

英国調査権限法  
(Investigatory Powers Act : IPA2016)  
～調査権限法の構成・内容と調査権限をめぐる司法判断～

2024年6月20日

田川義博

元情報セキュリティ大学院大学客員研究員

# 1. IPA2016の条文構成

調査権限：国家安全保障およびテロを含む犯罪予防・捜査目的で、国の機関がインターネット上を流通し、またはその中に保存されている通信内容と通信データ等を取得・分析・利用できる権限は、英国で調査権限と呼ばれている。またEU市民の個人データの米国への移転に関する欧州委員会決定では、ガバメントアクセスと呼ばれている。

\*272条（1編～9編）および10の細則から構成されている。

\*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

\*3編：（特定）通信データ取得許可

\*4編：通信データ保存（通知）

\*5編：（特定）機器干渉

- ・特定の情報通信機器に保存されている通信と機器に関するデータが対象

\*6編：バルク令状（バルク通信傍受、バルク取得、バルク機器干渉）

- ・対象を特定しない大量の通信傍受や機器干渉、通信データの取得を認める規定

\*7編：バルク・パーソナル・データセット

- ・大量の個人データが収録されている電子データ

\*8編：監督の仕組み

- ・調査権限コミッショナーおよび司法コミッショナー職の創設  
(4編の保存データの安全管理は、Information commissionerの役割)

\*9編：雑則および一般的規定

\*細則

## 2. 調査権限の種類

### 令状(warrant)

\* 特定対象令状：通信傍受令状（2編）、機器干渉令状（5編）

\* バルク令状：通信傍受、通信データ取得、機器干渉（6編）、パルク・パーソナル・データセット（7編）

注1：特定令状は、法執行機関とインテリジェンス機関が取得できる。バルク令状の申請権者は、GCHQ(General Communications Headquarters)、MI5(Security Service)、MI6(Secret Intelligence Service)の3つのインテリジェンス機関に限定されている。また通信傍受および機器干渉のバルク令状は、通信当事者の一方が海外にいることが条件。

注2：IPA2016にはバルク（取得）の定義はない。米国大統領令14086号（2022年10月7日）では、「技術的および運用上の考慮によって、識別子（discriminants）を使用しないで、大量のシグントデータの許可された収集」と定義

### 許可 (authorisation)：特定対象の通信データの取得許可（3編）

注：令状取得と比較すると、許可取得手続きのハードルは低い。また許可件数の約95%は法執行機関による取得。

### 通知 (notice)

\* 通信データの保存通知（4編）

\* national security notice（9編252条）

注：電気通信事業者に対して、IPA2016以外の法律において、インテリジェンス機関の活動へ支援を求める規定

\* technical capability notice（9編253条）

注：電気通信事業者および郵便事業者に対して、IPA2016に基づく令状と併せて交付される通知

\* 9編の2つの通知では、発出前に交付対象となる事業者との事前協議を行うこととされている（255条）。

注：事業者には協力・守秘義務が課される。また協力の伴う必要経費については、国務大臣が適切と考える金額が支払われる(249条)。

### 3. 調査権限に関する司法判断1：取上げた判決

いずれの判決においても、国内法、EU指令および欧州委員会決定に対して違法・無効判決が下されている。

判決名	不適合性判断の対象
第1判決：データ保存指令無効判決 (CJEU) 2014年4月8日	1. EU基本権憲章に対して、同指令が不適合
第2判決： <u>DRIPA2014違法判決</u> (CJEU) 2016年12月21日	2. プライバシー・電子通信指令に対して、 英国国内法 (DRIPA2014)が不適合
第3判決： <u>IPA2016違法判決</u> (英国国内裁判所) 2018年4月27日	3. プライバシー・電子通信指令に対して、 英国国内法 (IPA2016)が不適合
第4判決： <u>Privacy International判決</u> (CJEU) 2020年10月6日	4. プライバシー・電子通信指令に対して、英国国内法 (1984年電気通信法94条、RIPA2000(21条等) が不適合
第5判決：La Quadrature du Nez判決 (CJEU) 2020年10月6日	5. プライバシー・電子通信指令に対して、フランス ・ベルギー国内法が不適合
第6判決： <u>Big Brother Watch判決</u> (ECHR) 2021年5月25日	6. 欧州人権条約に対して、英国国内法 (RIPA2000)が 不適合
第7判決：セーフハーバー無効判決 (CJEU) 2015年10月6日	7. データ保護指令に対して、欧州委員会決定が不適合
第8判決：プライバシー・シールド無効判決 (CJEU) 2020年7月16日	8. GDPRに対して、欧州委員会決定が不適合

注1：CJEU：EU司法裁判所 (Court of Justice of European Union)

ECHR：欧州人権裁判所 (European Court of Human Rights)

注2：8つの判決の4件を占める英国国内法に関する判決のうち、IPA2016に関する判決は1件のみ。

### 3. 調査権限に関する司法判断2：審理事項、不適合理由(1)

判決名	審理事項	不適合理由
第1判決	全ての人の全てのトラフィックデータの一律最長2年間の保管義務	全ての人の全てのトラフィックデータの一律最長2年間の保存義務は、比例原則を超えている。基本的権利への干渉の程度を規律する明確かつ詳細なルールを定めていない。
第2判決	トラフィックデータの全体的な保存義務、保存データへの国の機関のアクセス権限	一般的かつ無差別なデータ保存義務を規定している。国の機関のアクセスを重大犯罪の場合に限定していない。裁判所または独立行政機関による事前承認を得ていない。
第3判決	IPA2016（4編）	国の機関のアクセスを重大犯罪の場合に限定していない。裁判所または独立行政機関の事前承認を得ていない。（但し、IPA2016の4編は、一般的かつ無差別なデータ保存規定ではない。）
第4判決	インテリジェンス機関のバルク通信データへのアクセス	一般的かつ無差別なトラフィックデータおよび位置データを、インテリジェンス機関へ引渡すことを可能にする国内法は認められない。
第5判決	電子通信事業者への一般的かつ無差別な通信データの保存義務、特定対象の通信データのリアルタイム収集	一般的かつ無差別なトラフィックデータおよび位置データの保存を義務付ける国内法は、予防措置としては認められない。 （但し、当該加盟国が国家安全保障への重大な脅威に直面し、その決定が裁判所または独立行政機関による脅威の存在および保護措置遵守の検証に従う場合には、真に必要な期間認められる。）

### 3. 調査権限に関する司法判断2：審理事項、不適合理由(2)

判決名	審理事項	不適合理由
第6判決	バルク通信傍受、外国のインテリジェンス機関からのインテリジェンス情報の受取、通信事業者からの通信データの取得	バルク通信傍受には、かなりの濫用の可能性があるが、エンド・ツー・エンドの保護措置の規定がない。通信データ取得とともに、人権条約8条および10条に違反。
第7判決	欧州委員会のセーフハーバー決定のデータ保護指令に対する適合性	米国がEUと本質的に同等な保護水準を保障していることを認定していない。（干渉の）手段の範囲・適用および最小限の保護措置がない。（干渉の）手段の範囲・適用および最小限の保護措置に関して、明確かつ詳細な規定を置かなければならない。
第8判決	欧州委員会のプライバシー・シールド決定のGDPRおよびSCCに対する適合性	米国がEUと本質的に同等な保護水準を保障していない。干渉を認める立法には、範囲・適用に関する明確かつ詳細な規定が必要である。しかし米国では、監視プログラムの実施権限に制約がなく、最小限の保護措置がなく、救済の仕組みも不十分である。（同決定は無効、SCCは有効）

### 3. 調査権限に関する司法判断3：正当で必要と認められた調査権限

判決名	正当で必要と認められた調査権限
第1 判決	国際テロとの戦いは、一般的利益である。特に組織犯罪との戦いでは、電子通信利用に関するデータが特に重要なツール。従って、国の機関に対してデータへのアクセスを認めることは、一般的利益の目的を真に満たす。
第2 判決	犯罪防止・捜査・探知・訴追の分野では、重大犯罪と戦う目的だけが、保存データへのアクセスを正当化できる。
第5 判決	<ul style="list-style-type: none"><li>・ 一般的かつ無差別なトラフィックおよび位置データの保存については、当該加盟国が現在または予見できる将来に国家安全保障への重大な脅威に直面している場合で、このような決定が裁判所または独立行政機関による脅威の存在および保護措置遵守の検証に従っている場合には、真に必要な期間認められる。</li><li>・ 国家安全保障、重大犯罪との戦いおよび公共の安全への真の脅威を防止する目的で、厳に必要な期間に限定した、特定対象のトラフィックおよび位置データの保存は認められる。</li><li>・ トラフィックおよび位置データのリアルタイム収集は、一定の条件を満たす場合に、法的拘束力のある裁判所または独立行政機関の事前承認に従う場合に認められる。 など</li></ul>
第6 判決	バルク通信傍受は、加盟国が自国の国家安全保障への脅威を判定するためには、不可欠な重要性を有していることを認める。また外国のインテリジェンス機関から、インテリジェンス情報を受取ることも認められる。

### 3. 調査権限に関する司法判断4：各判決の比較

#### (1) 各判決に共通していると考えられる事項

調査権限の範囲および人権制約に関して、明確かつ詳細なルールを定めなければならないとの判断は共通しているように考えられる。明確かつ詳細なルールが定められていれば、調査権限を行使する側にとって、行ってよい行為かどうかの判断が容易になり、逸脱行為の抑制につながる。また人権制約を受ける側にとっても、不法な調査権限からの救済を求めやすくなると考えられる。

#### (2) 各判決で違いがあると考えられる事項

##### 一般的かつ無差別なトラフィックおよび位置データの保存義務規定の適合性に関する判断

EU司法裁判所の判決（第1、第2、第4、第5判決）のうち、第1、第2および第4判決では、一般的かつ無差別な通信データ保存規定は、EU法に照らして不適合であると判断されているのに対して、第5判決では、予防的措置としては認められないとしつつも、重大脅威の存在および保護措置遵守が、裁判所または独立行政機関による検証に従っている場合には、真に必要な期間認められるなど、他の判決よりも広範な調査権限を認めている。

またIPA2016の4編の規定は、この一般的かつ無差別な通信データの保存規定ではないとの英国国内裁判所の判決もある。欧州委員会の英国に対する十分性認定の審査においても、英国のバルク調査権限は制限と保護措置があるので、大量監視（mass surveillance）ではないと認定されている。

注：バルク調査権限については、米国ではスノーデンの暴露以来、EU市民の個人データの越境移転に関する取決め交渉において、見直し縮小の動きを見せたのに対して、IPA2016においては人権保障に関する規定の充実はなされたものの、バルク調査権限自体は縮小されておらず、対照的な対応となっている。

また欧州人権裁判所のBig Brother Watch判決でも、調査権限プロセスの各段階におけるプライバシー侵害リスクについて分析を行いつつも、バルク通信傍受の必要性については認めている。

## 4. 調査権限法に関する2つの課題

### 課題1：効果的・効率的な調査権限活動

人権（自由）を制約すると、安全が高まるというものではなく、安全は効果的・効率的な調査権限活動を行うことで達成される。脅威の変化や技術進歩を踏まえて、調査権限の内容・手法が、調査権限の目的にふさわしいかが問われる。英国政府は、この観点（fit for purpose）からの見直しを行うために、調査権限強化とともに、プライバシーや言論の自由に関する保護措置や監督の仕組みの強化を行うために、IPA2016の改正を行っている。このfit for purposeの視点からの見直しに関しては、「迅速性」が求められると考えられる。

### 課題2：調査権限の恣意的運用や濫用・誤用防止

課題1と共に、人権が不当に制約されないようにすることが求められる。この課題に対処するために、IPA2016には調査権限の範囲と制限の明確化、人権に対する保護措置、調査権限コミッショナー・司法コミッショナーなどによる監督、不法に権利侵害された人に対する救済の仕組みに関して数多くの規定がある。これらの規定については、制定過程を含めて「透明性」が求められると考えられる。

注1：保護措置規定は、大別すると人・情報に関する規定と調査権限執行に関する規定があって、調査権限の情報収集、検証、保存・破棄および開示・配布の各段階において、人権に対する保護規定が置かれている。

注2：監督は調査権限コミッショナー・司法コミッショナーの仕組みに加えて、議会による監督・統制が重要であり、英国議会ではJustice and Security Act2013などの規定によって、監督・統制が行われている。またこれに国内裁判所と欧州人権裁判所による司法的な統制が加わる。

## 5. 人権制約を認める法規定およびその制約の限界を定める法規定

### (1) EU法

\*EU基本権憲章：52条において、法に基づく場合で、権利や自由の本質的な尊重の下で、比例性原則に従った基本権の制限を認めている。

\*プライバシー・電子通信指令：15条(1)において、国家安全保障や犯罪への対処の目的で、必要、適切および比例的な手段によって、5条（通信の秘匿性）、6条（トラフィックデータ）、9条（位置データ）などの規定を加盟国が制限することを認めている。

\*GDPR：23条において、国家安全保障などのために、その制限が基本的権利および自由の本質的部分を尊重するもので、必要かつ比例的な措置を講ずる場合には、12条から22条などの義務・権利の適用を制限する国内法を認めている。

(2) 欧州人権条約：私生活及び家族生活、住居および通信の尊重が8条(1)に規定されている。同条(2)において法律に基づき、国の安全や犯罪防止などのために、この権利が制限される場合があることを認めている。

### (3) IPA2016における調査権限と人権保障の両立を図る規定

2条において、令状等の発出時にプライバシーとともに、調査権限の必要性にも配慮すべきとされている。また司法コミッショナーは、令状発出の審査において公益に反する行動を取らないこととの規定（229条(6)）があり、同条(7)では、インテリジェンス機関や法執行機関の運用の有効性を不当に害する行動を取らないことが規定されている。

これらの規定は、調査権限行使とプライバシーなどの人権尊重の両立を求めている規定と考えられる。

## 6. 調査権限と人権の関係および「通信の秘密」の保護法益

### (1) 調査権限と人権の関係

国家成立の3要素の一つである主権が敵対勢力によって失われると、国民の生命・財産に悪影響があるとともに、人権の存立基盤が失われるので、国家安全保障には不可欠な価値がある。一方で国家安全保障のための法制度が人権侵害を引き起こすなら、民主主義国家としての正当性が失われる。

国家安全保障に寄与する目的を有する調査権限は必要な権限ではあるが、一方濫用の歴史もあり、人権を過度に制約する可能性を有している。このため調査権限法においては、司法判断で示されたように、効果的・効率的な調査権限行使と人権保護の両面に関して、明確かつ詳細なルールを定めることが要請される。また法執行に関する第3者による監督も必要である（229条）。

注：調査権限コミッショナーは、調査権限等の執行状況に関する年次報告書を公表している（234条）。

### (2) 「通信の秘密」の保護法益

日本国憲法上の保護法益は、プライバシーと表現の自由であるとの解釈が通説である。「通信の秘密」との用語は使われていないものの、IPA2016および司法判断においても、この保護法益が論点である。

インターネット利用の進展に伴い、従来厳格に守られていた「通信の秘密」を制約する事象が生じている。その制約の一つとして、サイバー攻撃への対処のために、「通信の秘密」の制限がガイドラインで認められている。重要インフラである通信システムの機能維持が、事業法での「通信の秘密」の保護法益に加わると考えれば、安全確保のために、自由（憲法上の「通信の秘密」の保護法益）を制限することになる。「通信の秘密」を保護するために、「通信の秘密」を制限する、いわば「入れ子状態」になっていると考えられる。但し「通信の秘密」を制限する場合には、これまで分析してきたように、明確かつ詳細なルールを定めることが必要であると考えられる。