.*

ユーロの送金を受けたりしていたという。

そして同人の電話は傍受対象になっていたが、2014 年 2 月を最後に米国人との連絡が途絶え、更に、既述した BND 内スパイ、マルクスの家宅捜索において、その所持品内から、連邦憲法擁護庁が BND に対してレオニドについて照会した文書が発見されたという。

そこで、レオニドの家宅捜索や取調べとなった訳であるが、同人は、米国のスパイであることを頑強に否定し、且つ、家宅捜索からはスパイ容疑を立証する証拠が発見されなかった。そのため、同人は逮捕されておらず、捜査も進んでいない。証拠が発見されなかったのは、マルクスからの通報で、レオニドが証拠物を破棄したためではないかと疑われているという。

ウ　ドイツ政府による圧力

斯かる状況下、2014 年 7 月 7 日には、内務大臣が外国諜報機関による対独活動については、全方位対策が必要である旨を述べた。また同日、内務省報道官も「全方位の効果的な防諜活動が重要であり、改革の必要がある」と述べて、米国による諜報活動を連邦憲法擁護庁の監視対象とすることを示唆した。

また、ドイツ政府は、6 月下旬に米企業ベライゾンと独政府のインターネット回線サービス契約（2015 年迄）を更新しないと発表したが、その理由について、内務省報道官は、ベライゾン社は、法律により NSA に対して一定のものを提供するように義務付けられているようであることが、理由の一つであると語っている[76]。

エ　米独間の調整の停滞[77]

上記事件、特にマルクスのスパイ事件を受けて、米独間では、CIA 長官や駐独大使が関与して調整が行われたが、米国の対応はドイツにとっては全く不本意なものであったという。

即ち、先ずブレナン CIA 長官がドイツ首相府のフリッチェ諜報活動統括官と協議したが、ブレナン長官は、BND 職員のスパイとしての CIA による運営自体を認めなかったとされる。

また、米国のエマーソン駐独大使がシュタインマイヤー外務大臣と会談したが、ここでも米国からの謝罪も無く捗々しい進展も見られなかったとされる。

オ　駐独の CIA 代表の事実上の追放[78]

---

[76] Andrea Peterson, “German government to drop Verizon over NSA spying fears,” *The Washington Post*, 26 June 2014, accessed 30 June 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/06/26/german-government-to-drop-verizon-over-nsa-spying-fears/

[77] Blome, et. al., “Hunting American Spooks:…,” *Spiegel Online.*

そこで、2014 年 7 月 10 日、連邦憲法擁護庁長官が CIA 代表を召喚して、直接同人に、国外退去を勧告した。駐独の CIA 代表とは、即ち、米国の諜報コミュニティの代表であり、米国諜報コミュニティ代表の国外退去措置は、友好国間では極めて異例である。第２次世界大戦後初めての事例ではないかと思われる。

ドイツ政府として、米国による対独諜報活動がドイツに於いて極めて深刻な問題であることが米国では十分認識されていない、そこで、この問題について何らかの進展を図るには、相当の強いメッセージを米国政府に対して送る必要がある、と判断したと見られる。

カ　米大統領首席補佐官のドイツ派遣と対話の開始[79]

米国政府は、この CIA 代表の事実上の追放により、漸く問題の深刻さを理解したようであり、オバマ大統領はメルケル首相と電話で話した後に、マクドノー大統領首席補佐官をドイツに派遣した。

７月２２日、マクドノー首席補佐官はドイツのアルトマイヤー官房長官と長時間の協議の後、両国の（インテリジェンス活動について）協力の指針を定めるための対話を開始することで合意をした。

従来、米国は、UKUSA 諸国以外の国とインテリジェンス活動についての特別の合意を結ぶ先例を作りたくないとして、このような合意制定については消極的であった。他方、ドイツは、ノー・スパイ合意の締結を要求してきたが、それは米国が決して受け容れないことが明確であるので、ドイツ国内の外国人やテロ容疑者を米国の諜報対象としないことまでは無理としても、ドイツの政治家や諜報機関を諜報対象とすることを禁止する合意を得たいと考えている模様である。

その後、この対話の進行状況に関する報道は見られないが、事の性質上、合意が形成されたとしても、その内容が公表されることはないであろう。

（４）連邦議会 NSA 調査委員会の活動

2014 年 3 月、連邦議会に NSA 調査員会が特別に設置され、NSA 関連の調査を開始

---

[78] Matthias Gebauer, “Germany Asks CIA Official to Leave Country,” *Spiegel Online,* 10 June 2014, accessed 11 June 2014, http://www.spiegel.de/international/germany/germany-asks-top-cia-official-to-leave-country-a-980372.html

[79] Paul Lewis, “US and Germany hold restorative talks after series of spy scandals,” *The Guardian*, 22 July 2014, accessed 23 July 2014, http://www.theguardian.com/world/2014/jul/22/us-germany-restorative-talks-spy-scandals -- US, Office of the Press Secretary, *Readout of the Chief of Staff's Meetings in Berlin, Germany,* 22 July 2014, accessed 24 March 2015, https://www.whitehouse.gov/the-press-office/2014/07/22/readout-chief-staff-s-meetings-berlin-germany

した。委員は与野党の議員８人で構成され、委員長はゼンスブルグ議員である。

委員会は、関係者や専門家 100 人以上からのヒアリングを行う予定であり、最終報告書の提出は 2016 年後半と見込まれている。ヒアリングは、公開部分と非公開部分とからなり、非公開部分では機密資料や機密情報も提供されている。ヒアリングの議題としては、NSA 活動、NSA と BND の協力関係、UKUSA 諸国の活動の順とされている。NSA と BND の協力関係に関しては、BND 職員からヒアリングを受けており、その中には相当機微な内容も含まれている[80]。この委員会による調査の進展によっては、今後、注目すべき情報が開示される可能性がある。

但し、同委員会の運営では、既に種々波乱が起きている。

先ず、同委員会の発足当初、スノーデンの召喚を野党委員が強く要求したため、召喚するか否かで相当揉めた経緯がある。これは、ドイツ政府が同人への査証発給を拒否したため、召喚されなかった。ところが、この査証発給拒否については、2015 年 3 月に至り、副首相のガブリエル氏（連立与党・社会民主党党首）が、米国政府による圧力による旨を述べて注目を集めるところとなった[81]。

また、同委員会の委員の一人は、携帯電話を点検してもらったところ、第三者に浸透されていたのが発見されたほか、その他にも不審な動向が見られたという。そのため、同委員会のゼンスブルグ委員長は、委員会室の盗聴防止策ほか情報セキュリティ対策を取ると共に、委員には自分達自身が諜報対象となっている可能性について注意を喚起して、委員用の暗号付き携帯電話を準備したという[82]。

更に、2015 年春には、BND が委員会に機密資料を提供し続けるならばドイツとテロ対策での協力を停止するとの通告を英国 GCHQ から受けた[83]とか、或は、BND が提

---

[80] "German investigation of the cooperation between NSA and BND(1)," *Top Level Telecommunications,* 23 November 2014, accessed 25 November 2014, http://electrospaces.blogspot.jp/2014/11/german-investigation-of-cooperation.html

[81] 副首相のガブリエル氏は、査証発給拒否に関連して、仮にスノーデンを召喚して同人がドイツに入国すれば、犯罪人引渡協定に基づき米国に引き渡す義務があるため出来なかったと述べた。しかしその後、ジャーナリストのグリーンワルド氏が（亡命を認めれば引き渡す義務が無くなるので）なぜ亡命を認めないのかと尋ねたところ、副首相は、亡命を認めたら、米国はドイツとのインテリジェンス協力を停止するとしており、テロを未然に防止する情報を入手できなくなるからであると述べたという。但し、グリーンワルド氏は、この理由付けは、独政府内でスノーデン召喚に反対する者が、米国 NSA と共謀して作り上げたストーリーである可能性もあることを示唆している。
--Glenn Greenwald, "US Threatened Germany over Snowden, Vice Chancellor Says," *The Intercept*, 19 March 2015, accessed 20 March 2015, https://firstlook.org/theintercept/2015/03/19/us-threatened-germany-snowden-vice-chancellor-says/

[82] Blome, et. al., "Hunting American Spooks:…," *Spiegel Online.*

[83] "NSA-Ausschuss: Britischer Geheimdienst will Zusammenarbeit mit BND stoppen," *Spiegel Online*, 5 February 2015, accessed 1 April 2015, http://www.spiegel.de/politik/deutschland/gchq-britischer-geheimdienst-will-bnd-zusammen

出していなかった機密資料の存在が発覚する[84]などしており、委員会運営での波乱が続いている。

今後の委員会の展開が注目される。

arbeit-aufkuendigen-a-1016933.html

[84] Von Annett Meiritz, "Aufklaerung der Spaehaffaere: BND gibt Akten-Schluderei zu," *Spiegel Online,* 5 March 2015, accessed 1 April 2015, http://www.spiegel.de/politik/deutschland/nsa-affaere-bnd-versaeumte-lieferung-von-hundert-dokumenten-a-1021799.html

終わりに

米国 NSA の実態について、そのシギント戦略、シギント収集態勢、収集分析活動、サイバー作戦、そしてセカンド・パーティ、サード・パーティとの関係など各種の観点から分析してきた。

ここで判明したのは、NSA が、米国の国益のため必死にシギント力を磨いている姿である。即ち、そのシギント戦略にも記載されているように、「シギント技術の向上と自動化を進めて、世界ネットワークに対する支配を劇的に拡大する」、そして、「必要なシギント・データを誰からでも、何時でも、何処からでも獲得する」ということが、単なる題目ではなく、本当の実践目標として、膨大な資源を投入して、日々取り組んでいる姿である。また、英国初め UKUSA 諸国は、これに積極的に参加協力して、その諜報力の配分に与っている。

国益増進のためシギントやインテリジェンスに必死に取り組んでいるのは、独り、米国や UKUSA 諸国に限られない。当然、中国、ロシア、北朝鮮、韓国を初めとする諸国も、技術的には米国を手本に、そして、法律的にはより少ない制約の下、或は全く制約無しに、国益のため必死に取り組んでいるのである。米国と異なるのは、今回のスノーデンのようにその実態を暴露告発する者がいないことだけなのである。

嘗て、某氏が述べたように「戦時に国益を賭けて戦うのが軍隊であり、平時に（おいても）国益を賭けて戦うのがインテリジェンスである」。　世界の諸国は、平時にもインテリジェンスの矛と盾を磨き、戦っているのである。

他方、我が国を見ると、第二次世界大戦に於ける敗北以来、「米国の平和」の内に安住して、世界のパワーポリティクスへの参加を免除され、軍事やインテリジェンスから目を背けてこれらを直視しない文化が出来上がってしまった。そうしている間に、ナイーブで幼稚な空想的平和主義の言語思想空間にどっぷりと漬かって、これが蔓延し血肉化され、国際政治が国益を賭けた戦いの場であることさえ直視しない、直視できない者が大多数となってしまった。正に、国政政治面でのガラパゴス化現象と言えよう。筆者は、我が国の所謂、軍事やインテリジェンスについての有識者を自認する者でさえ、どれだけ本当に軍事とインテリジェンスを理解しているか疑問を感じる時がある。

我が国情を見ると、近い将来、我が国に真当なインテリジェンス諸機関が設置される可能性は極めて低いと考えざるを得ない。NSA 並みの組織はおろか、英国、豪州或はドイツ並みのインテリジェンス機関の設置も不可能であろう。しかし、インテリジェンスの関係者、或はインテリジェンスに関心を持つ者は、少なくとも、諸外国のインテリジェンスの実態を理解すること位は必要であろう。そのため、本研究が、真のインテリジェンス理解に僅かでも資することが出来れば幸いである。

附録　スノーデンによる告発の背景

エドワード・スノーデンによる情報漏洩は、米国インテリジェンス史上、最大のものである。そこで、何故、スノーデンが大量の機密資料を漏洩してまで告発するに至ったのかについて、同氏の各種インタビュー、グリーンワルド、ハーディング両氏による著作、各種報道を基に記述したい[1]。

---

[1] 主たる参考文献は次の通り。
--Edward Snowden, interview by Glenn Greenwald and Ewen MacAskill on 6 June 2013, *The Guardian*, 10 June 2013, accessed 12 July 2013, http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
--Edward Snowden, interview by Glenn Greenwald and Laura Poitras on 6 June 2013, *The Guardian*, 9 June 2013, accessed 12 June 2013, http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video, http://www.theguardian.com/world/video/2013/jul/08/edward-snowden-video-interview.
--Edward Snowden, interview by Glenn Greenwald, *The Guardian,* 17 June 2013, accessed 18 June 2013, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.
--Edward Snowden, interview by Barton Gellman, *The Washington Post,* 24 December 2013, accessed 25 December 2013, http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations...
--Edward Snowden, interview by NBC TV, 29 May 2014, http://www.theguardian.com/world/video/2014/may/29/edward-snowden-nbc-interview-video.
--Edward Snowden, interview by Alan Rusbridger and Ewen MacAskill, *The Guardian,* 18 July 2014, http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.
--Edward Snowden, interview by James Bamford in June 2014, *Wired magazine*, August 2014, accessed 18 August 2014, http://www.wired.com/2014/08/edward-snowden.
--Glenn Greenwald, *No Place to Hide* (London: Hamish Hamilton, 2014) 1-89.
--Luke Harding, *the Snowden Files* (New York: Vintage Books, 2014).
--Suzanna Andrews, Bryan Burrough and Sarah Ellison, "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair,* May 2014, accessed 9 January 2015, http://www.vanityfair.com/politics/2014/05/edward-snowden-politics-interview.
スノーデンの経歴や取材経緯に関しては、上記資料中、最後の Vanity Fair の記事が、相対的に正確でバランスが取れているように見える。

ところで、筆者は、このような告発と資料漏洩が生れてくる社会的背景には、米国社会に特有の幾つかのイデオロギー（支配的な正統思潮）の間の相克が存在すると考える。現代の米国社会は、ピルグリム・ファーザーズの建国神話を基礎としながら、次の三つのイデオロギー要素からなっていると考える。即ち、

① アメリカ革命イデオロギー（神から与えられた固有の人権を守るため、英国王の圧制に反抗して革命を成し遂げ、社会契約により米国民主主義国家を建設したというイデオロギー）
② 資本主義イデオロギー（自由競争による富の獲得。アメリカン・ドリームの実現）
③ 指導国家イデオロギー（民主主義と自由主義経済の指導国家（＝「覇権国家」）として、世界を導く使命があるというイデオロギー）

この三者は、対立の種を宿しながらも、基本的には、互いに補強し合い、総体として米国社会を支配し、支えているイデオロギーである。

これに対して、スノーデンは、この内の「アメリカ革命イデオロギー」の影響を特に強く受けたものと考えられる。「アメリカ革命イデオロギー」の視点のみに立てば、スノーデンが主張するように、本人は米国民主主義の信奉者にして愛国者であり、告発は愛国的行動であるということになろう。

これに対し、上記イデオロギーを総合的に捉える立場に立てば、世界の指導国家として9/11テロ事件を初め国際テロの脅威に晒されている状況下に、諜報機関が大統領の指揮命令を受け実施しているシギント活動、ましてその予算と主要事業は連邦議会の情報特別委員会で審議了承を受けているものであり、その正当性に問題はないということになる。更に、米連邦政府の立場に立って、国際政治に於ける国家利益を考え、資料漏洩によって生じる米国のインテリジェンス能力への打撃を考えるならば、スノーデンは国家反逆者と言うしかないということになろう。

しかし、米国社会のイデオロギー構造が上記の如くであるとすれば、仮に米国政府が米国民に対して広汎な情報収集態勢を構築し、それが国民の権利を不当に侵害していると受け取られるような事があれば、今後もスノーデンのようにアメリカ革命イデオロギーを一途に信ずる者からの告発が惹き起こされる可能性があろう。実際、スノーデンの前にも、NSA を告発した職員は、James Bamford、William Binney、Thomas Drake と続いていたのである。

以下、スノーデンの生立ちを含む人物像、漏洩告発の経緯、漏洩告発の動機の順に述べる。記述は基本的にスノーデンのインタビューなどスノーデン側からの資料によっているので、彼の立場を反映したものとなっていることをお含み願いたい。

１　スノーデンの生立ち

エドワード・スノーデンは、1983 年 6 月米国東海岸ノースカロライナ州エリザベス市の生れである。父親ロニーは、元沿岸警備隊員（現在退職）、母エリザベスは、メリーランド州ボルチモア市の連邦地方裁判所の事務官、姉は連邦司法センターで働く弁護士である。スノーデン家は、このように全員が連邦政府で働き、連邦政府に信頼を置く家族であった。

幼少のスノーデンが育ったエリザベス市は、米国沿岸警備隊の米国東海岸最大の基地を擁する地である。スノーデン一族は当地の旧家であり、一族には軍人、沿岸警備隊員や法執行官が多いという。父親ロニーも、一族の伝統を引き継ぎ、祖父同様沿岸警備隊員となった。彼は、愛国的であり、保守的であり、自由主義者でもあった。沿岸警備隊員として米国憲法（権利章典を含む）への忠誠を宣誓しており、米国憲法はアメリカにおける国民と国家の間の契約であると考えていたという。スノーデン少年はその薫陶を受けて育ったのである。

一家は、1992 年スノーデンが 9 歳の時、米国の首都ワシントン DC の近郊メリーランド州アン・アランデル郡に引っ越した。同郡には NSA の本部フォート・ミードが所在し、近隣は NSA など諜報機関職員や軍人が多く居住する地域である。NSA 本部はスノーデンの自宅から車で十数分の距離にあり、NSA 本部のお膝元で育ったのである。NSA を意識することも多かったと考えらえる。

スノーデンは、同郡の小中学校を卒業したが、ギリシャ神話などの読書好きで頭の良い子供であったという。1997 年秋 14 歳で、アランデル高校に入学したが、1998 年秋の 2 年生の初めに白血球の病気である単球増加症に罹り 9 ヶ月近くに亘り休学し、そのまま、1999 年に 15 歳で中退した。中退には、病気による休学に加えて、両親が不仲になったこと（後 2002 年に離婚）も影響しているとされる。

高校を中退したスノーデンは、アン・アランデル短期大学（コミュニティ・カレッジ）に入学し 1999 年秋から 2001 年までの 2 年間コンピュータ・サイエンスを履修する。但し、単位不足のためこの時点では高校卒業同等の認定資格（GED）は取得出来なかった。

スノーデンはこの頃からコンピュータにのめり込み、ネット・オタクと言われる様な状態となったようである。2001 年 17 歳でコンピュータ技術を利用して、相当高給のアルバイトも出来るようになり、2001 年 12 月には「アルズ・テクニカ」という人気サイトの常連となる。このサイトは、コンピュータや科学技術、そしてビデオゲームに力点を置いていて、大学院生などが多く参加するサイトである。スノーデンはここで相当の知的刺激を受けたと考えられる。更に 2002 年には MCSE（Microsoft Certified Systems Engineer）の資格を取得している。

また、スノーデンは、10 代の早い頃から日本に憧れを持っており、日本の格闘

ゲーム「鉄拳」の大ファンであった[2]。更に、日本のアニメが大好きであり、2002年から 2004 年の間には自ら日本アニメのウェブサイトを開設して運営していた程である。つまり、彼はゲーム・オタク、アニメ・オタクでもあった。

但し、この時点でのスノーデン青年は、コンピュータの技能は持つものの、他には学歴もセキュリティ・クリアランスもない、オタク青年であり、人生の展望が明るいとは言えない境遇であった[3]。

2　インテリジェンス社会への参加と幻滅

そうしたオタクのスノーデン青年に、転機が訪れる。2003 年のイラク戦争である。スノーデンは、イラクの抑圧された人々を助け、また、自らの学歴もない状況を克服すべく、陸軍特殊部隊というエリート部隊員を目指して、2004 年 5 月 20 歳で陸軍の訓練部隊に入隊した。ところが、スノーデンは軍人には不向きだったようであり、訓練中に両足を骨折して、同年 9 月には除隊した。

しかしスノーデンは、この挫折にめげずに、家族の例に倣い連邦政府で働きたいと考え、2005 年メリーランド大学の高等言語研究センターの警備員として勤務を開始する。実は同センターは NSA の研究施設である。スノーデンは、NSA 本部のお膝元で育ち、家族は連邦政府関係者であるので、同センターでの勤務が、（警備員勤務であろうとも）より高度なセキュリティ・クリアランス取得に道を開き、インテリジェンス諸機関に入るための入口になることを期待していたと考えられる。

当時、米国の諜報コミュニティは、コンピュータ技術者を必死に採用していた時であり、情報技術に優れ（大学卒業の年長者よりも技量が高かった由）、且つ（途中除隊したとは言え）軍歴を有するスノーデンはセキュリティ・クリアランスも取得し易く、諜報コミュニティに就職することができた。

即ち、2006 年 5 月には、CIA に情報技術者として採用されていた[4]。 年収は 7 万ドルであり、高校卒業資格も持っていないにも拘わらず、そのコンピュータ技

---

[2] 日本の格闘ゲームの『鉄拳』は、不利な状況においても強大な相手に立ち向かうという構想のゲームであるという。日本のビデオゲームのモチーフが、スノーデンの考え方に影響を与え、今回の告発にも影響を与えたとされることは興味深い。Greenwald, *No Place,* 45.

[3] 2003 年にスノーデンは、ウェブサイトに自分は学歴もクリアランスもない MCSE (Microsoft Certified Systems Engineer)保持者であると自己紹介している（Harding, *Files*, 22）。 米国では諜報諸機関初め連邦政府の多くの職では、セキュリティ・クリアランスが必要とされており、スノーデンはこの頃から既に連邦政府での勤務を希望していたことが伺える。

[4] 2006 年のこの頃スノーデンは、学歴がなくても、高い情報技術とセキュリティ・クリアランスさえあれば、政府の良いポストに就くことができるとウェブに記載している（Harding, *Files*, 24）。

術で一躍日の当たる職に就くことができたのである。その後、スノーデンは海外勤務を希望し、2007 年 3 月 23 歳でジュネーブの米国国連代表部に、CIA の情報システム技術者として派遣された。彼の任務は CIA 及び代表部のコンピュータ・セキュリティ担当であり、その卓越した技術で活躍した。しかしながら、ジュネーブ勤務中に、CIA には大いなる幻滅を持ち、2009 年 2 月 CIA を辞職して帰国した。辞職の直接の原因は、コンピュータのソフトウェア構築に関して上司と衝突したためという。

しかし、スノーデンの失業状態は長くは続かなかった。デル社に日本勤務で採用されたからである。2009 年春にはデル社の NSA 派遣社員として、日本に赴任した。日本を勤務地に選んだ理由は、10 代から日本への憧れを持ち一度日本で生活してみたいと考えていたからという。

日本の勤務場所は、米軍横田基地内の NSA 施設、主任務はネットワークのセキュリティで、主たる脅威は中国のハッカーからの攻撃であったという。この間、スノーデンはコンピュータの技量を更に高め、日本滞在中に、高級サイバー工作員（high-level cyber operative）の資格を認定された。同資格は、他国の軍や非軍のシステムに侵入して痕跡を残さずに情報を奪取し、或いはサイバー攻撃の準備をする資格であるとされる[5]。

他方、日本で勤務中に、NSA による広汎且つ人権侵害的な諜報能力の実態に触れ、益々、米国政府、特に NSA に幻滅を感じ、告発を考えるようになっていったという。

日本勤務は 2011 年春に終了したが、スノーデンは引き続きデル社の社員として働いた。即ち、メリーランド州の CIA 事務所で、約 1 年間マイクロソフトその他の民間情報会社と共に安全な情報データ保管システムの開発に当たった。この間に、NSA と民間会社が協力して人々の通信を掌握しようしているのを直接見聞すると共に、更に、インターネットに於けるプライバシーが失われようとしていることを知り、告発に傾いていったという。

スノーデンは 2012 年 3 月には転勤となり、ハワイ州オアフ島にある NSA の地方本部（クニア地域センター）勤務[6]となった。ここでのスノーデンの職務は、NSA のシステム管理者であったが、特別任務として、NSA 本部のサーバーから必要なファイルをコピーしてハワイ地方本部のサーバーに蓄積する任務を与えられたという。これは、万一 NSA 本部とハワイ地方本部間の通信に障害が発生し

---

[5] Greenwald, *No Place*, 44

[6] ハワイの地域センター(Regional Security Operation Center)は、 NSA が米国領土内に展開する 4 つの地方本部の一つ（他の三つはテキサス州、ジョージア州、コロラド州に所在）という重要拠点であり、主としてアジア方面を担当すると共に、米太平洋軍司令部に対する支援もその任務に含まれると推定される。

た場合でも、ハワイ地方本部が十分機能するようにするためのものであった。同時に、国防総省の防諜訓練アカデミーにおいて中国によるサイバーインテリジェンスからの防御方法の講師を務めるまでになったという。

他方、この間に益々告発の決意を固め、2012 年夏にはデータの違法なダウンロードを始めた。このダウンロードが可能だったのは、上記の特別任務のため、怪しまれずに膨大なファイルにアクセスすることが出来たためという[7]。

スノーデンは、2013 年 3 月にブーズ・アレン・ハミルトン社[8]に転職した。この転職は、より機微な資料(デル社の派遣社員の立場ではアクセスできないもの)を取得したいと考えたからという。事務所はホノルル市内にあり、標的分析官或は（世界中の）インフラストラクチャー分析官という職務で、特別に機密度の高いポストである。任務は、米国の通信やコンピュータ・ネットワークを狙うサイバー空間の敵を調査することであり、その為、NSA が浸透した世界中のシステムリストにアクセスすることが出来たという[9]。この転職のために、スノーデンは、転職前の年収約 20 万ドルから転職後の年収約 12 万ドルへの減額を受け入れた。

かくして、スノーデンは 5 月上旬までにはジャーナリストに提供したい機密資料を全てダウンロードして、告発するばかりの準備を整えたのである。

3　告発と資料提供

スノーデンが、告発に当たり先ず白羽の矢を立てたのがグレン・グリーンワルドである。スノーデンは、過去の経歴から判断して自分の告発の趣旨を正しく理解して報道してくれると見込んだジャーナリストを選んだのである。

グリーンワルドは、ブラジルのリオデジャネイロ在住の米国人である。元々憲法や市民権問題を扱う弁護士であったが、ジャーナリストとなり、2006 年には NSA の盗聴監視によるプライバシー侵害を厳しく批判したベストセラーを出版した。そして 2012 年からは、米国に開設された英紙ガーディアンの米国支局のコラムニストとなっていた。

スノーデンは、グリーンワルドに接触しようとして、2012 年 12 月から数回に亘りメールを送付して秘密保持の為に暗号通信を導入するよう教示したが、同氏

---

[7] Andrews, Burrough and Ellison, “The Snowden Saga,” *Vanity Fair.*

[8] ブーズ・アレン・ハミルトン社は、米諜報諸関と極めて密接な関係を持つ企業であり、現国家諜報長官のクラッパー氏は元同社の重役であった。他方、スノーデンの告発があった 2013 年 6 月時点の副会長マッコーネル氏は元国家諜報長官であり、その前は同社の重役、更にその前は NSA 長官であった。副社長のウールジー氏は元 CIA 長官である。年間売上は約 60 億ドル、従業員は 2 万 5 千人である。 Julian Borger, “Booz Allen Hamilton: Edward Snowden’s US contracting firm,” *The Guardian*, 9 June 2013, http://www.guardian.co.uk/world/2013/jun/09/booz-allen-hamilton-edward-snowden.

[9] Andrews, Burrough and Ellison, “The Snowden Saga,” *Vanity Fair.*

が暗号通信に明るくなかったことなどのため、連絡の確立には至らなかった。

そこでスノーデンは、2013 年 1 月末からローラ・ポイトラス女史との接触を図った。ポイトラスは、米国人のドキュメンタリー映画監督であるが、グリーンワルドの友人であり、同氏同様に米国の監視国家化を批判していた。そのためか、米国を出入国の度に数時間に及ぶ厳重な検査を受けるなどしたため、これを嫌ってドイツ・ベルリンに住んでいる。

彼女には暗号通信の素養があったので、インターネットによるスノーデンとの接触は徐々に進んだようである。スノーデンは、NSA に探知されないように、常に暗号通信を使い、且つ、自宅や事務所からは一切通信せず、更に自己の人定は一切明かさずに接触を続け、ポイトラスとの信頼関係を構築していったという。

そして 2013 年 5 月 20 日スノーデンは遂に、機密資料を持って、ハワイから香港に向けて出国。香港のホテルから、ポイトラスに「プリズム」他 20 数件の機密資料を暗号通信で送付。それと同時に、同女史の仲介でグリーンワルドとも接触に成功し、同氏にもこれらの機密資料を提供した。それと同時に、両者に直ちに香港に来るよう要請した。

両者はガーディアン米国支局と調整の上、香港にはグリーンワルド、ポイトラス両氏にガーディアン紙のイーウェン・マックアスキル記者を加えた三人が向かい、現地時間の 6 月 2 日に到着。その翌日からスノーデンと接触して取材を開始し、米国東部時間の 6 月 5 日にガーディアン紙電子版で「米国内電話メタデータの大量取得」を報道したのを皮切りに、6 日には「プリズム」、7 日には「大統領政策指令第 20 号」(サイバー攻撃に備え潜在攻撃目標のリスト化を指示した 2012 年 10 月の機密文書)、8 日には「バウンドレス・インフォーマント」を報道した。更に 9 日には、告発者であるスノーデン本人のインタビュー映像を報道して、世界にセンセーションを巻き起こした[10]。

---

[10] "Verizon forced to hand over telephone data – full court ruling," *The Guardian,* 6 June 2013, accessed 13 August 2014, http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
--Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian,* 7 June 2013, accessed 13 August 2014, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
--Glenn Greenwald and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian,* 7 June 2013, accessed 13 August 2014, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.
--"Obama tells intelligence chiefs to draw up cyber target list – full document text," *The Guardian,* 7 July 2013, accessed 13 August 2014, http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

なお、スノーデンは、ポイトラスを通じてグリーンワルドと連絡を取っただけではなく、同様にポイトラスが相談相手としたワシントン・ポスト紙のバートン・ジェルマン記者とも連絡を取るようになっていた。スノーデンは、告発報道を確実にするため、複数の選択肢を維持しようとしていたのである。スノーデンは、ジェルマン記者に対して 5 月 24 日「プリズム」関係資料を送付し、３日以内に報道するよう要求したが、その通りには進まず、結局ワシントン・ポスト紙は、6 月 6 日ガーディアン紙と同日「プリズム」について報道をした。

これを契機に、NSA の活動実態についての報道が世界中に波及して沸騰したのである[11]。

４　漏洩資料の量と所在

漏洩された資料件数の総数は膨大である。それだけ膨大な資料をダウンロードするため、スノーデンは「ウェブ・クローラー」というソフトウェアを使用したと言われる。これは、事前のプログラムに従い自動的にウェブサイトの中を探索し必要情報を取り出してくるソフトであり、探索した情報件数は 170 万件とされる[12]。しかし、探索し接触した情報の中から何件持ち出したかは NSA では特定できないとされている。

他方、スノーデンの言動から分かる資料件数は次の通り。即ち、先ず、グリーンワルドとポイトラス両氏に最初に提供したデータが 20 数件、次に両氏が 6 月 1 日米国を出国する直前に 3～4000 件。また、グリーンワルドが提供を受けた総件数は 1 万 5 千件から 2 万件であるとする当人の発言が報道されている。更に、スノーデンが最終的にグリーンワルドとポイトラス両氏に提供した資料は５万件から２０万件との推測もある[13]。なお、スノーデンが持ち出した資料の中心は NSA

--“Boundless Informant NSA data-mining tool – four key slides,” *The Guardian,* 8 June 2013, accessed 13 August 2014, http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides.

--“Boundless Informant: NSA explainer – full document text,” *The Guardian*, 8 June 2013, accessed 13 August 2014, http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text.

[11] スノーデン告発に関連する我が国の報道は、諸外国と比べて極めて低調であると感じる。これは、我が国に於けるインテリジェンス理解が低いために、関心自体が低いことと、漏洩資料の意味を十分理解できないことに起因しているのではないかと考える。

[12] David Sanger and Eric Schmitt, “Snowden Used Low-Cost Tool to Best N.S.A,” *International New York Times,* 8 February 2014, accessed 10 February 2014, http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.

[13] Andrews, Burrough and Ellison, “The Snowden Saga,” *Vanity Fair.*

資料であるが、協力関係にある英国のシギント機関 GCHQ から NSA に提供された資料も含まれており、この英国関係資料は 5 万 8 千頁である（件数ではない）とされている[14]。更に、他の UKUSA 諸国のシギント機関、加 CSE、豪 ASD、ニュージーランド GCSB 等の資料も含まれる。

さて、この膨大な機密資料は現在どこにあるのだろうか。上述の経緯からも分かるように、提供された機密資料の全部を当初保有していたのは、グリーンワルド、ポイトラスの両氏及びガーディアン紙の三者であった。その後、ガーディアン紙が危険分散と作業協力のため、米紙「ニューヨーク・タイムズ」とニュースサイト「プロパブリカ」にも全部を提供。また、ポイトラス氏は独誌「シュピーゲル」と、グリーンワルド氏はブラジルのニュースメディア「グロボ」と関係を有しており、両誌紙も相当多量の資料を保有していると考えられる。更に、スノーデンの意向では、関係国のマスメディアには当該国に関連する資料が提供されるべきであるとされており[15]、多くの諸国で報道されていることから判断して、多くの国のマスメディアが自国関連の機密資料の提供を受けていると推定される。

５　告発の理由

スノーデンが、年収２０万ドルの生活を放棄し、逮捕されれば一生悲惨な刑務所暮しとなる危険を冒してまで、告発に至った理由は何であろうか。同氏の多くのインタビュー、そしてインタビューを基にした報道を分析すると次の要因が挙げられる。

（１） アメリカ民主主義の信奉者

スノーデンは、米国民主主義の信奉者である。

彼は、米国は、良い価値観を持った善良な人々の国であり、基本的に良い国であると、米国を評価している。

しかし、自由で民主的な社会では、(統治機構は人々の同意の上に成り立っている以上)、統治される人々は統治機構が何をしているのかを知らされなければ、そもそも統治に対する同意が成り立たない。従って、必要な情報は人々に提供されなければならず、統治機構が人々の知らないところで勝手なことをすることは許されないと、スノーデンは考える。

彼にとって米国憲法は基本的人権を謳った特別なものであり、自分はその憲法

---

[14] Harding, *Files,* 144, 303.
--Reuter, “Glenn Greenwald: Snowden Gave Me 15-20,000 Classified Documents,” *The Huffington Post*, 6 August 2013, accessed 19 August 2014, http://www.huffingtonpost.com/2013/08/07/glenn-greenwald-edward-snowden-documents_n_3716424.html.

[15] Harding, *Files,* 145.

に忠誠を誓った愛国者である。そして、米国民としての公民権は、自分の政府を監視する義務をも伴うものであると考えている[16]。

（２） インターネットの価値と自由の信奉者

スノーデンは、ネット・オタクである。若い頃からインターネットの世界に入り浸っており、インターネットはゲームをし、新しい知識を得、多くの人々と交流する場であり、インターネットそのものが人生と言えるような存在である。（現在のロシアでの亡命生活でも、インターネットさえあれば退屈しない由。）

つまり、インターネットは、同氏にとって、単なる道具ではなく、精神と人格が成長する場、自由と探求の場であり、知的成長の場でもあった。スノーデンは「インターネットによって自分は自由を経験し、人としての能力を開発することができた。」[17]「インターネットは全人類史上、最も重要な発明である、と考えたことさえある。」[18]と述べている。

しかしながら、インターネットがこのように自己実現の場であり得るためには、インターネットの世界でプライバシーと匿名性が確保されなければならず、誰にも監視されずに試行錯誤を重ねることができなければならない。プライバシーが確保されなければ、インターネットは自由な空間ではなくなってしまう。彼は「インターネットからプライバシーと自由が失われ、インターネット特有の価値が失われた世界には住みたくない。」と述べている[19]。

（３） 米政府、諜報諸機関に対する幻滅

このようなスノーデンにとって、インテリジェンスの世界での体験は、彼の信条を裏切るものであった。更に、「連邦政府は、インターネットをハイジャックして、これを全人口を監視するための装置に変えようとしている。」[20・21]との認識

---

16 スノーデンは NSA のハワイ地域センターでは勤務場所に米国憲法典を机の上においていたという。Harding, *Files*, 46, 110.

17 Greenwald, *No Place,* 46.

18 Edward Snowden, interview by Glenn Greenwald and Ewen MacAskill（6 June 2013）, *The Guardian*, 10 June 2013, accessed 12 July 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

19 Greenwald, *No Place,* 47.

20 Harding, *Files,* 110.

21 但し、分析官は、「最少化手順」により米国人のデータに対するアクセスは制限されている。スノーデンは、分析官ではないのでこの制限を十分知らずに、分析官による米国内通信へのアクセスを過大に理解した可能性がある旨の指摘がされている。
“Snowden would not have been able to legally ‘wiretap anyone’,” *Top Level Telecommunications*, 12 February 2015, updated 19 February 2015, accessed 20

を持つようになった。

ア　CIA ジュネーブ勤務での経験（2007～2009 年）

スノーデンは、コンピュータ・セキュリティ担当として勤務する内に、多くの秘密に接することができたが、そこで実際の CIA の活動が、米国民主主義の理念とは背反することを知ったという。

その一例は、CIA の工作である。工作員が、スイスの銀行家を協力者として獲得するために、わざと酒を飲ませて飲酒運転をさせ、逮捕された後に各種の支援活動をした。しかし、結局、協力者として獲得することができず、この工作が銀行家の人生を狂わせるだけで終わったことを挙げている。

そして CIA は、世界に対して善よりも遥かに多くの悪をなしていると考えて、その組織の一員であることに対して良心の呵責を感じるようになったという[22]。

イ　NSA 日本勤務での経験（2009～2011 年）

次の、日本における NSA 勤務では、米国政府や NSA による広汎且つ人権侵害的な諜報能力の実態を目の当たりにして、幻滅を深めた。

例えば、無人飛行機による上空からの監視活動や、人々がインターネットで通信するのをリアルタイムで監視している状況を知ったという[23]。

或いは、コンピュータへの秘密のアクセスを確保するために、大学、病院、企業など民間施設に対してハッキングを行っているが、そこで間違いを犯せば枢要なシステムがクラッシュして多くの人々に影響を及ぼす危険な行為であり、誤った活動を行なっていると考えた[24]。（但し、標的国が何れかは明確でない。）

ウ　CIA メリーランド州事務所での経験（2011～2012 年）

ここでは、NSA と民間通信企業が密接に協力しているのを目の当たりにしたが、政府の目的は、インターネットの世界からプライバシーを排除して、電気的に通信すれば、必ず、その通信を捕捉し、蓄積し、分析できるようにすることという認識に達した。

エ　NSA ハワイ勤務での経験（2012～2013 年）

February 2015,
http://electrospaces.blogspot.jp/2015/02/snowden-would-not-have-been-able-to.html

[22] Greenwald, *No Place,* 42; Harding, *Files,* 35.

[23] Greenwald, *No Place*, 43.

[24] Edward Snowden, interview by Glenn Greenwald, *The Guardian,* 17 June 2013, accessed 18 June 2013,
http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

なお、スノーデンによれば、2012 年 11 月 29 日にシリア国内のインターネット回線が殆ど全て不通になったが、これは NSA 工作員が工作の一環でシリアのインターネット回線の中枢ルータに侵入したところ、何らかのミスを犯して生じさせたものであるという。Edward Snowden, interview by Bamford in June 2014.

更に NSA の活動実態を詳しく知るようになり、最終的に告発の意思を固めた。

例えば、イスラエルとのインテリジェンス協力では、アラブ系アメリカ人のメールや電話情報を人定事項を削除せずに提供している。この情報を基に、イスラエルが占領するガザや西岸地区に居住する親族のパレスチナ人が攻撃の対象とされかねないなど、明らかな権力の濫用行為を知ることとなったと主張する。

更に、ブッシュ政権時代における NSA のデータ収集を総括した内部機密資料（2009 年 3 月付）[25]を読む機会があった。スノーデンの理解では、同資料に記されたブッシュ政権時代の NSA による広汎なデータ収集は明らかに憲法違反・違法行為であるにも拘わらず、その後 NSA の最高幹部は全く責任を問われていないことに、大きな憤りを感じたという。

（4） インターネットの自由の消滅への危惧と議論の喚起

スノーデンは、アメリカ民主主義の信奉者であり、インターネットの価値と自由の信奉者であるが、政府・諜報諸機関がこれらの信条を裏切り、米国民の知らないところで監視態勢の強化を進めており、このまま放置すれば、やがてインターネットの世界からプライバシーと自由が失われてしまう、これは民主主義の存続に対する脅威であると危機感を持った。

そこで、彼は NSA の情報収集の実態を公表し、プライバシー、インターネットの自由そして監視国家化の危険性に関して、世界的な議論を巻き起こすことを目的として告発をしたという。即ち「自分の告発の動機は、公衆の名の下に公衆の利益に反したことが行われている実態を、公衆に知らせることである。」そして「公衆がそれに対して自ら決定することを可能とすることである。」と述べている[26]。

彼にとって、これは国家に対するサービスであり、自分が恐れるのは、自分の身の将来ではなく、告発に国民が何の反応も示さず、人生を賭けた自分の行為が無駄に終わることである。

その後の展開は周知の通りであり、スノーデンによる告発は米国そして世界中に大きな反響を及ぼしている。スノーデンは、2013 年 12 月のインタビューで、

---

[25] ス資料 Office of the Inspector General, NSA/CSS, *Working Draft,* 24 March 2009. In “NSA inspector general report on email and internet data collection under Stellar Wind – full document,” *The Guardian,* 27 June 2013, accessed 30 June 2013, http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection

[26] Greenwald, *No Place,* 18, 47; Harding, *Files,* 246.

「自分自身に限定して言えば、自分の任務は達成された」と述べている[27]。

以上がスノーデンの告発の背景となった論理である。他方、諜報活動は何れにしろ諜報源の秘匿を必要とする活動である。民主主義国家に於いては、諜報機関に対する民主的統制と諜報活動の秘匿という、二つの相矛盾する要請を如何にして両立させ、実現していくか、永遠の課題である。

[27] Edward Snowden, interview by Barton Gellman, *The Washington Post,* 24 December 2013, accessed 25 December 2013, http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations...