英国 IPA（Investigatory Powers Act）2016 に関する調査報告書

2017 年 6 月 12 日

情報セキュリティ大学院大学

（執筆：田川義博・林紘一郎）

目次

執筆者連絡先：
田川義博：情報セキュリティ大学院大学セキュアシステム研究所客員研究員
tagawa@iisec.ac.jp
林紘一郎：情報セキュリティ大学院大学教授　hayashi@iisec.ac.jp

Executive Summary

1. IPA 2016 の注目点

IPA 2016 は、条文だけでも A4 で 300 ページ以上に及ぶ大部であるため、調査結果を要約するのは容易ではない。ここでは著者の 2 名が選んだ、注目すべき事項を箇条書きするに止める。

＊バルク・データも含め規定されている令状、許可、通知に関する権限は、新たな権限ではないが、従来多くの法律に分散して規定されていたものを、IPA 2016 に一元化したことで、権限が分かりやすくなった。

＊プライバシー保護の規定が強化された。

・1 編「一般的プライバシー保護」の規定が新設された。

・調査権限の行使に際して、プライバシーをより重視する観点から、各種の保護措置（safeguards）が強化された。

・調査権限の監督強化のために、新たに調査権限コミッショナー職と司法コミッショナー職が新設された。

・国務大臣が令状発出を許可する際に、司法コミッショナーの承認を要することとされた。この仕組みは、double lock と呼ばれている。

＊一方で、デジタル時代にふさわしい権限規定を追加した。すなわち、インターネット接続記録（ICRs：Internet Connections Records)の取得や保存の規定が新設された。この規定によって、政府は人々の通信の仕方が変化したために失われた、調査能力を回復できるとしている。

＊バルク令状としては、通信傍受、コミュニケーション・データ取得、機器干渉、バルク・パーソナル・データセット（BPD：bulk personal dataset）の 4 つがある。バルク令状は、一般人のプライバシー侵害のリスクが大きいので、特定令状・許可と比較すると、その手続き要件が厳しくなっている。

＊バルク令状の申請権者は、3 つのインテリジェンス機関（保安部、秘密情報部、GCHQ）に限定されており、法執行機関や国防インテリジェンス機関には認められていない。

＊通信傍受令状および機器干渉令状に関しては、特定対象向け令状が英国内外に及ぶのに対して、バルク令状は英国外の通信や機器に対象が限定されている。

＊バルク令状には、原則として司法コミッショナーの事前承認が必要である。

＊特定令状の発出根拠・理由が、① 国家安全保障、② 重大犯罪の予防・探知、③ ①に係る経済的繁栄の三つであるのに対して、バルク令状では、これに加えてより詳細なレベルの「特定の運用目的」があることを要する。

＊またこの運用目的は、インテリジェンス機関の長が現行維持すること、国務大臣の同意を得ていること、この運用目的の写しを議会のインテリジェンス・安全保障委員会に 3 カ月末毎に提出すること、首相は少なくとも年 1 回この運用目的を審査す

ることが定められている。

＊これらを踏まえて、以下の内容を整理した。

・令状・許可・通知における保護措置を類型化して対比

・調査権限コミッショナーと司法コミッショナーの選任方法や役割

・National security notice や Technical capability notice の要件

・インテリジェンス活動におけるバルク・データの必要性と制約

・スノーデンの暴露以降、バルク・データの扱いに関して、米英で対照的な差がでてきた経過と内容

・調査権限とプライバシー保護のバランスを図るための主要事項

・バルク・データの収集、検証、保存・破棄、開示・配布の各局面でのプライバシー侵害リスク

・調査権限活動を適正に執行するための法体系、議会による統制・牽制、行政内部における統制・牽制。

2. IPA 2016 におけるバルク・データとプライバシー保護のバランス

この課題は、「自由と安全」の問題として引き続き考察されなければならないが、IPA 2016 に関する限りは、アンダーソンの以下の考えが受け入れられたものと考えられる。

＊バルク権限はその定義上、国家安全保障への脅威や重大犯罪への関与の容疑がほとんどない非常に多くの人々のデータに対して、国家がアクセスする可能性がある。

＊これらの権限のいかなる濫用も、無実の人々へ特に幅広い効果を及ぼし得る。

＊濫用が探知できないまま、利用が可能であるとするならば、大きな不信感が生じ得る。

＊バルク権限の利用は、それを不可欠とする運用事例があること、および適切で目に見える保護措置に従ったものである場合にのみ是認されるべきである。

＊バルク傍受権限は GCHQ のみが、バルク取得権限は保安部（MI5）と GCHQ が、BPD 権限は保安部と秘密情報部（MI6）が利用しており、他の特定令状の権限やヒューミントなどの手段で代替することはできない。

＊GCHQ のインテリジェンス・レポートは、50%弱はバルク傍受から、約 5%はバルク令状から、約 20%は特定機器干渉から得られたデータに基づいている。

＊バルク機器干渉権限は（現在認められていないし）今まで利用されたことがない。今後もあまり利用されないであろうし、特に強力で技術的な監督が必要である。

3. 今後の外部的不確定要因

IPA 2016 は昨年 11 月に成立して、一部の規定は既に施行されているが、大部分の規定は、国務大臣の定める規則によって施行日が決まることになる。しかし施行されたとしても、① EU 司法裁判所の判決、② Brexit 後における EU 法の適用、③ ヨーロッパ人権条約という 3 つの外部的不確定要因がある。

1. 研究テーマと報告書の性格

当大学院では、2012 年度と 2013 年度に、「インテーネットと通信の秘密」に関する研究会を組織し、ISP（Internet Service Provider）の実務家と研究者との共同作業によって、伝統的な「通信の秘密」の概念がインターネットの時代にどのような変容を迫られているかを考察した。

その結果は、以下の 2 つの報告書に要約されている。

- 「インターネットと通信の秘密」研究会(第 1 期)『インターネット時代の「通信の秘密」再考』(2013 年 6 月)
- 「インターネットと通信の秘密」研究会(第 2 期)『インターネット時代の「通信の秘密」各国比較』(2014 年 5 月)

(いすれも、http://lab.iisec.ac.jp/~hayashi/ からアクセス可)。

この間 2013 年 6 月には、エドワード・スノーデンが秘密裡に行われていた米国 NSA（National Security Agency）[1] の活動を暴露したことで、米英を中心とするインテリジェンス機関が、膨大な通信データ等（いわゆるバルク・データ）を利用して行うテロ対策等において、法的手続きが不十分あるいは遵守されておらず、人権侵害が懸念される事態が明らかになった。

インテリジェンス活動の一環としてシギント （SIGINT :SIGnals INTelligence）があることは古くから知られていたが[2] 、インターネットが標準的な通信形態になり、あらゆる活動がそれに依存するようになったため、この重要性はかつてないほど高まっている。米国のインテリジェンス・コミュニティにおいて NSA の地位が相対的に高まったこと、英国のサイバーセキュリティの全国責任部署が GCHQ（Government Communications HeadQuarters）内部に置かれたことなどが、その有力な証拠である。

インテリジェンスは必然的に、個人の自由と衝突する局面を有している。この両立が困難な 2 つの法益をどう調和させるかに、先進諸国は苦慮してきた。しかし IS（いわゆるイスラム国）など非国家主体による予測困難なテロ行為の多発とともに、一定の要件を満たした場合にシギント情報を分析することで予兆を察知することは、各国とも認めている。ただし先進諸国の対応も、バルク・データ（対象者を特定しない情報）の扱いを巡って二分されている。

一方の立場は EU に代表され、バルク・データの取得と分析には否定的である（なお、これは EU 総体に関してであって､加盟国間にある温度差については別途の検討を要する)。

---

[1] NSA（National Security Agency：国家安全保障庁）は、インテリジェンス（政策決定者が国家安全保障上の問題に関して判断を行うために政策決定者に提供される、情報から分析・加工された知識のプロジェクト、あるいはそうしたプロジェクトを生産するプロセスのことをいう）活動のなかでもシギント(SIGINT：Signals Intelligence）は信号（data transmission）から収集される素材情報（中略）に基づくインテリジェンス活動のことである。「インテリジェンス」と「シギント」の定義の出典：小林良樹[2014]『インテリジェンスの基礎理論［第二版］』立花書房、p.4、p.94

[2] SIGINT の範囲が広すぎるため、電気通信システムを介した部分をとくに COMINT（COMmunications INTelligence）と呼んで区別することがあり、米国では法律用語になっている（18 U.S.C. 798)。

他方の立場が英国であり、バルク・データの扱いは一定の要件の下で従来から認められてきたが、プライバシーへの配慮条項を加え監督機関を強化することで、これを追認した法律、すなわち IPA（Investigatory Powers Act）2016 を成立させた（しかも下院の議決では圧倒的多数が賛成した）。

これは EU の影響を受けて従来のセーフハーバー協定を改定し、プライバシー・シールド協定としてバルク・データの扱いに慎重な態度に転じた米国とも異なり、ましてや、世界一厳格に「通信の秘密」を解釈・運用してきたわが国とは著しい対照を示している。英国が、スノーデン事件の後であっても、このような姿勢を堅持するのはなぜか、この点を究明することが、インターネット時代の「通信の秘密」のあり方についてヒントになるのではないか、というのが本調査の問題意識である。

前 2 回の研究会では「わが国はどうすべきか」という提言に主眼があったが、本報告は提言を含んでおらず、法律の内容やインプリケーションをできるだけ客観的に分析することに主眼がある。したがって、前 2 回と違い、参加者のお名前は記載しておらず、文責は執筆者 2 名のみにある。

2. IPA 2016 成立までの経緯

(1) 英国におけるインテリジェンス活動に関する法制度[3]

インテリジェンス機関である保安部（Security Service＝SS、通称 MI5）と秘密情報部（Secret Intelligence Service＝SIS、通称 MI6）は 1908 年に設置されていたが、保安部は Security Services Act 1989 によって、秘密情報部とシギント活動の GCHQ（Government Communications Headquarters）は、Intelligence Services Act 1994 によって組織と権限の法的根拠が与えられた。

また調査権限については、通信傍受法（Interception of Communications Act）1985 を経て、調査権限法（Regulation of Investigatory Powers Act＝RIPA）2000 によって規定されていた。

なおここで、調査権限にはインテリジェンス機関によるものだけではなく、法執行機関や地方自治体による調査権限（一般的には「捜査権限」）も含まれていることと、調査手続きが司法手続きを要せず行政手続きだけで行えたことが、米国の法制度（さらにはわが国の法制度）とは異なる点である。

(2) IPA 2016 の成立を促した契機

スノーデンの NSA 活動の暴露の翌年、2014 年 4 月に EU 司法裁判所はデータ保存指令の無効判決を下した。この対応策として、2014 年 7 月に DRIPA（Data Retention

[3] 以下の文献を参照。小谷賢［2015］「米英における情報機関の行政権限」大沢秀介(監修) [2015]『入門・安全と情報』成文堂、pp.180~185

and Investigatory Powers Act：データ保全・調査権限法）2014 が制定された[4] 。

しかしながら、同法は 2016 年 12 月までの時限立法となっていて、そのときまでに新たな法律を制定する必要があった。このため、政府は 2016 年 3 月調査権限法案（Investigatory Powers Bill）を議会に提案した。

(3) IPA 2016 の成立に至る経過

1）2015 年に政府から独立した 3 つの報告書[5] が公表され、法案の基礎となった。

2）2015 年 11 月に政府は調査権限草案（Draft Bill）を議会に提案、法案提出前の議会における事前審議（pre-legislative scrutiny）[6] が行われた。

3）この事前審議における意見を踏まえて、政府は 2016 年 3 月に調査権限法案（Investigatory Powers Bill）を付属文書[7] とともに議会提案した。

4) 英国の EU 離脱（Brexit）の是非を問う、6 月 23 日の国民投票日に先立つ 6 月 7 日に、下院において賛成 444 票対反対 69 票で可決された。その後上院審議で修正可決、両院間での ping pong[8] を経て、11 月 17 日成立した。

5) 法案審議中の 2016 年 8 月に、論議の焦点の一つであるバルク・データに関するアンダーソン・レポートが公表された。

6) 11 月 29 日に女王の裁可（royal assent）を得て公布、一部は直ちに施行されているが、大多数の規定は国務大臣が規則（regulation）によって定める期日に施行される。いつ施行されるかについては、いくつかの要素により影響されると考えられる。

なお、経過規定は細則（Schedule) 9 において定められている。DRIPA は全面的に廃止されるが、IPA 2016 はシギント活動に特化した法律であるので、RIPA 2000 のこの部分の規定は新法が施行されると同法に置き換わるが、ヒューミント(HUMINT：HUMan INTelligence)[9] 活動など、シギント活動以外の RIPA 2000 の規定はその後も依然として効力を有する。

---

[4] DRIPA 2014 の成立の経過および内容については以下の文献を参照。今岡直子「イギリスにおけるデータ保全及び調査権限法の制定：EU データ保全指令の無効判決を踏まえて」外国の立法 264（2015.6）

[5] 以下の報告書を指す。① “Privacy and Trust”、議会インテリジェンス・安全保障委員会報告書、② “A Question of Trust”、Queen’s Counsel である David Anderson による報告書、③ “A Democratic License to Operate”、Royal United Services Institute (RUSI) による報告書。

[6] 議会の 3 委員会（合同委員会、インテリジェンス・安全保障委員会、下院科学技術委員会）が審議を行い、2016 年 3 月に草案審議結果の報告書を公表している。出典： “Investigatory Powers Bill (HL BILL 40 of 2016-27” House of Lords Library Note, 21 June 2016

http://researchbriefings.files.parliament.uk/documents/LLN-2016-0032/LLN-2016-0032.pdf

[7] 付属文書の例：“A response to pre-legislative scrutiny”、“An operational case for bulk powers”、“Operational case for the retention of internet connection records”、“Codes of practice: retention and use of bulk personal datasets, National Security Notices, Interception of Communications”

[8] 英国では下院と貴族院の議決内容が異なった場合に、日米のように両院協議会による調整の仕組みがなく、両院間で修正案が往復して調整が行われる。調整がつかない場合には、下院の議決内容を尊重することが慣習になっているようである。

[9] ヒューミントとは、「人的な情報源から収集されあるいは提供された素材情報に基づくインテリジェンス」と定義される。出典：注 1 文献 p.9

3. IPA　2016 の構成[10]

本法は 272 条（1 編から 9 編）及び 10 の細則から成り、各編の表題は以下の通り。

＊1 編：一般的プライバシー保護：プライバシーに係る一般的義務（2 条）など

＊2 編：合法的（特定）通信傍受[11]

＊3 編：コミュニケーション・データ[12] 取得許可

＊4 編：コミュニケーション・データの保存（通知）

＊5 編：（特定）機器干渉[13]（Equipment Interference）

＊6 編：バルク[14] 令状（1 章：バルク傍受令状、2 章：バルク取得令状、
3 章：バルク機器干渉令状）

＊7 編：バルク・パーソナル・データセット[15] 令状

＊8 編：監督の仕組み[16]（Oversight Arrangements）

＊9 編：雑則および一般的規定[17]

＊細則：細則 1～10

---

[10] 英国の正式名称は、the United Kingdom of Great Britain and Northern Ireland である。2011 年の国勢調査では人口は全体で 6500 万人であるが、そのうちイングランドが 84.1%、スコットランドが 8.3%、ウエールズが 4.8%、北アイルランドが 2.8%である。歴史的経過があるためか、英国の法律ではイングランド以外のエリアに関しては、イングランドとは別の法的な役割を果たす大臣などを指定している規定が多いが、本報告書では人口の太宗を占めるイングランドに関する法的規定を中心に述べることとする。
人口の出典：Countries of the United Kingdom by population, Wikipedia

[11] 傍受はコンテンツ（通信内容）を取得する行為である。コンテンツの定義は 261 条(6)にある。

[12] コミュニケーション・データとは、261 条(5)によって entity data または events data を意味するとされているが、通信によって伝送される情報のうち通信日時、対地、受発信者情報など通信内容を除く情報を指している。EU 指令などでも communications data の用語が使われているが、通常は米国では meta data、日本では通信の構成要素と呼ばれている。本報告書では各国の用例に従う。

[13] 5 編の機器干渉は、特定のコンピュータなどの機器に対する、通信と機器に関するデータを取得する目的で行われる行為である。合法的ハッキングであるとの指摘もある。ドイツにおいても、「私人のコンピュータに侵入してその中の情報を入手するいわゆるオンライン捜査を行う権限が認められている。但し、2020 年末に失効することが定められている」出典：山口和人「ドイツの国際テロリズム対策法制の新たな展開-「オンライン捜査」を取り入れた連邦刑事庁法の改正」外国の立法 247 (2011.3)

[14] 2 編、3 編および 5 編の規定は、対象を特定した規定であるのに対して、6 編のバルク令状は対象を限定しない大量の通信傍受や機器干渉、コミュニケーション・データの取得を認める規定である。バルク・データの定義は IPA 2016 にはない。
なお、スノーデンが NSA 活動を暴露した翌年 2014 年 1 月に発出された米国の PPD（Presidential Policy Directive：大統領政策指令）28 号では、バルク・データの収集について、識別子を用いないデータ収集（without the use of discriminants (e.g. specific identifiers, selection terms, etc.)であるとしている。

[15] 7 編で規定されているバルク・パーソナル・データセットというのは、通信過程によって得られる情報ではなく、大量の個人データが収録されている電子的なデータベースのことである。インテリジェンス機関に与えられている権限であり、インテリジェンス機関が求めている情報は、収集されている個人データのごく一部である。パーソナル・データセットには、例えば医療情報（health records）のようなセンシティブ・データが含まれている場合には、検証や保存が制限されている。

[16] いままでの法律でも、インテリジェンス機関や法執行機関の権限行使に関しては、Intelligence Service Commissioner、Interception of Communications Commissioner、Chief Surveillance Commissioner などのコミッショナーが置かれていた。IPA 2016 においては分散して規定されていた 6 つのコミッショナーを廃止して、調査権限コミッショナー（Investigatory Powers Commissioner）にほぼ一元化された。これらのコミッショナーの廃止については 240 条に規定されている。なお、4 編に関する規定を監督する Information Commissioner 職は統合対象外である（244 条）。

[17] 9 編では、国務大臣の権限として、事業者に対して National Security Notice および Technical Capability Notice を発出できる規定などがある。

調査権限は 2 編から 7 編と 9 編に規定されている。すなわち特定対象の通信傍受令状（2 編）、特定対象のコミュニケーション・データ取得許可（3 編）、コミュニケーション・データの保存通知（4 編）、特定対象の機器干渉令状（5 編）、バルク令状（通信傍受、コミュニケーション・データ取得、機器干渉）（6 編）、バルク・パーソナル・データセット令状（7 編）、National security notices、Technical capability notices（9 編）である。

4. 主な改正点と議会審議[18] における論議内容

インテリジェンス機関に従来から認められていたバルク権限は、その利用に関する制限規定が加えられたものの、権限自体は縮小されておらず、米国の法制度見直しや EU-米国間の新たなプライバシー・シールド協定において、バルク・データ収集が大幅に制限されたこととは大きく異なっている。むしろ従来バルク機器干渉が認められてなかったとすれば（後述 11.(3)のアンダーソン・レポート）、バルク取得の範囲を拡大したことになる。

政府の提出法案に関しては、以下のような特徴点がある。

(1) バルク・データも含め法案に規定されている令状、許可、通知に関する権限は、すでに付与されているものであって、新たな権限ではないものの、従来多くの法律に分散していた権限規定[19] を IPA 2016 に一元化したことで、権限が分かりやすくなった。

(2) プライバシー保護の規定が強化された。

1 編には、プライバシーに関する一般的保護義務（2 条）を規定するとともに、他のプライバシー保護規定を網羅的に記している。令状の発出時等に配意すべきプライバシーに関する事項が規定されている一方で、調査権限の必要性の根拠など他に考慮すべき事項が規定されている。この一般的保護義務規定は、調査権限とプライバシー保護のバランスを図ろうとする規定である。また調査権限の行使に際して、プライバシーをより重視する観点から、各種の保護措置(safeguards)が規定されている。

(3) 一方で、デジタル時代にふさわしい権限規定を追加した。すなわち、インターネット接続記録（ICRs：Internet Connection Records）の取得や保存の規定[20] が新設された。この規定の新設によって、政府は人びとの通信の仕方が変化したために失われた調査能力（capability）を回復できるとしている。

---

18 法案審議模様については注 6 の文献を参照。

19 付属文書の一つ “Operational Case for Bulk Powers”p.8 には、改正前の根拠法が記載されている。

20 インターネット接続記録の定義は 3 編の 62 条(7)にあるように、コミュニケーション・データの一部である。しかしながら、他のコミュニケーション・データにはないような利用制限がかかっている。(62 条)。後述 p.13 の 3) 表参照。

(4) 調査権限の監督のための新たな職位の創設と調査権限に関する令状発出に際する承認手続きの新設などの規定が盛り込まれた。

調査権限全般を統合的に監督する調査権限コミッショナー（Investigatory Power commissioner）職と、司法コミッショナー（Judiciary Commissioner）職が新設されて（注 16 参照）、国務大臣が令状発出を許可する際に、司法コミッショナーの承認を要することとされた。この仕組みは、double lock と呼ばれている。

(5) 政府は草案に関する事前審議において議会から出された提言に関して、以下のように応えたとしている。

1）技術的定義を見直し、またどのように権限が行使され、なぜ必要なのかを説明するために、法案と併せて付属文書を提出すること

2）プライバシーの保護措置を、より明確かつより強力にすること

3）委員会の提言に応じて、インターネット接続記録の保存のための実施計画に関して、産業界とより緊密に協議すること

(6) 法案審議は、議会審議の各段階において、調査権限の必要性、プライバシーに関する懸念と保護措置の強化、double lock 強化など、数多くの論点に関して活発な議論が行われた。またその議事録も、審議後にすみやかに公表されている。

下院の審議において、以下の点について政府修正案が提出され可決されている。

＊プライバシー原則と保護

＊違法傍受に対する民事責任

＊令状を修正する場合の司法コミッショナーの承認

＊national security notice、technical capability notice を発出する場合の司法コミッショナーの承認

＊労働組合の正統な活動に対する保護措置

＊報道資料に関するコミュニケーション・データへのアクセスに関する保護および医療記録を含むバルク・パーソナル・データに関する保護措置

(7)調査権限が強化された面と制約が加えられた面という視点からみると、以下の特徴がある。

1）調査権限が強化された面

＊インターネット接続記録の取得・保存が可能になった。

＊バルク機器干渉が可能になった。

2）調査権限が制約された面

＊プライバシーに関する一般的義務規定が新設されて、国務大臣や司法コミッショナー

の令状等発出に関する判断において配慮すべき事項となった。
＊各種のプライバシーの観点からの保護措置規定が強化された。
＊新たに調査権限コミッショナーおよび司法コミッショナー職が創設されて、調査権限行使に関する監督体制が強化された。

5. 特定データとバルク・データ

一般人のプライバシー侵害のリスクが大きなバルク令状としては、通信傍受、コミュニケーション・データ取得、機器干渉、バルク・パーソナル・データセット（BPD：bulk personal dataset）の 4 つが認められている。バルク令状を特定人、特定機器を対象とする令状および特定のコミュニケーション・データの取得許可と比べると、令状申請権者、令状発出者、発出要件などの手続き要件が厳しくなっている。

(1) 4 つのバルク令状に共通する事項と議会における議論
＊バルク権限は、権限の明確性と範囲、その合法性、有効性および保護措置に関して、法案でもっとも議論が行われた分野の一つである。
＊バルク令状の申請権者は、インテリジェンス機関の長に限定されており、法執行機関の長には認められていない。上記インテリジェンス機関は、具体的には、保安部、秘密情報部および GCHQ の 3 機関[21] であり、国防 Intelligence にはバルク令状の取得権限は認められていない。
＊通信傍受令状および機器干渉令状に関しては、特定対象向けの令状は英国内外に及ぶのに対して、バルク令状は英国外の通信や機器に対象が限定されている。
＊バルク令状発出には、司法コミッショナーの事前承認が必要である。但し、バルク機器干渉令状およびバルク・パーソナル・データセット（BPD）令状のうち特定 BPD 令状については、緊急時には例外的に事後承認で良いと規定されている。
＊インテリジェンス・安全保障委員会委員長は、下院の審議において、今日のインターネット利用の現状を考えればバルク権限は必要である、また膨大なバルク・データの 99%以上はインテリジェンス機関によって見られることはないので、個人のプライバシーが損なわれることはないと述べている。
＊国務大臣の特定通信傍受、特定機器干渉令状発出許可および特定のコミュニケーション・データ取得許可の根拠・理由は、① 国家安全保障、② 重大犯罪の防止・探知、③①に係る経済的繁栄（economic well-being）があること、の三つである。

バルク令状の許可発出の根拠・理由としては、この①から③の根拠・理由に加えて、さらにこれらの理由・根拠よりも詳細なレベルの「特定の運用目的（specified operational purpose)」があることを要すると規定されている[22] 。

---

[21] インテリジェンス機関（Intelligence Service）は、8 編 263 条において、 Security Service(保安部)、Secret Intelligence Service(秘密情報部)、or GCHQ を意味すると規定されている。
[22] 法案の付属文書として議会に提出された“Operational Case for Bulk Powers”においては、高度の秘密性があるので運用目的の全面的な開示は困難であるとしつつも、テロ対策、敵対的な勢力への対策、重大

この「運用目的」に関しては、インテリジェンス機関の長が現行維持している「運用目的一覧」にある目的から特定すること、この「運用目的一覧」は国務大臣の承認を得ていること、国務大臣は「運用目的一覧」の写しを 3 カ月末毎に、議会のインテリジェンス・安全保障委員会に提出すること、首相はこの「運用目的一覧」を少なくとも年 1 回は審査しなければならないことが、6 編の各章に規定されている。バルク令状の発出に当たっては、この面においても特定令状の発出よりも厳重な手続き規定となっている。

(2) 特定取得とバルク取得の比較

以下は通信傍受令状、機器干渉令状、コミュニケーション・データ取得に関して、特定対象データとバルク・データの規定の比較を行う。また、比較対象がないバルク・パーソナル・データセット令状については、他の令状と同様の項目で規定内容を述べる。以下の表を要約すると、いずれにおいてもバルク令状発出に関しては、要件が加重されている。これは裏返してみると、バルク令状がプライバシーを侵害する恐れがより強いことを意味しているともいえる。

1) 特定通信傍受令状とバルク通信傍受令状の比較

	特定令状（2 編）	バルク令状（6 編 1 章）
令状の種類	3 種類：傍受、検証、相互支援	1 種類
調査範囲・内容	英国内外	海外（受発信者の一方）
申請権者	インテリジェンス機関、法執行機関､国防インテリジェンス機関など	インテリジェンス機関（MI5、MI6、GCHQ の 3 機関）の長
発出権限者	国務大臣、Scottish Ministers	国務大臣
発出根拠・理由	1）国家安全保障 2）重大犯罪の防止・探知 3）1）に係る経済的繁栄	左欄 1)~3) に加えて「特定の運用目的(specified operational purpose)」があること
発出手続き	緊急時（事後承認で良い）を除き、司法コミッショナーの事前承認が必要	常に司法コミッショナーの事前承認が必要であり、緊急時の規定はない
有効期間	6 か月、更新時 30 日	6 か月、更新時 30 日

2) 特定機器干渉令状とバルク機器干渉令状の比較

	特定令状（5 編）	バルク令状（6 編 3 章）

犯罪への対処を例として挙げている。 出典：同文書、pp.24~25

令状の種類	2 種類；機器干渉、検証	1 種類
調査範囲・内容	英国内外	海外（受発信者の一方）
申請権者	インテリジェンス機関、国防インテリジェンス機関、細則 6 の 1～2 編の表にある法執行機関	インテリジェンス機関の長
発出権限者	国務大臣、Scottish Ministers、上記法執行機関の長	国務大臣
発出根拠・理由	1）国家安全保障 2）重大犯罪の防止・探知 3）1）に係る経済的繁栄	左欄 1)~3）に加えて「特定の運用目的」があること
発出手続き	緊急時（事後承認で良い）を除き、司法コミッショナーの事前承認が必要	同左
有効期間	6 か月、更新時 30 日	6 か月、更新時 30 日

3）コミュニケーション・データ（インターネット接続記録＝ICR を含む）の取得許可とバルク取得令状の比較

	コミュニケーション･データの取得許可（3 編）	バルク取得令状（6 編 2 章）
令状の要否	令状は不要で許可で良い。ただし ICR については許可の要件が他のデータよりも加重されている	令状が必要
調査範囲・内容	英国内であるが、域外適用の規定がある	英国内外
申請権者	細則 4 に記載のある機関 地方自治体	インテリジェンス機関の長
発出権限者	申請機関の指定上級者	国務大臣
発出根拠・理由	1）国家安全保障 2）重大犯罪の防止・探索 3）1）に係る経済的繁栄 など、10 の事由	左欄 1)~3）に加えて「特定の運用目的」があること
発出手続き	自治体の場合には治安判事などの許可が必要。報道源が対象の場合には司法コミッショナーの事前承認が必要	常に司法コミッショナーの事前承認が必要
有効期間	1 カ月、更新時 1 カ月	6 か月、更新時 30 日

なお 4 編のコミュニケーション・データの保存は、国務大臣が電気通信事業者に保存通知（retention notice）の発出により行うが、司法コミッショナーの事前承認が必要で、有効期限は 12 カ月以内。

4) バルク・パーソナル・データセット（BPD：bulk personal dataset）令状

＊令状の種類：クラス BPD 令状、特定 BPD 令状の 2 種類[23]

＊申請権者：インテリジェンス機関の長またはその代理人

＊発出権限者：国務大臣

＊発出根拠・理由：国家安全保障など他のバルク令状と同じ。

＊発出手続き：国務大臣が緊急時であると判断する場合を除き、司法コミッショナーの事前承認が必要。なおクラス BPD 令状の場合には、この緊急時の例外規定はない。

＊令状の有効期間は 6 カ月、更新時 30 日

6. 令状・許可・通知における保護措置の類型

プライバシー保護強化の観点から、IPA 2016 には様々な保護措置があるが、大別すると次の類型になると考えられる。各編の項目については別紙 1 参照

(1) 特定の人・情報に関する保護措置

・議会議員、法的特権に服する事項、秘匿性のある報道資料、報道の情報源

(2) 令状等の執行に関する制限規定

・資料の保存、検証、開示に関する保護措置

(3) 事業者に対する義務

上記の保護措置規定にも関連して、各編において事業者への通知方法、事業者の協力義務や守秘義務、義務違反に対する措置が規定されている。この事業者の義務について、各編の規定を比較したのが別紙 2 である。

7. 監督の仕組み（oversight arrangements）（8 編）

「4」で述べたように IPA 2016 の特徴点の一つは、新たに調査権限コミッショナーと司法コミッショナー職が創設されて、調査権限行使に関する監督体制が強化されたことである。両コミッショナーの選任方法および役割などは以下の通りである。

(1) 選任方法と地位保障

＊高位の司法上の地位（high judicial office[24]）にある人々の中から、司法関係者の同意を得て首相が任命する。なお、司法コミッショナーの選任に関しては、上記に加えて調査権限コミッショナーの同意も必要である。

---

[23] 特定 BPD 令状は、クラス BPD 令状の類型に該当しない場合、または該当するが 202 条(1)から(3)の規定によりクラス令状で取得することが制限される場合に発出される。

[24] この high judiciary office は、憲法改革法 2005 の 3 編の意味である。同法 3 編 25 条において、最低 2 年以上 high judiciary office に在任していることが、最高裁判事への任命資格の一つとなっている。

＊任期は 3 年で再任可。
＊地位保障規定があって、議会両院の決議で罷免されない限り、任期途中で職を免じられることはないが、任命後に破産宣告などの欠格事項が生じた場合には、首相は罷免することができる。

(2) 役割
＊調査権限コミッショナーは、全体的な監督（oversight）の役割を担い、司法コミッショナーは、令状発出などに際する承認を行う。
＊両コミッショナーの権限・役割は、8 編 1 章に詳細に規定されているが、調査権限コミッショナーの多くの監督事項は 229 条に規定されている。そのうちの主要事項としては、以下の事項が挙げられる。

- 通信傍受、コミュニケーション・データの取得および保存、2 編 1 章または 6 編 1 章に基づく二次データまたは関連システム・データの取得、および機器干渉に関して公的機関が法的役割を果たすことに関して、監査（audit）、監察（inspection）、捜査（investigation）の方法を含む審査（review）
- インテリジェンス機関のバルク・パーソナル・データの取得、保存、利用に関する審査
- 252 条の national security notice の通知および運用に関する審査
- 特に保護措置運用におけるプライバシー保護の審査

＊首相は、調査権限コミッショナーや議会のインテリジェンス・安全保障委員会に対して、230 条に関する事項について指示することができる。またこの指示は公益などに反すると判断する場合を除き、公表しなければならない。首相に対して原則として公表義務を課すことは、指示が適切であるかについて外部からも判断できるように配慮した規定であると考えられる。
　これらの規定をみると、調査権限コミッショナーは司法部門の出身者から選出されるが、行政府から独立した司法機関ではなく、いわば行政内部の独立委員会的な位置づけであると考えられる。
＊調査権限コミッショナーは、司法コミッショナーでもある。また、調査権限コミッショナーは、自分で調査権限コミッショナーの役割を遂行するか、他の司法コミッショナーにその調査権限の一部を委任することができる。但し、他の司法コミッショナー任命の同意などに関しては委任できない。

8. その他の規定（9 編）

(1) 多くの種類の令状や許可の発出が規定されているが、248 条において、国務大臣が令状等を発出する際に、令状および許可を組み合わせ（combination of warrants and authorisations）て、一つの文書で行うことに関して細則 8 で定めるとの規定がある。

細則 8 には詳細な規定が置かれていて、9 ページに及んでいる。

(2) 事業者に協力義務を課す場合に、国がその協力に伴うコストを負担することも規定されている（249 条)。

(3) National security notice の規定(252 条)

国務大臣は国家安全保障上必要かつ比例的であると判断する場合に、司法コミッショナーの承認を得て、英国内の電気通信事業者に対して、National security notice（国家安全保障通知）を交付する。

National security notice は、特に IPA 2016 以外の他の法律の下でのインテリジェンス機関の活動への支援を、電気通信事業者に求める規定である。支援内容としては、インテリジェンス機関が行う行為を容易にすること、（Civil Contingencies Act 2004 の 1 編の意味[25] における）非常事態に対処すること、インテリジェンス機関が安全かつ効果的に役割を遂行するために、電気通信事業者がサービスまたは施設提供を含む行為を行うことである。

(4) Technical capability notice の規定（235 条）

National security notice が IPA 2016 以外の法律の規定のもとでの電気通信事業者への支援を求めるものであるのに対して、Technical capability notice は IPA 2016 における令状と併せて、事業者に交付される通知である。

国務大臣は、本法律に基づいて発出する許可に関連して、求める支援能力（capability）を事業者が有することを確保するために必要であり、事業者に求める行為が比例的であると認めた場合で、司法コミッショナーの承認が得られた場合に、この通知を交付する。

本条における許可とは、2 編、5 編、6 編の規定により発出された令状および 3 編の規定により発出された許可または通知を意味する。

通知を受けた事業者は、施設やサービスの提供、所有・運用している装置、通信またはデータに対する電子的保護の取り外しに関する義務を負う。

対象になる事業者は、National security notice では電気通信事業者のみであるのに対して、Technical capability notice では、郵便事業者、電気通信事業者、またはこの二つの事業の事業者になることを申請している者である。

国務大臣は規則を制定して、事業者に対する義務を規定することができるが、この規則制定時には、245 条に規定されている技術アドバイザリー・ボードおよび関係者と協

[25] 同法 1 編 1 条において非常事態（emergencies）として以下の三つの出来事または状況が規定されている。① 英国内における人間に関する福祉（human welfare：人命の喪失・病気・負傷、財産への損害、金銭・食料・水・燃料供給の途絶、通信システム・交通・医療サービスの途絶など）に関する重大な損害への脅威。② 英国内における環境に関する重大な損害への脅威（生物上・化学・放射線に関する土地・水・大気汚染および動植物の生命破壊）③ 英国の安全に関する重大な損害への脅威である戦争またはテロリズム

議しなければならない。

(5) National security notice および Technical capability notice の共通事項
＊notice の交付に際しては、司法コミッショナーの承認を要することに加えて、発出前に通知の交付を受ける事業者と事前協議を行うことなどが定められている。
＊通知を受けた事業者には、通知に対する遵守義務が課されるとともに、通知の受取自体および通知内容に関して守秘義務が課されている。また事業者のこれらの義務違反行為に対しては、刑事罰を課すことおよび injunction の手続き（英国においては不作為命令だけではなく、作為命令も含む）を行使することが可能である。（別紙 2 注 5 参照）

9. インテリジェンス活動におけるバルク・データの必要性と制約

(1) バルク・データの必要性

バルク・データの必要性については、以下の諸要素が複合しているものと思われる。
1) かつてインテリジェンス機関は「通信当事者を特定して通信内容を傍受すること」を基本に情報収集活動を行っていた。しかしながら、テロリストがあらゆる通信手段を駆使し、インテリジェンス機関が傍受対象として特定していない home-grown terrorist が出現するなど、「点と線を結ぶ」ことが必要になってきた。このため、情報収集対象者を特定しない、バルク・データ収集の必要性が高まっている。

ちなみに、スノーデンが暴露した NSA の著名な 3 つのプログラムのうち、プリズム・プログラムは特定の対象の通信内容とメタデータ（コミュニケーション・データに相当）の両方を OTT 企業から収集している。これに対して、電話のメタデータ収集では電話会社からメタデータを、またアップストリーム・プログラムではインターネットの基幹回線へアクセスして、通信内容とメタデータをバルクで収集していた[26] 。

なお英国では、GCHQ が「テンポラ・プログラム」によって、バルク・データ収集を行っていたことも暴露された。
2) 暗号通信の比率が高まってきていることが、バルク・データの必要性が高まる背景の一つである。土屋 [2007][27] は、暗号化と通信傍受の有効性に関して以下のように説明している。

> 電話口でいくらひそひそ話をしても意味はないが、電子メールの文章の暗号化（クリプトグラフィー）や画像にメッセージを埋め込む暗号化（ステガノグラフィー）といった技術を使えば簡単にメッセージの機密性を上げることができる。これがインテリジェンス・コミュニティには脅威となりつつある。

[26] スノーデンが暴露した NSA のシギント活動については、以下の文献を参照。林紘一郎・田川義博「サイバーセキュリティにおけるバルクデータの意義」情報セキュリティ総合科学第 8 号、2016 年 11 月
[27] 出典：土屋大洋 [2007]『情報による安全保障』慶應義塾大学出版会、p.138

3) この指摘は 2007 年になされたものであるが、暗号化の与える影響はそれ以降さらに大きくなっている。暗号通信の増加による通信傍受の有効性減少の対処策としては、次の二つの方法がある。

一つ目は、通信を発信者から受信者へ送るために必要であって、暗号化すると通信が届かなくなるコミュニケーション・データをバルクで取得する方法である。

二つ目は、通信傍受に加えて、通信が完了してコンピュータ、サーバやストレージに蓄積されている情報に、5 編や 6 編 3 章に規定されている機器干渉（equipment interference）によって、インテリジェンス機関が必要とする情報を得る方法である。この方法は英国や米国だけではなく、前述（注 12）したようにドイツでも行われている。

(2) バルク・データに関する制約

以上述べたように、効果的なインテリジェンス活動を行うためには、バルク・データの必要性は高いが、実際には以下のような制約がある。

1) バルク・データは膨大な情報を意味するものの、インターネット上を流通するすべてのデータを収集しているわけではない。

2) インテリジェンス機関が情報収集の対象とするような人々だけではなく、一般人をも対象にした情報収集であるために、バルク・データ収集は特定データの収集よりも、人々のプライバシーがより侵害されるリスクも大きくなる。

このバルク・データの問題にどう対処するかについて、以下で章を分けながら述べることとしたい。

10. スノーデンの暴露以降のバルク・データの扱い

インテリジェンス活動ないしバルク・データ利用がもたらすプライバシー侵害のリスクへの対応は、米国・EU と英国では異なっている。米国および EU-U.S.間のプライバシー・シールド協定で、バルク・データ収集が大幅に縮小された一方で、英国の IPA 2016 ではバルク・データ収集権限自体は縮小されていないからである。この経過とその背景は以下のとおりである。

(1) スノーデンの告発に対する米国の対応

米国では、テロリスト容疑者 A を特定し、A とテロリスト容疑者として特定されていないものの容疑者になる可能性のある未知の人物 B を探し出して、さらに A と B とのつながりから未知の容疑者 C を探し出す方法で、テロリスト・グループの全体を把握する。このように点と線をつなぐような捜査を行うには、バルク・データが役立つということで、9. 11 以降米国では幅広くバルク・データの収集・分析が行われていた。これを 2013 年 6 月にスノーデンが暴露したのである。

NSA はプリズム・プログラム、電話のメタデータ収集、アップストリーム・プログ

ラムの下で、米国内外の市民の個人データを大量に収集している現状は、米国法令で認められている活動なのか、法律に違反していないとしても憲法上許される行為なのかについて、多くの議論がなされた。

2013 年 6 月のスノーデンの暴露があってから間もない 8 月に設立された、オバマ政権下の検討委員会が 12 月に公表した最終報告書では、9.11 以降拡大された法的規定が、個人の自由・プライバシーおよび民主的ガバナンスを不当に犠牲にしているとして、46 の提言を行っている。

この報告書を基礎として、2014 年 1 月に PPD（Presidential Policy Directive：大統領政策指令）28 号が発出された。PPD 28 号では、インテリジェンス活動ないしバルク・データの必要性を指摘する一方で、その濫用によって自由・プラバシーが侵害されるリスクも増えており、自由・プライバシーと国家安全保障・人々の安全のバランスをどう取るかの議論が必要であるとして、以下のような指摘をしている。

① インテリジェンスは国家の安全と我々の自由を守るのに役立っている。9.11 以降はより重要になっている。

② 政府の行き過ぎのリスクや核心的な自由の一部を失うとの指摘が多くなった。

③ インテリジェンス活動は秘密なしには成り立たないので、公の場での議論が少ない。そのため、政府の行き過ぎの危険はそれだけ大きくなる。

④ 国家権力の特性を考えると、指導者が我々を信頼してほしい、収集したデータを濫用しませんというだけでは十分ではない。我々の自由は権力者を制約する法律に依存している。

上記のような問題意識に基づき、米国では PPD 28 号および 2015 年米国自由法（USA Freedom Act：同法は愛国者法 215 条が失効した 2016 年 5 月 31 日の直後の 6 月 2 日に成立した）によって、バルク・データ収集が制限されることとなった。

例えば PPD 28 号では以下の内容が定められている。

1) 新しいもしくは顕在化しつつある脅威はネットワークに潜んでいるので、それを見つけ出すにはバルク・データ収集が必要であるが、外国諜報活動の対象者以外の人々の情報も集めてしまうことになる。

2) バルク・データを収集する場合であっても，その利用は以下の6項目の国家安全保障目的への対処に限定する。(2条) ① 外国勢力等によるエスピオナージなどの脅威、 ② テロの脅威、 ③ 大量破壊兵器の開発、保有、拡散および利用、④ サイバーセキュリティ、⑤ 米軍や同盟軍または米国人や同盟国人への脅威、⑥ 国境を超える犯罪の脅威

3) シギント活動で収集された個人データへの安全管理措置を講ずる。（4 条）例：以下の方針と手続きに関する事項：情報共有・配布・保存の最小化。データセキュリティとアクセス。データの正確性 (quality)、監督 (oversight)

また米国自由法では、FISA (Foreign Intelligence Surveillance Act：外国諜報監視法) 402 条（ペンレジスターとトラップ・アンド・トレース権限）、同 501 条（旧愛国者法 215 条）お

よびNSL（National Security Letter：国家安全保障書簡）を根拠とするバルク・データ収集を禁止しており、代わって特定の選択語（selection terms）を利用することを要求している[28]。

この問題認識を国家安全保障[29]、インテリジェンス活動、人びとの自由・プライバシー・安全の3者関係で捉えると以下のようになると考えられる。

① 国家を成立させる3要素（主権、領土、国民）が失われると、基本的人権を実現する基礎が失われる。この観点からは、国家安全保障のための有効なインテリジェンス活動は必要である。

② 一方で、国家安全保障のための法制度が、プライバシーや市民的自由などの基本的人権を侵害するとすれば、国家の必要性と正当性の根拠が失われる。

③ 但し国家安全保障の目的には、「国民の生命と財産を守ること」も含まれているので、国家対国民という枠組みでの二者択一の問題ではない。

(2) EU-米国間のセーフハーバー協定の無効判決と新たなプライバシー・シールド協定の発効

スノーデンの暴露によって、2000年に発効したセーフハーバー協定が保障している保護レベルが、実際には十分に守られていないのではないかとの疑念がEU側に生じた。

そこでEU内部での検討を経て、2014年に入ってからEU-米国間で見直し交渉が始められた。この交渉途中の2015年10月に、EU司法裁判所がセーフハーバー協定の無効判決[30]を下したため、同協定の見直しは必須の状況になり、交渉が加速された。

---

[28] 注26 文献 p.24 および p.26

[29] 小林良樹は「国家安全保障」という言葉には普遍的かつ明確な学術上の定義はないとしつつも、「伝統的には、国家が、自国の領土、独立、および国民の生命、財産を、外敵による軍事的侵略から、軍事力によって、守る」とも定義され得る、とする。しかしながら、冷戦後の現在では安全保障には、幅広い要素が含まれるとの考えが多くなった。このために国家安全保障に寄与するためのインテリジェンス活動の範囲も、軍事的脅威の分析・評価から、国際テロ、国際組織犯罪やサイバーセキュリティまで広がっている、としている。注1 文献 pp.9～10

このことは、国家安全保障のためのインテリジェンス活動と法執行機関が担っている犯罪捜査のための情報収集・分析活動の境界があいまい化することを意味している。例えばテロ行為は伝統的な意味での国家安全保障の側面と重大犯罪の側面とを有している。

またインテリジェンス機関はテロリストに対する捜査権・逮捕権のような強制権限を有しておらず、このテロ行為への対処に関しては、インテリジェンス機関が上流、法執行機関が下流との位置づけになる。

インテリジェンス機関と法執行機関がテロ対策のための情報共有を行うとすれば、両者の境界は情報の面で少なくともテロ対策という観点からは限りなく融合することにもなる。

ドイツではナチス時代に両者の機能を併せもっていた秘密国家警察ゲシュタポへの反省から、戦後「警察と情報機関の分離の原則」を堅持してきた。ところが、テロ対策強化の観点から、2006年12月に「テロ対策データベース法」が施行されて、両者間での情報共有が行われるようになった。

この法律はこの分離原則違反ではないかとの指摘に対して、2013年4月の連邦憲法裁判所の判決では、国際テロ対策の公益は非常に大きいため、両者の情報交換は正当化されるとしたものの、この情報交換は、情報自己決定権の重大な侵害でもあり、緊急の例外的な場合にのみ正当化されるものであるとした。この分離原則と連邦憲法裁判所判決については、以下の文書を参照。渡辺富久子「ドイツにおけるテロ防止のための情報収集―テロ対策データベースと通信履歴の保存を中心に」外国の立法269（2016.9）pp.25~29

[30] 判決内容に関しては、以下の文献を参照。石井夏生利［2017］『新版　個人情報保護法の現在と未来』勁草書房、pp.305~312。宮下紘［2016］『事例で学ぶプライバシー』朝陽会、pp.109~112。

米国側では、前（1）の法的見直しに加えて、無効判決の理由の一つとして、権利を侵害された個人の救済措置が不十分であるとの判断に応えるように、2016 年 2 月に「司法救済法（Judiciary Redress Act of 2015）」が成立した。

これら一連の経過を経て、米国へ移転された EU 市民の個人データの保護水準が、EU の個人データの保護水準と「同等な水準にあると認定され」、新たに 2016 年 7 月にプライバシー・シールド協定が発効した。同協定では、米国企業の個人データの取扱に関する強い保護義務、米国政府の明確な安全管理措置と透明性の義務、および個人の権利の効果的な保護のために権利を侵害されたと考える EU 市民に対して、直接紛争解決手段を設けるなど、EU 市民の個人データ保護のために重層的な規定が設けられてた[31] 。

この協定の本文は 44 ページあるが、交渉経過と概要を除く 29 ページのうち、「3. プライバシー・シールドのもとで米国に移転された EU 市民の個人データへの米国の公権力によるアクセスと利用」が 22 ページと過半を占めていて、この問題に関心が集中していることが伺える。

特にバルク・データ利用の見直しに以下のように多くの記述がなされている。なお、この記述は EU 側の視点からのものである。

1）シギント活動は外国諜報または防諜目的のためにだけ行われるもので、収集は識別子（discriminants, e.g. specific facilities, selection terms and identifiers）を利用して、特定の外国諜報対象に向けて行われると、 ODNI（Office of Director of National Intelligence：国家情報長官室）は説明している。

2）特定データ収集は、バルク・データ収集よりも優先するのが一般原則である。また ODNI は、バルク・データ収集は大量（mass）でも無差別 （indiscriminate）でもなく、例外が一般化することはないことを保障している。

3) PPD 28号ではバルク・データ収集を行う必要がある場合には、特定データ収集を可能にするような代替策を優先するよう規定していて、バルク・データ収集は対象者の e－mail アドレスや電話番号のような識別子が利用できない場合にのみ行われる。

4）特定データを収集する際に一致語（identifiers）が利用できない場合に、可能な限り収集範囲を狭めるようにすると説明されている。米国のシギント活動はインターネットを流れている通信のわずかな部分しか扱っていない。また無関係な情報収集を最小化するために、できるだけ詳細にデータ収集範囲を絞るように、フィルターなどを利用していると説明されている。

5）バルク・データ収集を必要とする場合であっても、PPD 28号ではその利用は特定の6項目の国家安全保障目的に限定されている。

6）これらの制限はプライバシー・シールドの下で移転された個人データに適合的である。特に個人データの収集が米国外で行われる場合に適合的である。これにはEUから米国への大西洋横断ケーブルによって伝送中の個人データも含まれている。

---

[31] 以下の文献を参照。“Commission Implementing Decision of 12.7.2016:（中略）adequacy of the protection provided by the EU-U.S. Privacy Shield”（協定本文）と ANNEX Ⅰ~Ⅶ、“EU-U.S. Privacy Shield FAQ: Fact Sheet”, Brussel , 12 July 2016

7) 法律用語を用いてはいないものの、これらの原則は必要性と比例性の原則の本質を踏まえている。特定データ収集は明らかに優先されており、バルク・データ収集は特定データ収集ができない例外的な場合に制限されている。
8) 米国のインテリジェンス機関は、一般のヨーロッパ市民を含む誰に対しても、無差別な監視を行っていないと米国政府はEU委員会に保障している。 米国内で収集されている個人データに関しては、インターネット上を流通している全体のデータと比べれば、相対的に少数しか対象になっていないことは、NSL や FISA によるアクセス要求に関する経験的な証拠によって支持されている。
9) 正当なプライバシーや市民的自由を守ることと、シギント活動の実践的必要性とのバランスを取ることが必要であることを、米国政府は説明している。

プライバシー・シールドではこの他、need to know原則[32] によって権限のある者からのアクセスを限定すること、個人データを適切な保護の下で処理・蓄積することなどデータセキュリティに関する事項、データの配布と保存を最小化するような安全管理措置を取ること、保存期間は例外を除き最長5年に制限することなども規定されている。

(3) 英国の IPA　2016

(1) および (2) でみたように、米国における法的見直しや EU-U.S.間のプライバシー・シールドにおいては、バルク・データの収集を大幅に縮小している。

一方 IPA 2016 では、従来いろいろな法律に分散していた諸規定を、IPA 2016 に一元的に巻き取ったものの、バルク権限自体は縮小されていない。

PPD 28 号は、インテリジェンス活動の必要性とプラバシーや市民権的自由を守ることのバランスを取ることに腐心している。IPA 2106 でもバルク・データを含み調査権限は維持する一方で、プライバシー保護規定は強化されている。このように、英米ともいかにして、この両者のバランスを取るかという問題意識は共通している。

米国と英国でバルク・データに対する対処方針が分かれたのは、英国では伝統的にインテリジェンス活動に対する国民的な理解がある[33] とされており、このことがバルク・データの必要性をより是認する方向に働いているようにも考えられる。

---

[32] need to know 原則とは、「軍事情報など機密性の高い情報を扱う部門では『need to know の原則』が強調される。これは『(仮にアクセス権があっても) 現在の職務に必要な情報にしかアクセスしないし、させない原則』をいう。出典：林紘一郎・田川義博・淺井達雄[2011]『セキュリティ経営』勁草書房 p.69

[33] 小谷賢は「イギリスでは情報機関に対する信頼が厚く、スノーデン事件後もまだ過半数の世論は情報活動に理解を示している。イギリス人にとってテロとの戦いは、IRA による数々のテロ事件からその重要性が実感されたし、また歴史において情報機関が国を救ってきたという定説が、英国民の間に広く共有されているためだろう。」と述べている。出典 : 小谷賢 [2015]『岩波現代全書 079 インテリジェンスの世界史』岩波書店、p.196

11. 調査権限とプライバシー保護のバランス

(1) 1 編のプライバシーの一般的保護義務（2 条）では、令状等の発出時にプライバシーに配慮することに併せて、調査権限の必要性等にも考慮すべきことが規定されている。

(2) 新たな監督の仕組み：調査権限コミッショナーと司法コミッショナー

調査権限コミッショナーおよび司法コミッショナーの役割に関する 1 編と 8 編には、国家安全保障などのための調査権限の必要性・比例性とプライバシーの両方を考慮することを両者に求める規定があるが、同様の規定は各編にもある。

なお、米国ではプライバシーと並んで市民的自由（civil liberties）を守ることも規定されているが、IPA 2016 ではプライバシー保護のみについて規定されている。

2 編 23 条では、司法コミッショナーが令状発出を承認する際には、① 令状の発出根拠・理由に関してその必要性および比例性があるかを判断すること、② 裁判所が司法審査を行うのと同じ原則を適用すること、③ 2 条において課されている義務の遵守に関して十分な配意をすること、が定められている。またこの規定と同趣旨の規定が、各令状等の発出を定めた各編にも置かれている。

このように令状等の発出に際して、その必要性・比例性とプライバシーの保護義務の両方を判断要素としなければならないことが定められている。

また「7(2)」で述べたように、調査権限コミッショナーは、特に保護措置の運用についてプライバシー保護状況を審査することが定められている。

一方で 229 条(6)において、本法の役割を果たすうえで、司法コミッショナーは安全保障など令状発出の根拠・理由に関する公益に反すると考えられる行動をとってはならないこと、また 229 条(7)において、以下のことを行わないようにすべきことが規定されている。

① インテリジェンス機関や法執行機関の運用（operation）を阻害すること
② 当事者の安全またはセキュリティを損なうこと
③ インテリジェンス・サービス、警察力、政府省庁または軍隊の運用の有効性を不当に害すること

これらの規定は、司法コミッショナーが役割を遂行する際には、プライバシー保護と並んで安全保障目的など令状等の発出の必要性や比例性を考慮することに加えて、調査権限を行使する機関の運用を阻害しないことを定めたもので、プライバシーと調査権限行使の円滑な使命遂行の両立を求めている規定と考えられる。

(3) 2016 年 8 月に議会に報告されたアンダーソンの「バルク権限レポート」[34]

1）この報告書において、アンダーソンはバルク・データ収集と保存が人権問題として

[34] 正式な文書名は“REPORT OF THE BULK POWERS REVIEW by DAVID ANDERSON Q.C. Independent Reviewer of Terrorism Legislation” August 2016 である。

の国際的なプライバシー保護と両立するかについて、以下のように述べている。
＊バルク権限はその定義上、国家安全保障への脅威や重大犯罪への関与の容疑がほとんどない非常に多くの人々のデータに対して、国家がアクセスする可能性がある。
＊これらの権限のいかなる濫用も、無実の人々へ特に幅広い効果を及ぼし得る。
＊濫用が探知できないまま、可能であるとするならば、大きな不信感が生じ得る。
＊上記の要素は、それ自身、バルク権限を放棄する理由にはならないが、バルク権限の利用は、それを不可欠とする運用事例があり、適切で目に見える保護措置に従ったものである場合にのみ是認されるべきである。
2）またこの報告書では、バルク権限の実態について以下のように述べている。
＊バルク傍受権限は GCHQ のみが、カウンターテロやサイバー防衛などの分野で利用している。バルク取得権限は MI5（保安部）と GCHQ が、BPD 権限は MI5（保安部）と MI6（秘密情報部）が利用している。
＊調査した大多数の事例では、バルク権限を他の特定令状の権限やヒューミントなどの手段で代替することはできない。
＊GCHQ のインテリジェンス・レポートは、50%弱はバルク傍受から、約 5%はバルク取得令状から、約 20%は特定機器干渉から得られたデータに基づいている。
＊バルク機器干渉権限は（現在認められていないし）今まで利用されたことがない。バルク機器干渉は、あまり利用されないであろうし、特に強力で技術的な監督が必要である。

12. バルク・データの各局面におけるプライバシー侵害リスク

プライバシー理論に関して活発な問題提起を行っているダニエル・ソローヴは、プライバシーを多元的・文脈的に理解するためにプライバシー類型論を提起している。

「この類型論は、社会的に認識されたさまざまな種類のプライバシー侵害を特定し、理解する試みであった、この枠組みによって法廷や政策立案者がプライバシーとそれに対立する利害との間でよりよい均衡を実現できることを筆者は望んでいる[35]。」と述べ、具体的な類型論として、情報収集、情報処理、情報拡散（information dissemination）、侵襲（invasion）の 4 つの局面を挙げている。

このソローヴの類型論を参考に、IPA 2016 におけるプライバシーの各局面を、収集局面、検証局面、保存・破棄局面および配布・開示局面に分けて考察する。

IPA 2016 には数多くの保護措置規定があるが、「6」で述べたように、大別すると特定の人・情報に関する規定と令状等の執行に関する制限規定に分かれている。後者に関する保護措置規定は収集局面が圧倒的に多く、他の局面に関しては以下の通りである。
・検証局面：152 条・155 条（6 編 1 章）、172 条・173 条　（6 編 2 章）、193 条・196 条　（6 編 3 章）、221・222 条・224 条　（7 編）

[35] 出典：ダニエル・ソローヴ（大谷卓史訳） [2013]『プライバシーの新理論』みすず書房、pp.11~12

・保存・破棄局面：92 条、129 条　(5 編)、171 条　(6 編 2 章)、191 条　(6 編 3 章)、223 条　(7 編)
・開示・配布局面：57 条・58 条・59 条　(2 編)、129 条・132 条・133 条・134 条　(5 編)、171 条・174 条　(6 編 2 章)、191 条　(6 編 3 章)

(1) 収集局面

調査権限に基づくデータの収集は、国家安全保障や重大犯罪の予防・探知などのために必要な情報を効果的に得ることを意図して行われるものであるが、その過程でこれらの必要情報につながらない膨大な人々の情報も同時に収集せざるを得ないため、本来的に人権侵害の度合いの高いものである。

したがって、調査権限の行使によって得られる利益・成果と個人の権利の比較衡量を行い、権利を上回る利益・成果が見込めるとの比例性が認められることが必要である。

議会審議の中では、バルク・データの収集に関して多くの議論がなされた。また前述した通り、米国の PPD 28 号、2015 年米国自由法およびプライバシー・シールドにおいては、バルク・データ収集が大きく制限されるようになった。また「13(4)」で後述するように、Transparency Report の統計数値も過誤件数を含め、収集局面に集中している。このように、バルク・データ収集がもたらすプライバシー侵害リスクに配慮する対処策に関心が集まっている。

他方でこのリスクに対して、それほど問題ではないとの以下のような意見もある。

①下院の審議において、インテリジェンス・安全保障委員会委員長は、「今日のインターネット利用の現状を考えればバルク権限は必要である。また膨大なバルク・データの 99%以上はインテリジェンス機関によって見られることはないので、個人のプライバシーが損なわれることはない」と述べている。

②「ポズナー（Richard A. Posner[36]）は、莫大な量の個人情報（データ）の収集がプライバシーに影響することを認めながら、（中略）コンピュータは意思を持っていないことから（中略）意思を持たない機械が情報を集めてもプライバシーが侵されたことにはならないので、プライバシー権の問題は生じないというのである。[37]」

しかしながら、仮に収集局面でのプライバシー侵害リスクはそれほど大きくないとしても、収集範囲を拡大し収集量が増大すれば、後工程での誤用・濫用のリスクも増大するので、やはり収集局面での比較衡量に基づく限定・制限は必要であると考えられる。

(2) 検証局面

この局面では特定データとバルク・データの両方で、例えばテロリストの特定に関して、false positive（テロリストではない人をテロリストとする誤り）や false negative（テロリストをテロリストではないとする誤り）など、検証誤りが発生することは避け

[36] 筆者注：米国連邦控訴裁判事であるとともに「法と経済学」の権威
[37] 出典：大林啓吾 [2015]『憲法とリスク』弘文堂、p.199

られないが、これには分析ツールの性能が大きく影響する。

また大量のバルク・データを保存して検証するためには、膨大なコンピュータ・ストレージ装置が必要になる。このためすべてのメタデータを長期間保存することはコスト的にも困難なので、前述した NSA のアップストリーム・プログラムでは、一定期間（通信内容・コンテンツは 3 日間、メタデータは 30 日間）保存[38] され、このバルク・データの中から抽出された必要情報は、別のデータベースに長期間保存されているようである。

XKeyscore[39] は「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る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[40]。」ので、本来目的外の検索、例えば反政府運動をしている活動家などのプロファイリングに利用されるリスクもある。

また本来、検証局面に移行せずに廃棄されるべき情報が、何らかの理由・過誤によって検証されるとのリスクもある。

(3) 保存局面・破棄局面

保存されたデータに対するサイバー攻撃や内部者の情報持ち出しおよび不適切な管理のリスクが考えられる。このリスクに対して、4 編 92 条（データの完全性とセキュリティ）では、電気通信事業者の義務として、以下の事項が規定されている。

① データが収納されていたシステムにおける状態と、同じ完全性および同じセキュリティ・レベルの保護を行うこと

② 適切な技術的・組織的方法によって、データが特別に許可された人物によってのみアクセスされ得るようにすること

③適切な技術的・組織的方法によって、データを偶発的または不法の破壊、事故によってデータの喪失や改変（alteration）、無許可または違法なデータの保存・処理・アクセス・開示から守ること

④ データ保存通知（4 編）の許可期間が経過したならば、また法によって他に許可されていないならば、データを破棄すること

⑤ データの破棄は、各月または事業者にとって実行可能であればさらに短い間隔で行ってよい。

(4) 開示・配布局面

開示に関する保護措置の規定の数が多いのは、本来の開示先ではない組織・人物に開示すると、調査権限を行使する本来的な目的から逸脱して、調査結果が外部に流出する

[38] 出典：「米国国家安全保障庁の実態研究」警察政策学会資料　第 82 号、2015 年 9 月、p. 117

[39] 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。注 38 文献 p.115

[40] 注 38 文献 p.119

ことでプライバシー侵害リスクが大きくなるからである。

以上各局面におけるプライバシー侵害リスクを述べてきたが、各局面におけるデータの扱いが適正に行われているかどうかを、誰が、いつ、どこで、どのような手段によって監査するのかという共通の問題が残る。

13. 調査権限活動の適正執行を確保するための課題

この課題は二つに分かれる。一つは、調査権限活動の目的・理由である安全保障や重大犯罪の防止・探知に役立つ、有効かつ効率的な活動を行えているかとの課題である。この点については、活動の根拠法である IPA 2016 およびその細則である code of practice の規定内容が、調査権限活動を行う機関のミッションと整合的かどうかが問われる。また有効な活動となるような分析ツールなどの技術開発を進め、かつ設備の充実を図ることも求められる。さらに組織整備や組織能力の向上も重要である[41]。

もう一つの課題は、調査権限を行使する組織が、その調査権限を濫用せずに、適正執行する方法であり、本章においてはこの点を担保するためのいくつかの方法について考察する。

(1) IPA 2016 や code of practice など一連の法体系において、濫用を防ぐ規定が整備されているかがまず問われる。これに関しては、1 編にプライバシー保護重視の観点からの規定が置かれたこと、また特定の人・情報に関する保護措置規定と令状等の執行に関する規定が置かれたこと、さらに第三者の監督・審査機能を強化する観点から調査権限コミッショナーや司法コミッショナーの制度が新設されたことが挙げられる。

以上のような規定の整備によって、従来よりも適正執行を確保する規定の充実が図られたと政府は強調しているが、評価視点としては、これらの規定が調査権限を行使する際の明確な判断・行動指針として実際に機能しているか、またその判断・行動が実際にどのように行われているかについてその組織外の人々が把握できるかが課題である。

(2) 立法機関である議会による統制・牽制機能

まず議会の調査権限法案の審議過程において、プライバシー保護などの観点から活発な議論がなされ、またその議論に基づき政府が修正案を提出して可決されるなど、立法権に基づく調査権限機関の行動の統制が行われている。

また調査権限の執行過程でも、Justice and Security Act 2013 の規定に基づき、インテリジェンス・安全保障委員会（ISC：Intelligence and Security Committee）の権限

[41] 2016 年 3 月に GCHQ 内に、National Cyber Security Center が正式に発足している。また組織の内部に異論を述べる部門を置くことの重要性を指摘する以下の文献を参照。ミカ・ゼンコ[2016]『レッドチーム思考：組織の中に「最後の反対者」を飼う』文藝春秋。なお本書では、「内省や直感に反するようなレッドチーム思考から最も恩恵を受ける組織が軍隊」であるので、「アメリカ軍の中で磨かれ、体系化された（p.71）」としている。またインテリジェンス機関でも、「代替分析チームの役割は、政策立案者に他の選択肢を考えさせ、主流分析官ができない形で未来を見せることにある（p.170）」と述べられている。

が強化されている。ISC は上下両院の 9 名の議員で構成されているが、議会の委員会ではあるものの、首相の指名に基づき議会によって任命されている。

監督権限としては、対象は IPA 2016 でインテリジェンス機関として指定されている 3 機関だけではなく、国防インテリジェンス機関や内閣府の合同インテリジェンス委員会（Joint Intelligence Committee）などに及んでいる。また監督権限が及ぶ範囲は、各インテリジェンス機関の行う個別のオペレーションにも及んでいる[42] 。

もっとも「英国の議会委員会は米国のものと比べると、権限や調査能力の点ではかなり限定されたもので（中略）ISC が情報機関の予算や人事承認権を有して」いないとの指摘もある[43] 。

このように英国においては、政府と議会の相互連携の下で、調査権限の適正執行の確保が図られているように考えられるが、この相互連携の背景には、「長い歴史の中で、行政府内の各組織の間及び立法府との間に collegiality（同輩的協力関係）」が育まれていると説かれている[44] 。

(3) 司法機能による統制・牽制機能

司法部門による特に人権に関する問題に関する統制・牽制については、EU 加盟国においては EU 司法裁判所の存在抜きには考えにくく、また Brexit 後の課題に関する考察も要するので、章を改めて「14」において述べる。

(4) 行政部門内部における調査権限の統制・牽制

これには二通りの方法がある。一つは行政部門内部ではあるが、調査権限を行使する機関の外部に監督・監査組織を設ける方法である。もう一つは調査権限を行使する機関内部に監査組織を設ける方法である。

1）インテリジェンス機関の外部からの統制・牽制による方法

英国では、調査権限コミッショナーや司法コミッショナーがその役割を果たしている。これらのコミッショナーは、司法において実績を有する人々の中から、首相が任命するものであり、特に調査権限コミッショナーは首相の指示を受けたり、首相に報告したりする役割を担っていて、3 権の中では行政部門に属する組織ではないかと考えられる。

また 2017 年 2 月に、内務大臣が 108 ページからなる“HM Government Transparency Report 2017: Disruptive and Investigatory Powers” を公表して、インテリジェンス機関と法執行機関の活動について、制度的な解説を加えながら記述している。

このなかには、いくつかの統計も記載されている。例えば、テロ関連犯罪の逮捕者数、取得されたコミュニケーション・データの種別・取得機関別内訳・取得目的[45]、2015

[42] 注 1 文献 pp.192~193
[43] 注 3 文献 p.185
[44] 注 1 文献 pp.246～247
[45] トラッフィク・データが 48%、サービス利用情報が 2%、加入者情報が 50%である。機関別内訳は、

年の通信傍受コミッショナーへ報告のあった通信傍受に関する過誤件数の原因別内訳[46] や他の過誤件数が記載されている[47] 。

2) インテリジェンス機関内部における統制・牽制による方法

この方法は、英国でも当然実施されていると思われるが、詳細な情報は得られなかった[48] 。

3) 調査権限活動を公表する実例と意義

調査権限活動の公表（透明性の確保）が、市民からの調査権限活動への理解と信頼を得ることにつながるとの指摘[49] がある。

英国では、保安部（MI5)、(秘密情報部 MI6、GCHQ の公式ウエブ・サイトでは、かなりの情報が公開されており、保安部のサイトでは過去のトップ・シークレットのファイルも公開されている。以前は、その存在さえ明らかにされなかったことを考えれば、透明性は増しているといえる。

また前述したように、内務大臣が公表した“HM Government Transparency Report 2017: Disruptive and Investigatory Powers” では、2015 年の通信傍受コミッショナーへ報告のあった通信傍受に関する過誤件数の原因別内訳や他の過誤件数が記載されている。

このような適正執行から逸脱した件数が公表されることは、調査権限機関に対してより適正な執行を促す効果もある。また国民の調査権限の行使状況に関する「情報の非対称性」を低減することに役立ち、国民の側の状況判断力の向上にも資することになると

警察および法執行機関が 93%、地方自治体が 0.1%、インテリジェンス機関が 5.7%、その他が 0.5%と警察および法執行機関による取得がほとんどを占めている。取得目的は取得機関が警察および法執行機関がほとんどであることを反映して犯罪防止・探索などが 85.8%を占めている。

[46] RIPA15～16 条の保護措置侵害が 35%、通信傍受のアドレス間違いが 24%、法的権限のなく取得された蓄積通信が 11%、法的な権限のない通信傍受が 6%、通信傍受取消手続きの失敗が 22%、不正確な令状執行が 2%となっている。

[47] 米国では、連邦政府のテロ対策とプライバシーや市民的自由のバランスを取るミッションをもつ PCLOB（Privacy and Civil Liberties Oversight Board）が知られている。同委員会は大統領から指名され、議会の承認を得た 5 人の委員からなる委員会である。同委員会は、行政府のテロ対策やテロ関連法令の自由への配慮に関する審査を行うとともに、大統領や議会への助言や報告を行っている。またスノーデンの暴露後の 2014 年 1 月に公表した報告書において、愛国者法 215 条に基づいて行われていた電話のバルク・メタデータの収集を終了することを提言している。http://www.pclob.gov/

但し、英米の制度比較を行う場合には、英国の議会主権や司法の違憲立法審査権がないなど三権分立のあり方が異なることや、行政内部の統制・牽制の基本的な仕組みが異なっていることから、個別の制度の背後にある基礎的な制度的差異に留意が必要である。

[48] 米国では行政機関内部の監察組織として、連邦・州・ローカルの各機関に Office of Inspector General があって、NSA にもその組織が置かれている。http://www.nsa.gov/about/oig/ なお、英米の制度比較を行う場合の留意点は、注 47 と同じ。

[49] 「プライバシー保護の観点からは、『監視』に対する『監視』の必要性を認識すべきである。監視プログラムの透明性の確保はテロ対策の有効性を薄める可能性を有している一方で、市民からの監視への信頼を得ることができる。」出典：宮下紘 [2015]『プライバシー権の復権』中央大学出版部 p.208

考えられる。さらに、これらの報告書を時系列で比較することで、これらの機関のパフォーマンスの向上度も推定することも可能になると考えられる。

(5) 調査権限活動に携わる職員の意識

上記のような法および制度的な仕組みに加えて、調査権限活動に携わる職員が、活動のミッションとプライバシー保護のバランスを意識して活動することが重要である。

以上述べたように、調査権限の適正な執行を図る方法として、事前対処策としては法の規定に加えて code of practice に規定することおよび行政部門内部監査方針がある。事後対処策としては、議会における監査および Transparency Report のような行政による過誤件数を含む報告書の公表がある。これらに職員の意識づけが加わる。

14. IPA 2016 と Brexit

IPA 2016 の大多数の規定は、国務大臣が規則によって指定する期日に施行されるが、その前段として 2017 年 2 月 23 日に、code of practice 案[50] が公表されて、4 月 6 日までの 6 週間の期間で、意見募集がなされた。現在はこの意見募集に基づく検討が行われていて、今後議会へ提案されることになる見込みである。

但し、IPA 2016 が付属規定とともに施行されたとしても、IPA 2016 の修正を求められるかもしれない外部的不確定要因があるので、その点について述べておきたい。

(1) EU 司法裁判所の判決

EU データ保存指令（Directive 2006/24/EU on retention of data）は、法執行機関やインテリジェンス機関は、コミュニケーション・データを最短で 6 か月から最長で 24 か月まで保存するよう、電子通信事業者等に要請出来るとする指令である。このデータ保存指令に対して、Digital Rights Ireland によって訴訟が提起され、EU 司法裁判所は 2014 年 4 月 8 日、保存期間を定めることの必要性は認めつつ、「すべての者のすべてのコミュニケーション・データの保存」は比例原則に鑑みて基本権を侵害しているとして、無効判決を下した。

この判決への対応策として、英国政府は「2 (2)」で述べたように、2016 年末までの時限立法として DRIPA 2014 を成立させたが、EU 司法裁判所はこの DPIPA 2014 に対して、IPA 2016 が女王裁可を得た 11 月 29 日のすぐ後の 12 月 21 日に、無効判決を下した。

この判決はスウェーデンの事案と併合された裁判に対するものであるが、英国に関しては、EU プライバシー・電子通信指令（2002/58/EU）15 条（1）の解釈上、DPIPA 2014

[50] 細則 7 において、国務大臣が定める code of practice は、調査権限コミッションバーの審査を受けるとともに、制定前に公表して、集まった意見を検討して必要なら修正すること、議会の承認決議を得ることが定められている。

は EU 基本権憲章に違反するとして、以下の理由を述べている。

即ち、EU 基本権憲章 7 条・8 条・11 条・52 条（1）の趣旨に照らして、EU プライバシー・電子通信指令 15（1）条は、

1）すべての電子通信に関する全ての加入者・登録利用者の全てのトラフィック及び位置データの一般的かつ無差別な保存を規定する国の立法を、排除するように解釈されなければならない。（下線は付加）

2）トラフィックおよび位置データの保護と安全、特に権限のある国家機関の保存データに対するアクセスを規定する国の立法は、以下の場合には排除されるように解釈されなければならない。

①アクセスの目的が重大な犯罪に対処するためだけに限定されていない場合

②アクセスが裁判所または独立行政機関による事前審査を受けていない場合

③当該データが EU 内に保存されるという要件が課されていない場合。

もし 1）の「一般的かつ無差別な保存」を認めないとの判決理由が、バルク・データ利用を認めないとする意味であれば、EU 法および EU 司法裁判所では、バルク・データ利用は認められないことになる。

また同判決においては、英国からは「データ保存無効判決は、EU 基本権憲章 7 条・8 条の範囲を、ヨーロッパ人権裁判所の管轄であるヨーロッパ人権条約 8 条の範囲を超えて拡大するものか？」との第 2 質問も提起されている。これに対して、判決では提起は「相当とは認められない」と判示された。

EU 基本権憲章 52 条 3 項には、本憲章において、ヨーロッパ人権条約で保障されている権利に対応する権利が含まれている場合には、これらの権利の意味と範囲は、ヨーロッパ人権条約と同じものとすると規定されているので、EU 司法裁判所はこのように判断したものと思われる。

この判決の影響について、法的には専門的な論点を多数含んでいるが、英国の EU 離脱交渉の影であまり注目されていない。そして英国内では、IPA 2016 においては、上記裁判所の懸念は払拭されている、という見方が強いようである。また Brexit 後は EU 法および EU 司法裁判所の対象から外れるので、この判決の影響はミニマムである[51] との見方もある。

(2) Brexit 後における EU 法の適用

EU 法の適用を受けない米国が、プライバシー・シールドによって EU の個人データ保護と同等の水準にあるとの認定を受けて、EU 市民のデータ移転が可能になったこと

[51] David Anderson は、次項(2)の事情を考慮すべきとして、この見解に懐疑的である。以下の文献を参照。“Brexit: implications for national security” House of Commons Library, Briefing Paper Number CBP7798, 31 March 2017、p.22

で分かるように、Brexit 後であっても、英国が EU 市民の個人データを扱う場合には、IPA 2016 の規定を含めて、EU と同等の水準にあるとの認定を受ける必要がある。

前述したように米国およびプライバシー・シールドでは、バルク・データ利用が大きく縮小・制限されているに対して、IPA2016 では維持されているので、EU 法および EU 司法裁判所がバルク・データの法規定に対して否定的な判断を下す可能性がある。

(3) ヨーロッパ人権条約

英国が当初からの加盟国である Council of Europe（欧州評議会）のヨーロッパ人権条約およびヨーロッパ人権裁判所判決は、Brexit 後もその遵守を求められる。

ヨーロッパ人権条約の英国国内法に対する優位が示されたのが、1975 年のヨーロッパ人権裁判所の Golder v United Kingdom 判決である。この判決では英国は、「長らく議会主権の原則のもとで否定されてきた、違憲立法審査権の行使による人権保障の方式に等しい法的構造をもっていた」、と評されている[52] 。

もともと英国では、最高裁判所の機能は長い間貴族院が担っていた。これが 2005 年の憲法改革法によって 2009 年に最高裁判所が新設されるとともに、その役割を担うことになった。しかし英国では議会主権の原則によって、「国会の通常の制定法よりも上位の法は想定され」ていないし[53] 、この原則を否定するような成文憲法がないため、裁判所には違憲立法審査権はない[54] 。

この矛盾を調整するのが、ヨーロッパ人権条約の国内実施法として制定された Human Rights Act 1998 である。同法は国内法がヨーロッパ人権条約に抵触する可能性がある場合、国内法をヨーロッパ人権条約に適合的に解釈する義務（同法 3 条 1 項の条約適合解釈の原則）がるとされ、裁判所が可能な限り適合的に解釈したにも関わらず、ヨーロッパ人権条約に適合しないと判断されるときに裁判所は「不適合宣言」を行うことができる（4 条）。不適合宣言がなされると、大臣は救済命令にもとづき、不適合を除去するのに必要な立法を行うことができる（10 条）。

これらの規定によって、ヨーロッパ人権条約に関するヨーロッパ裁判所の判決と国内法の矛盾が一定程度解消されている。今後ヨーロッパ人権裁判所が EU 司法裁判所と同様の判決を行う可能性も十分あり得るので、(1)で述べた「上記裁判所の懸念は払拭されている」という英国内の見方が、ヨーロッパ人権裁判所でも認められるかは現時点で定かではない。

---

[52] 出典：高野敏樹「イギリスにおける憲法改革と最高裁判所の創設：イギリスの憲法伝統とヨーロッパ法体系の相克」上智法学 Vol.30 2010、p.92

[53] 出典：中村民雄「EU の中のイギリス憲法」早稲田法学 87 巻 2 号（2012）p.327

[54] 議会主権、憲法、ヨーロッパ人権条約に関しては、注 52 文献、注 53 文献および以下の文献を参照。中村民雄「欧州人権条約のイギリスのコモン・ロー憲法原則への影響」早稲田法学 87 巻 3 号（2012）

謝辞

バルク・データ研究会に参加され貴重なインプットをいただいた、メンバー諸氏に感謝する。ただし本報告書のうち事実の評価に関する部分は、著者 2 名の責任に属するものであって、必ずしも研究会全体を代表するものではないことをお断りする。

（別紙 1）（Additional） safeguards and restriction on use and disclosures

	（Additional ）safeguards :特定の人・情報に関する保護措置規定
2 編 通信傍受	26 Members of Parliament etc. 27 Items subject to legal privilege 28 Confidential journalistic material 29 Sources of journalistic information 54 Safeguards relating to disclosure of material overseas 55 Additional safeguards for items subject to legal privilege
5 編 特定機器干渉	111 Members of Parliament etc. 112 Items subject to legal privilege 113 Confidential journalistic material 114 Sources of journalistic information 130 Safeguards relating to disclosure of material overseas 131 Additional safeguards for items subject to legal privilege
6 編 1 章 バルク通信傍受	151 Safeguards relating to disclosure of material overseas 153 Additional safeguards for items subject to legal privilege 154 Additional safeguard for confidential journalistic material
6 編 3 章 バルク機器干渉	192 Safeguards relating to disclosure of material overseas 194 Additional safeguards for items subject to legal privilege 195 Additional safeguard for confidential journalistic material
7 編 BPD	206 Additional safeguards for health records 207 Protected data: power to impose conditions 222 Additional safeguards for items subject to legal privilege : examination 223 Additional safeguards for items subject to legal privilege : retention following examination

	Restriction on use or disclosure of material obtained under warrants 令状等執行に関する制約規定：罰則は令状申請権者にも適用される場合有
2 編 通信傍受	53 Safeguards relating to retention and disclosure of material 56 Exclusion of matters from legal proceedings etc. (他編にはない規定、但しこの規定の適用除外が細則3に規定されている) 57 Duty not to make unauthorised disclosures

	58 Section 57: meaning of “excepted disclosure” 59 Offence of making unauthorised disclosures
3 編　コミュニケーション・データの取得許可	*Filtering arrangements for obtaining data* 67 Filtering arrangements for obtaining data 68 Use of filtering arrangements in pursuance of an authorisation 69 Duties in connection with operation of filtering arrangements
5 編 特定機器干渉	(Supplementary provision) 129 Safeguards relating to retention and disclosure of material 132 Duty not to make unauthorised disclosures 133 Section 132: meaning of “excepted disclosure” 134 Offence of making unauthorised disclosure
6 編 1 章 バルク通信傍受	150 Safeguards relating to retention and disclosure of material 152 Safeguards relating to examination of material 155 Offence of breaching safeguards relating to examination of material 156条に56条をバルク通信傍受にも適用するとの規定がある。
6 編 2 章 バルク取得	171 Safeguards relating to the retention and disclosure of data 172 Safeguards relating to examination of data 173 Offence of breaching safeguards relating to examination of data 174 Offence of making unauthorized disclosure
6 編 3 章 バルク機器干渉	191 Safeguards relating to retention and disclosure of material 193 Safeguards relating to examination of material etc. 196 Offence of breaching safeguards relating to examination of material
7 編 BPD	220 Initial examinations: time limits 221 Safeguards relating to examination of bulk personal datasets 222 Additional safeguards for items subject to legal privilege : examination 223 Additional safeguards for items subject to legal privilege : retention following examination 224 Offence of breaching safeguards relating to examination of material

（別紙 2）令状等における事業者等の義務

1. 事業者[注1]への指示方法：a.令状の写しの送付　b.通知[注6]
2. 義務内容：c.協力義務等、d.守秘義務
3. 義務違反に対する措置：e.刑事罰、f.民事訴訟（差止命令:injunction[注5]など）

	1.指示方法	2.義務 c.協力義務 d.守秘義務	3.義務違反への措置
(特定)通信傍受令状：2 編	a	c: 43 条	e :43 条(7) f :43 条(8) e :57 条, 59 条 不法開示[注2]
(特定)機器干渉令状：5 編	a	c :128 条	f :128 条(7) e :132 条, 134 条 不法開示[注2]
コミュニケーション・データの取得許可：3 編	b	c :66 条 d：82 条	f :66 条(5) e :82 条 不法開示[注3]
コミュニケーション・データの保存：4 編	b	c :95 条(1), d (2) data integrity and security(92 条) disclosure of retained data(93 条)	f :95 条(5)
バルク通信傍受令状：6 編 1 章	a	特定傍受令状と同一 43 条適用(149 条(5))	e.f.43 条適用
バルク取得令状：6 編 2 章	a	c :170 条	f :170 条(5) e :174 条 不法開示[注3]
バルク機器干渉令状：6 編 3 章	a	特定機器干渉と同一 128 条適用(190 条(5)) 132 条~34 条適用(197 条)	f :128 条(7) e :132 条~134 条 不法開示[注2]
national security notice technical capability notice	b	c :255 条(9) d :255 条(8)	f :255 条(10)

注 1:電気通信事業者と郵便事業者の両方に協力義務:特定通信傍受令状、バルク通信傍受令状、Technical capability notice。電気通信事業者だけに協力義務：コミュニケーション・データ取得許可（通知）、コミュニケーションズ・データ保存（通知）、特定機器干渉令状、バルク取得令状、バルク機器干渉令状、National security notice

注 2：不法開示禁止の対象者は、電気通信事業者だけではなく令状申請関係者等も対象。

注 3：不法開示禁止の対象者は電気通信事業者とその従事者のみ

注 4:上記の規定の他一般的な規定として、不法傍受罪(3 条)、不法傍受に対する民事責任(8 条)、コミュニケーション・データの不法取得罪(11 条)、資料の検証の保護規定違反罪(155 条)(173 条)(193 条)の規定がある。

注 5:エクイティ訴訟の救済手段は、いろいろなものがあるが、差止命令と特定履行が一番典型的なものである。これらは、コモン・ローによる救済では著しい不公正が生じると考えられる場合にのみ、例外的に認められる救済である。事後的な金銭による損害賠償だけでは公正な救済ではない、ということが証明されてはじめて認められるのが、差止命令である。この差止命令には、一定の行為を行うことを禁止するものと、違法な状態を継続するのを差し止める、つまり違法排除を命ずる作為的差止命令がある。

出典：田島裕[2001]『イギリス法入門』信山社、p.200

注 6：この他の通知としては、Investigatory Powers Commissioner の発出する monetary penalty notices（細則 1　1 編）および information notices（細則 1　2 編）がある。