英国 IPA2016 と調査権限をめぐる司法判断

～調査権限（ガバメント・アクセス）の人権制約の許容度を探る～

2024 年 4 月

田川義博

（元情報セキュリティ大学院大学客員研究員）

目次

エグゼクティブ・サマリー ……5
はじめに ……8
1. IPA 2016 成立までの経過 ……9
1.1 EU データ保存指令[2006/4/EC] (2006 年 3 月 15 日)
1.2 EU 司法裁判所のデータ保存指令無効判決（2014 年 4 月 8 日）
1.3 DRIPA2014（時限法）の成立（2014 年 7 月 17 日）
1.4 IPA2016 の成立（2016 年 11 月 29 日）
2. IPA 2016 ……21
2.1 条文構成と調査権限の種類
2.2 議会における審議状況と法案修正
2.3 IPA 2016 によって強化された調査権限と調査権限行使に対する制限
2.4 バルク令状
2.5 特定令状・特定通信データ取得許可とバルク令状の比較
2.6 通知制度
2.7 電気通信事業者および郵便事業者の協力・守秘義務
2.8 令状・許可件数
3. IPA 2016 成立後の経過と IPA2016 の改正 ……34
3.1 EU 司法裁判所の DRIPA 2014 違法判決(2016 年 12 月 21 日)
3.2 英国国内裁判所の IPA 2016 違法判決（Liberty 判決）(2018 年 4 月 27 日)
3.3 IPA2016 の 2018 年改正.
3.4 EU 司法裁判所の Privacy International 判決（2020 年 10 月 6 日）
3.5 EU 司法裁判所の La Quadrature du Nez 判決（2020 年 10 月 6 日）
4. 欧州人権裁判所の Big Brother Watch 判決と英国政府の対応 ……57
4.1 欧州人権裁判所の Big Brother Watch 判決（2021 年 5 月 25 日）
4.2 Big Brother Watch 判決に対する英国政府の声明（2022 年 3 月 31 日）
4.3 調査権限コミッショナー年次報告書 2021（2023 年 3 月 20 日）
4.4 IPA2016(Remedial) Order 2023
5. 英国政府の IPA2016 の改正検討 ……65
5.1 IPA 2016 改正に関する検討視点と検討事項
5.2 IPA (Amendment) Bill（2023 年 11 月 8 日議会提出）
6. EU 市民の個人データを米国に移転する取決め（その 1） …… 71
～セーフハーバー成立からプライバシー・シールド発効まで～
6.1 セーフハーバー成立までの経過と欧州委員会決定
6.2 セーフハーバー見直し交渉の契機と経過
6.3 EU 司法裁判所のセーフハーバー無効判決（Schrems Ⅰ）

（2015 年 10 月 6 日）
6.4 セーフハーバー無効判決後の見直し交渉と
欧州委員会のプライバシー・シールド実施決定
7. EU 市民の個人データを米国に移転する取決め（その 2）……80
~プライバシー・シールド判決からデータ・プライバシー・フレームワークまで~
7.1 EU 司法裁判所のプライバシー・シールド無効判決(Schrems Ⅱ)
（2020 年 7 月 16 日）
7.2 プライバシー・シールド無効判決後の EU-米国間の見直し交渉
7.3 欧州委員会のデータ・プライバシー・フレームワーク実施決定
7.4 プライバシー・シールドとデータ・プライバシー・フレームワークの比較
7.5 欧州委員会の新 SCC（2021/914）実施決定（2021 年 6 月 4 日）
7.6 欧州委員会の英国に対する 2 つの実施決定
7.7 英国側の対応
8. 調査権限の人権制約に関する許容度……109
8.1 EU 司法裁判所、欧州人権裁判所および英国国内裁判所の判決分析
8.2 調査権限の適正執行を確保する課題 1：効果的・効率的活動
8.3 調査権限の適正執行を確保する課題 2：濫用・誤用防止を含む人権保障
8.4 バルク・データ収集・利用の必要性および人権制約
8.5 EU 法における人権制約およびその限界に関する規定
8.6 IPA 2016 における調査権限とプライバシー保護の両立を図る規定
8.7 調査権限の必要性と人権保障に関する基本的考え方
8.8 明確かつ詳細なルール
8.9 EU　司法裁判所の Schrems Ⅰ および Schrems Ⅱ 判決と IPA 2016
9. 自由と安全……126
9.1 国家安全保障概念
9.2 自由と安全の関係
9.3 プライバシーの価値とは
9.4 脅威の増大
9.5 「通信の秘密」における自由と安全
別紙：調査権限（ガバメント・アクセス）に関する動向と司法判断の時系列

エグゼクティブ・サマリー

国家安全保障および犯罪防止・捜査・探知などのために、インターネットなど情報通信ネットワークシステム上を流通し、保存されている通信内容や通信データを、取得・分析・利用する権限を、国の機関に付与する法律が米英独仏などで制定されている。この権限は英国法では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。

本稿は、調査権限（ガバメント・アクセス）の人権制約の許容度を探るために、以下の事項について調査・分析を行い、それによって得られたと考えられる知見について述べる。

1. 英国 IPA(Investigatory Powers Act：調査権限法)2016 の成立までの EU データ保存指令、EU 司法裁判所の同指令無効判決および DRIPA2014 成立の経過をトレースした後に、IPA2016 について、1）調査権限の種類（令状、許可、通知)、調査権限について特定令状（通信傍受、通信データ、機器干渉）とバルク令状（通信傍受、取得、機器干渉）の比較、3）調査権限に対する制限、人権保障のための保護措置、監督および救済の仕組み、4）事業者の協力・守秘義務、5）調査権限実施件数について調査・分析を行った。

   これによると、IPA2016 は国の機関へ調査権限を付与する規定とともに、司法判断を含め不十分であるとの批判はあるものの、人権保障のための数多くの規定を置いている。
2. 英国政府は司法判断を反映するために、IPA2016 の改正を行っている。これとともに、IPA2016 の成立後の調査権限に関する脅威の変化や技術進歩を踏まえて、IPA2016 の規定が法目的達成のためにふさわしいか（fit for purpose）の視点から改正検討を行い、2023 年 11 月に IPA(Amendment) Bill を議会に提出している。

   英国政府の調査権限に関する取組みのように、調査権限の効果的・効率的実施と濫用・誤用防止を含む適正執行を確保する両方の視点が重要であると考えられる。
3. 個人データの越境移転について、1）米国への移転に関する欧州委員会のセーフハーバー、プライバシー・シールドおよびデータ・プライバシー・フレームワーク決定の構成と内容、およびこの 3 決定の相互比較、2）欧州委員会の新 SCC（Standard Contractual Clauses）決定、3）欧州委員会の英国に対する十分性認定の決定、4）英国の EU に対する十分性認定および新 SCC 決定について調査・分析を行った。

4. 司法判断における調査権限（ガバメント・アクセス）の人権制約の許容度を探るために、EU 司法裁判所の 6 判決（EU データ保存指令判決、DRIPA2014 判決、Privacy International 判決、La Quadrature du Nez 判決、セーフハーバー（Schrems Ⅰ）判決、プライバシー・シールド（Schrems Ⅱ）判決、欧州人権裁判所の Big Brother Watch 判決および英国国内裁判所の Liberty 判決の 8 つの判決の審理内容および判決について調査・分析を行った。
5. この 8 つの判決においては、訴訟対象となった調査権限（ガバメント・アクセス）に対して、EU 法または欧州人権条約に照らして、いずれも違法または無効との判決がなされた。

   その理由としては、調査権限が犯罪に関しては重大犯罪との戦いに限定されていないこと、令状等の発出に関して裁判所または独立行政機関の事前承認を得ていないこと、一般的かつ無差別なデータの保存を義務付けていること、明確かつ詳細なルールを定めていないこと、エンド・ツー・エンドの保護措置がないことなどが挙げられている。

   また欧州委員会決定については、米国が EU と本質的に同等の個人データの保護水準を保障していないことをその理由としている。
6. 一方司法判断においては、正当で必要な調査権限として、国際テロとの戦いでは電子通信利用に関するデータが特に重要であり、国の機関にデータへのアクセスを認めることは一般的利益である、重大犯罪と戦う目的だけが保存データに対するアクセスを正当化できるとしている。これに加えて、一般的かつ無差別なデータの保存については他の判例では認められていないが、La Quadrature du Nez 判決では、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認定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との判決になっている。

   欧州人権裁判所判決では、バルク通信傍受は、加盟国が自国の安全保障への脅威を判定するために、不可欠な重要性を有していることを認定している。またバルク通信傍受の人権制約の程度は、その取得から選別、検証、利用の段階に進むについて大きくなるとして、エンド・ツー・エンドの保護措置が必要であると判決している。

   IPA2016 においても、情報収集段階、検証段階、保存・破棄段階および開示・配布段階ごとに保護措置規定が置かれている。
7. EU 市民の個人データの米国への移転に関しては、2000 年 7 月 26 日の欧州委員会のセーフハーバー決定により十分性認定が行われたが、2013 年 6 月のエドワード・スノーデンの NSA の秘密文書の暴露を契機に、EU-米国間で見

直し交渉が開始された。その交渉の最中の 2015 年 10 月 6 日に、EU 司法裁判所が同決定の無効判決を下した。

8. これにより見直し交渉が加速される状況になり、2016 年 7 月 12 日に欧州委員会はプライバシー・シールドの実施決定により十分性認定を行った。

この決定に対して、2020 年 7 月 16 日に EU 司法裁判所は、同決定の無効判決を下した。この 2 つの欧州員会の決定内容および EU 司法裁判所の判断について調査・分析を行った。

9. プライバシー・シールド無効判決を受けて、EU-米国間での見直し交渉を経て、決定された欧州委員会の現行のデータ・プライバシー・フレームワークの内容を、プライバシー・シールド実施決定との比較を含め調査・分析を行った。これらの EU 司法裁判所の判決は、バルク・データ収集を行う監視プログラムの実施に制約がなく、米国法における国の機関による個人データへのアクセス・利用に関する権限の制限、保護措置、監督・救済の仕組みの規定が不十分であるなどの理由に基づくものと考えられる。

10. EU 法では、人権制約を認める規定があるが、その人権制約に限界があることも規定されている。また IPA2016 も調査権限とプライバシー保護の両立を意図して、規定が置かれている。

11.調査権限の必要性と人権保障に関する基本的考え方は、2014 年の PPD28 号発出時のオバマ大統領のスピーチが参考になると考えられる。

12. 司法判断で言及されているように、調査権限の内容と権限に対する制約を規定するとともに、調査権限に関する保護措置、監督の仕組みおよび調査権限による不当な人権侵害に対する救済措置の仕組みに関して、明確かつ詳細なルールを定めることが求められていると考えられる。

この明確かつ詳細なルールを定めることで、調査権限を行使する機関にとっては、人権制約を超えた調査権限行使を避けることができる。また調査権限の対象となる側からは、調査権限が適正に行使されているかを判断しやすくなるとともに、濫用・誤用に対する救済が求めやすくなると考えられる。

13. 2011 年米国同時多発テロ発生を契機に、欧米各国で数多くのテロ対策法が成立したが、その過程で「自由と安全」について多くの議論が行われた。

この自由と安全の枠組みで、調査権限のあり方について考察を行った。

自由は民主主義社会の根幹的価値であり、人権制約する側が制約を必要とする脅威の存在を挙証する責任がある。安全は自由を制約すると高まるものではなく、調査権限の効果的・効率的な行使によって高まるものであると考えられる。調査権限の法目的に整合的な法制度には迅速性が、また人権制約については透明性が求められていると考えられる。

はじめに

本稿では、調査権限（ガバメント・アクセス）とそれによる人権制約の許容度を分析する観点から、第 1 に、英国の IPA2016 の成立までの経過を概観した後、IPA2016 の規定内容を調査・分析する。第 2 に、EU 司法裁判所、英国裁判所および欧州人権裁判所での 8 つの判決を取上げる。これらの判決ではいずれも違法または無効判決が下されているが、この判決理由を調査・分析する。第 3 に、判決に対する IPA2016 の改正に加えて、法目的に合致するように IPA2016 の規定を見直すとの視点から行われた、IPA(Amendment)Bill の議会提出までの経過、およびその内容について調査・分析する。第 4 に、EU 市民の個人データの米国への移転に関する EU-米国間の交渉経過と欧州委員会決定の内容、この決定に対する 2 度にわたる EU 司法裁判所の無効判決を分析する。この無効判決では、ガバメント・アクセス（英国でいう調査権限）が焦点である。また欧州委員会の現行のデータ・プライバシー・フレームワーク決定の構成と内容について、プライバシー・シールド決定との比較を含めて調査・分析する。第 5 に、EU 司法裁判所、英国の国内裁判所および欧州人権裁判所判決の主要論点を横断的に比較分析することで、調査権限の人権制約の許容度、正当で必要な調査権限、調査権限執行の適正執行のあり方を、バルク・データの必要性と人権への影響を含めて探る。

そして最後に自由と安全の視点から、調査権限に関する基本的問題について考察する。

以上が本稿の目的と構成である。

1. IPA (Investigatory Powers Act) 2016 成立までの経過

1.1 EU データ保存指令[2006/4/EC] (2006 年 3 月 15 日)

1.1.1 規定内容

EU データ保存指令（1.1 では以下指令）はデータ保存義務を電気通信事業者に課するものである。権限を付与された国の機関が、重大犯罪の捜査・探知・訴追および国家安全保障目的で、この保存データへアクセスし利用することが、この義務によって可能になっている。

また権限を有する国の機関に保存データへアクセスし利用することを認める条件として、指令は基本権憲章、人権条約、データ保護指令やプライバシー・電子通信指令における人権規定を遵守することを求めている。

従って指令は、調査権限と人権尊重の両面の規定を有している。また保存データの保護やセキュリティおよび人権を侵害された人に対する救済措置の規定もある。

なお、指令の国内法化の期限は 2007 年 9 月 15 日であり、インターネットアクセス、インターネット電話と e-mail に関しては 2009 年 3 月 15 日である。

1.1.2 データの保存義務に関する規定

EU データ保存指令は、重大犯罪（各加盟国の国内法によって定義される）の捜査、探知および訴訟に利用するために、電気通信事業者が自ら生成し、取扱うデータの保存義務に関して、加盟国の規定の調和を図ることを目的としている（1 条)。

3 条でデータ保存義務を規定し、4 条では保存データが権限ある国の機関に対してのみ提供される措置を、加盟国が講ずることが規定されている。すなわち、指令に基づき国内法によって電気通信事業者に保存義務を課す一方で、権限ある国の機関による保存データの利用および制限は国内法で規定するという枠組みとなっている。

データ保存義務の対象は通信内容ではなく、通信データであるが、保存対象は以下のように幅広い範囲に及んでいる（5 条)。

・通信元を特定するために必要なデータ：固定電話と移動体電話に関しては、発信者電話番号や加入者・登録利用者の名前と住所、インターネットに関しては、利用者 ID、電話番号、加入者・登録利用者の名前と住所
・通信先を特定するために必要なデータ：固定電話と移動体電話に関しては、電話番号、加入者・登録利用者の名前と住所

・通信の日時と長さを特定するにために必要なデータ：固定電話・移動体電話に関しては通話の始期と終期、インターネットに関してはログインとログオフの日時、IP アドレス、加入者・登録利用者の利用者 ID
・通信のタイプを特定するために必要なデータ：固定網電話と移動体電話に関しては利用した電話サービス、インターネット電話と e-mail に関しては利用したインテ―ネットサービス
・利用者の通信機器または利用者の機器であるとされる機器を特定するために必要なデータ：固定網電話に関しては発着信番号、移動体電話に関しては発着信番号等、インターネットに関してはダイアルアップのための発信電話番号、デジタル加入者線など
・移動通信機器の位置を特定するために必要なデータ：通信開始時の基地局 ID など
・通信内容は保存対象ではない。

データの保存期間は、6 カ月以上 2 年以内（6 条)。データ保護とセキュリティ（7 条)、加盟国がデータ保護とセキュリティに関してモニタリングする公的機関を指定すること（9 条)、および指令によるデータ処理に関する司法的救済（judicial remedies)、賠償責任（liability）や刑罰（penalties）などについても規定（13 条）がある。

1.1.3 私的生活・通信の尊重や個人データ保護に関する規定

指令 7 条、9 条、13 条の規定に加えて、プライバシー・電子通信指令 15 条(1)では、加盟国が（市民の）権利や義務を制限する場合の条件は、制限に当たっては公的秩序（国家安全保障、防衛、公共安全または犯罪の防止、捜査、探知、訴追および電子通信システムの無許可利用の防止）のために、必要で適切で比例的でなければならないというものである（前文 4)。

欧州人権条約[1]（以下人権条約）8 条では、すべての人の私的生活および通信の権利が規定されている。国家安全保障、公共安全、騒乱および犯罪防止などのために、法に従い必要な場合以外は、公的機関がこの権利に干渉

[1] 人権条約は、人権と民主主義の組織として 1949 年に設立された欧州評議会（Council of Europe）が、採択した条約（1950 年署名、1953 年発効）である。この人権条約の加盟国による遵守状況を監督(oversee)するために、欧州人権裁判所が設立されている。

現在の加盟国は全 EU 加盟国を含め 47 か国で、英国は当初からの加盟国である。

出典：欧州人権条約前文および “What is the Council of Europe” Briefing Paper, House of Commons, 27 July 2017

（interference）してはならないと規定している。

データ保存は法執行のために必要で有効な捜査手法であることが証明されているので、本指令が規定する条件に従って、一定期間保存データを法執行機関が利用できるようにすることが必要である（前文 9）。

また、利用・保存期間が終了後、保存データを削除や匿名化することも規定されている（7 条 d）。

データ保護指令[95/46/EC]、プライバシー・電子通信指令[2002/58/EC]が、指令に従って保存されたデータに全面的に適用される（前文 15）。

次に、指令の基本憲章、プライバシー・電子通信指令およびデータ保護指令に対する適合性について、EU 司法裁判所がどのような判断を下したのかを分析する。

1.2 EU 司法裁判所のデータ保存指令無効判決（2014 年 4 月 8 日）

（Case C-293/12、C-594/12）

1.2.1EU 司法裁判所の先決付託手続きと比例原則

（1）先決付託手続き

EU 機能条約 267 条において、EU 司法裁判所[2]は、条約の解釈と EU の機関等の行為の適合性[3]（validity）および解釈に関して、先決判決[4]（preliminary rulings）権限を有すると規定されている。

加盟国の国内裁判所が訴訟審理において、いったん審理を中断して、EU 法の解釈について、先決判決を求める付託手続きを取る。この付託に対して、EU 司法裁判所が EU 法の解釈について判決を下すと、国内裁判所は審理を再

---

[2] EU 司法裁判所の組織、手続き、判決などについては、以下の文献を参照。中西優美子[2022]『EU 司法裁判所概説』

[3] 本稿で分析する 8 つの判例において、基本権憲章などの規定に照らして指令、国内法および欧州委員会の実施決定に関して、validity、legality、lawfulness および compatibility との用語が用いられているが、本稿では適合性、また invalid、illegal および incompatible は不適合との訳語を用いる。

[4] 出典：庄司[2013]『新 EU 法基礎編』第 4 章第 3 節 pp141~149。文献によって、preliminary ruling は先決判決または先決裁定、また Treaty of the Functioning of the European Union は EU 機能条約または EU 運営条約と日本語訳が分かれている。本稿では、本文献の日本語訳に従う。

開して、その解釈を当該訴訟に適用するとの流れになっている。なお先決判決に関しては、第1審でかつ終審である。

EU 司法裁判所の EU 法の解釈は、抽象的に与えられるため、先決判決によって、EU 全域で EU 法の統一的解釈および適用ができる役割を果たしている。

なお先決付託手続きは、EU 司法裁判所の訴訟の約 75%（2020 年の新規案件 753 件のうち 556 件）を占めていて、数の上からも、また EU 法の統一的解釈および EU 法の発展（EU 法の直接効果、EU 法の国内法に対する優位、適合解釈の義務付け）からの観点からも重要な手続きである[5]。

（2）比例性原則[6]

比例性原則は EU 条約 5 条(4)に「比例性原則のもとでは、同盟（Union）の行為の内容と形式は、条約の目的を達成するために必要性を超えないものとする」と規定されているが、EU 司法裁判所の比例性の審査においては、当該行為が意図された目的を達成するために、適切であったか、必要であったか、および当該行動が意図された目的に比して過剰な負担を課したかどうかの 3 段階で審理が行われる。

この比例性原則は、EU による行動に対する制約として、作用する。

1.2.2 付託事項、関係法条文、争点および付託された質問

(1)先決判決付託事項(judgment)

本判決は基本権憲章 7 条、8 条および 11 条に対して、指令に規定するデータ保存の適合性判断の付託に対する先決判決である。

先決判決の要請は、指令実施のために制定された国内法の適合性に関して、Digital Rights Ireland（以下 Digital Rights）がアイルランドの裁判所に提起した訴訟（Case C-293/12）とオーストリアの憲法裁判所への憲法判断を求めた訴訟（Case C-594/12）に関してなされた。本判決はこの 2 件の訴訟に対する判決である。

(2)関係法条文(legal context)

データ保護指令、データ保存指令、プライバシー・電子通信指令

---

[5] 出典：中西、前掲注 2 p69

[6] 出典：庄司、前掲注 4 pp38~39

(3) 先決判決へ付託された質問

アイルランド裁判所とオーストリア憲法裁判所における審理と先決判決を求めて提出された両裁判所からの質問

・アイルランド裁判所への Digital Rights の訴訟提起は、2006 年 8 月 11 日行われた。訴えで原告が求めたのは、原告の権利を制限する規定、すなわち電子通信のデータ保存に関する国内法の適合性、および指令の無効（invalid）宣言を行うことである。

・オーストリア憲法裁判所の質問は、指令 3 条から 9 条の規定と、基本権憲章 7 条・8 条・11 条との適合性に関する質問である。

1.2.3 付託された質問についての審理（consideration)および判決

指令の規定内容に関して、基本権憲章および人権条約の規定内容と対比して審理を行っている。

(1)基本権憲章 7 条・8 条に規定されている権利への干渉についての審理

・指令 3 条（保存義務）・6 条（保存期間）の義務は、基本権憲章 7 条で規定されている権利への干渉である。

・指令 4 条（データへのアクセス）・8 条（保存データの保存要件）も基本権憲章 7 条への干渉である。

・同様に、指令は基本権憲章 8 条（個人データ保護）への干渉である。加入者・登録利用者へ告知することなく、データを保存し利用することは、私生活が常時監視されているとの感情を生み出し得る。

(2)基本権憲章 7 条・8 条の権利へ干渉することの正当性についての審理

・指令データ保存が基本権憲章 7 条の権利への重大な干渉であるとしても、指令では通信内容の取得を認めていないので、権利の本質には悪影響を与えるものではない。

・また指令 7 条では、データ保護とセキュリティ原則の尊重を規定しているので、基本権憲章 8 条へも本質的な悪影響を与えていない。

・国際テロとの戦い[7]が一般的利益（general interest）であることは EU 司法

---

[7] 2001 年 9 月 11 日の米国同時多発テロを契機として、英国を含む欧米各国でテロ対策法が数多く制定された。以下の文献を参照：「特集 テロと非常事態を考える」論究ジュリスト 2017 年春季号。英国については、江島晶子「イギリスにおけるテロ対策法制と人権―多層的人権保障システムへの新たな挑戦」。英国のテロ対策法制の特徴として、江島は「人権の大幅な制限が容易という側面と、いったん導入した制約をもとに戻すことが可能

裁判所の判例で明らかである。さらに、基本権憲章 6 条は自由の権利だけではなくセキュリティの権利も規定している。
・指令の目的は、重大犯罪との戦いに、究極的には公共安全に貢献することである。
・犯罪防止特に組織犯罪との戦いにおいて、電子通信利用に関するデータは特に重要なツールである。
・従って、権限ある国の機関に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ものである。

(3)干渉に関する比例性についての検証
・比例原則は、当該立法による正当な目的を達成するのに、EU の機関の行為が適切であり必要な限度を超えないことを求めている。
・指令が求めるデータ保存の必要性に関しては、指令で保存しなければならないデータは、刑事訴追の権限を有する国の機関の犯罪捜査にとって貴重なツールである。従ってそのようなデータの保存は、指令の目的達成にとって適切であると考えられる。
・指令が求めるデータ保存の必要性に関しては、重大犯罪との戦い特に組織犯罪やテロとの戦いは、公共安全にとって極めて重要であり、かつその戦いの有効性は現代の犯罪手法に大きく左右される。しかし、そのような一般的利益目的は如何に基本的であっても、それ自身データ保存を正当化するものではない。
・基本権憲章 8 条 1 項の個人データ保護は、基本権憲章 7 条の私的生活の権利にとって特に重要である。
・問題になっている EU 立法においては、範囲と適用について明確で詳細なルールを定めるべきである。個人データを効果的に保護するためには、濫用のリスクや保存データへの不当なアクセスと利用を防止する保護措置を設けなければならない。

という側面がある。後者において重要な働きをするのが、1998 年人権法とヨーロッパ人権条約によって構成される多層的人権保障システムである(p57)。」と述べている。また大沢秀介・新井誠・横大道聡編著[2017]『変容するテロリズムと法』「第 5 章」に、英国で 2001 年から 2015 年の間に制定された 7 本のテロ対策法名とその内容が記載されている（pp271-274)。もっとも英国では、2001 年以前にも北アイルランド紛争などへの対応として多くのテロ対策法が制定されている。

(4)上記の審査に基づく指令の適合性の判断

・干渉が厳密に必要な場合に限定されているかとの質問に関しては、指令３条（データ保存）と５条１項（データの種類）では、指令はすべてのトラフィックデータの保存を求めており、指令３条ではすべての加入者・登録利用者を対象としている。従って、実質的にヨーロッパの全人口の基本権に対する干渉となっている。

・この点に関して第１に、指令はすべてのトラフィックデータを区分せずに、全ての人の全ての電子通信を対象としていて、職業上守秘義務を負う人の通信についても例外規定がない。

第２に、権限ある国の機関のデータへのアクセスと、それに引き続く利用の制限に関する客観的基準がない。またデータへのアクセスについて、裁判所または独立行政機関による事前審査がなされていない。

第３に、データ保存期間に関して、役立つ可能性があるからという理由でデータの種類を区分せずに、最小６カ月となっている。さらに、保存期間が６カ月から２年間と定められているが、保存期間は客観的な基準に基づいて決定しなければならない。

・以上述べたことから考えて、指令は基本権憲章７条・８条の基本的権利への干渉の程度を規律する、明確で詳細なルールを定めていないために、指令はＥＵ法における基本権に対する広範で重大な干渉となっている。

・さらにセキュリティとデータ保護に関する規律に関しては、基本権憲章８条で求める濫用リスク等に対する、十分な保護措置を規定していない。指令はプライバシー・電子通信指令とデータ保護指令の規定に照らすと、事業者に高度なデータ保護とセキュリティを求めておらず、経済的な考慮をすることを認めている。また、データ保存期間終了時にデータの不可逆的な破壊を規定していない。

・第４に、指令はデータをEU域内に保存することを求めておらず、その結果基本的憲章８条３項によって明確に求められている保護とセキュリティに関する、独立したコンプライアンス機関によるコントロールが行えなくなっている。このようなコントロールは、個人データの取扱いに関する個人の保護に関する必須の構成要件である。

・以上の審理から、基本権憲章７条、８条および52条１項に照らすと、指令を採択することでEU法は、比例性原則を超えている。以上のことから、基本権憲章11条との適合性については検証する必要はない。

(5)判決

以上の理由から、指令は無効である。

1.2.4 本判決の論点

本稿では、国家安全保障や刑事司法の目的で、インテリジェンス機関や法執行機関が、情報通信ネットワークを流通またはその中に保存されている情報へアクセスし、利用する「調査権限（ガバメント・アクセス）[8]」の人権制約に対する許容度を探ることを目的として、英国の IPA2016 および EU 司法裁判所などの判決を手掛かりに考察することを目的としている。

データ保護指令無効判決では、以下の判断を行っている。

（1）指令が規定する通信データの保存は、基本権憲章 7 条・8 条に対する干渉であることを認めている。

（2）この干渉の正当性の有無については、指令の目的である国際テロや組織犯罪など重大犯罪との戦いは正当なものであり、この観点から電子通信利用に関するデータは特に重要であると述べている。

（3）指令の目的である重大犯罪と戦うために重要なデータ保存と、基本権憲章が保障している権利を制限する許容度を判断する基準が比例性原則である。1.2.3 で述べた理由から、データ保存指令は、基本権憲章で保障された権利の制限の限度を超えているので無効とされたと考えられる。

---

[8] 英国法である DRIPA2014、RIPA2000 および IPA2016 では、調査権限（investigatory powers）との用語が用いられている。一方「6」「7」の EU-米国間の個人データ移転に関しては、ガバメント・アクセス（government access）との用語が用いられている。

ガバメント・アクセスは、「法執行及び国家安全保障の目的を追求する場合に、民間部門が保有又は管理する個人データへ政府がアクセスし、これを処理すること」と定義されている。出典： “Declaration on Government Access to Personal Data held by Private Sector Entities” OECD 2022。なお、日本語訳は、個人情報保護委員会の仮訳による。

本稿では、英国法などの場合には調査権限、EU-米国間の個人データ移転に関する場合にはガバメント・アクセスの用語を用いる。

上記定義から分かることは、サイバー攻撃による軍事を含む先端技術情報の窃取、重要インフラへのサイバー攻撃および通信傍受などによる政治・経済・軍事情報の収集は、仮に国家による行為であったとしても、ガバメント・アクセスには該当しない。

ガバメント・アクセスの焦点ないし関心事は、個人データの保護にあると考えられる。

1.3 DRIPA2014（時限法）の成立

1.3.1 成立の経過

2013 年 6 月のエドワード・スノーデンが米国 NSA の大量の秘密文書を暴露したことを契機として、英国の複数の NPO が 2014 年 7 月 8 日に IPT[9]（Investigatory Powers Tribunal：調査権限行政審判所）に、プリズム計画やテンポラ計画などが欧州人権条約違反との訴えを起こした。

この訴えについては、2014 年 12 月 5 日と 2015 年 2 月 6 日に、IPT はプリズム計画やテンポラ計画は原則的に適法との裁決を行った。

1.3.2 DRIPA2014 の規定内容[10]

通信傍受や通信データの保存に関する調査権限は RIPA(Regulation of Investigatory Powers Act)2000　1 編に規定されていたが、この規定を修正したのが、DRIPA（Data Retention and Investigatory Powers Act）2014（本項では以下 DRIPA）である。

DRIPA は 1 条から 8 条まであって、1 条～2 条で通信データ、3 条～7 条で調査権限に関する規定が置かれている。1 条で通信データの規定の整備、2 条で 1 条の補足、3 条では RIPA5 条（令状を伴う傍受）の改正、4 条で RIPA1 編 1 章の域外適用の規定を改正、5 条で電気通信サービスの定義の改正、6 条で RIPA58 条（通信傍受コミッショナーによる報告）の改正、7 条で調査権限の運用と規制の審査を行うための、テロリズム法制の独立審査官制度を規定している。

なおデータ保存指令はデータ保存期間については、最長 2 年と定められていたが、DRIPA では 1 年となっている。

そして最後の 8 条では、DRIPA の 1 条～7 条は 2016 年 12 月 31 日に廃止となることが規定されている。

---

[9] IPT は RIPA2000 の 4 章 65 条～70 条の規定によって、RIPA2000 の調査権限行使に関する訴訟について審査するために設立された。また、IPA2016 の調査権限行使に関する IPT の権限については、同法 243 条において規定されている。「行政審判所」との訳語は、以下の文献による。横山潔「イギリス調査権限規制法の成立～情報機関による通信傍受・通信データの取扱い等の規制～」外国の立法 214（2002.11）

[10] 出典：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)

1.3.3 調査権限（Investigatory Powers）

本稿のテーマである調査権限とは何かについて、ここで述べておきたい。IPA2016 には「2」で述べるように、様々な調査権限が規定されている。これらの規定は、インテリジェンスの一つであるシギント（signals intelligence）と呼ばれる活動に関する規定である。

（1）インテリジェンスとは

学術的にも実務的にも普遍的な定義を述べることは困難であるとしつつも、小林良樹は「国家安全保障上の重要な問題に関する知識が、要求に基づいて収集・分析されて政策決定者（policy maker）に提供される仕組み（プロセス又はシステム）」及び「そうした仕組みによって生産された成果物（プロダクト）と定義している[11]。

ローエンタールによればインテリジェンスには、仕組み（プロセス）としての、成果物（プロダクト）としての、および組織としてのインテリジェンスの 3 つの意義があるとされる[12]。

もっともインテリジェンスとの用語は、IPA2016 にも数多く登場するが、定義は示されていない。

またインテリジェンス予算については、米国で 8 兆円（国防予算の約 10%）、英国で 4,200 億円（同 7%）であると推定されている。ちなみに日本では 1,500～2,000 億円（防衛費の 3~4%）と推定されている[13]。

（2）情報源の違いによるインテリジェンスの分類

小林は、インテリジェンスを以下の 5 つに分類している[14]。

・オシント（公開情報に基づく：OSINT：Open Source Intelligence）
・ヒューミント（人的情報に基づく：HUMINT：Human Intelligence）
・シギント（信号情報に基づく：SIGINT：Signals Intelligence）
・ジオイント（地球空間情報に基づく：GEOINT：Geospatial Intelligence）

茂田忠良は、米国の対外諜報の枠組みとして、ヒューミント、シギント、イミントおよびマシント（MASINT：Measurement and Signature Intelligence：計測・特徴諜報：ミサイル発射など、相手方の発する電磁波、

---

[11] 出典：小林良樹[2021]『なぜ、インテリジェンスは必要か』p16

[12] 出典：マーク・M・ローエンタール[2011]『インテリジェンス』p11

[13] 出典：小谷賢[2022]『日本インテリジェンス史』p5

[14] 出典：小林良樹[2014]『インテリジェンスの基礎理論［第二版］』p83

光などを把握）の 4 つを挙げている[15]。

（3）シギントとは

シギントは上記によれば、信号情報に基づくインテリジェンスである。これは、「通信の傍受に基づくインテリジェンス」であるコミント（COMINT：Communications Intelligence）と、通信ではない信号の収集に基づくエリント（ELINT：Electronics Intelligence）に分かれる[16]。

茂田はこの二つに、フィシント（FISINT：Foreign Instrument Signals Intelligence：外国計装信号諜報：テレメトリー（遠隔監視）信号が典型的）を加えている[17]。

IPA2016 のシギントは、このうちコミントに属する。ただ IPA2016 では通信の傍受だけではなく、コンピュータやサーバーに保存されている情報の収集も行っているので、IPA2016 に限っていえば、この定義におけるシギントだけに留まらないといえる。

またインテリジェンスは上記の定義から、国家安全保障目的となっているが、IPA2016 では調査権限行使は、インテリジェンス機関だけではなく、法執行機関によっても担われている。

「2」で述べるようにバルク令状はインテリジェンス機関だけの権限であり、法執行機関の権限は特定令状や通信データ許可に限定されている。

しかし 2.8 で述べるように、特定機器干渉令状の取得件数はインテリジェンス機関とほぼ同数であり、通信データ許可は法執行機関による取得が極めて多くなっている。

このシギントについては、米国、英国、カナダ、オーストラリアおよびニュージーランドの 5 か国からなるファイブアイズ[18]が著名である。このファイブアイズ活動の根拠は、UKUSA 協定である。

---

[15] 出典：茂田忠良、江崎道朗[2024]『シギント 最強のインテリジェンス』pp50-51、61-62

[16] 出典：小林 前掲注 11　p183~184

[17] 出典：茂田、前掲注 15　p87

[18] 出典：小谷賢[2015]『インテリジェンスの世界史』p59。またファイブアイズの活動については、以下の文献も参照。茂田忠良「サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～」情報セキュリティ総合科学 第 11 号 2019 年 11 月

1.4　IPA2016 の成立（2016 年 11 月 29 日）

DRIPA2014 は 2016 年 12 月 31 日に廃止となる時限法であるため、これに代わる新たな法律が必要となる。この新しい法律が IPA2016 であるが、成立までの経過は以下の通りである。

(1) 2015 年に政府から独立した 3 つの報告書[19]が公表され、法案の基礎となっている。

(2) 2015 年 11 月に政府は調査権限草案（Draft Bill）を議会に提出、この草案について 3 委員会合同の事前審査[20]（Pre-Legislative Scrutiny）が行われた。
草案の審議結果の報告書は、2016 年 3 月に公表されている。

(3)この事前審査における意見等を踏まえて、政府は 2016 年 3 月に調査権限法案(Investigatory Powers Bill)を、付属文書[21]と併せて議会に提出した。
また法案審議中の 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[22]が公表された。

(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、調査権限法案は下院において賛成 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 ピンポン（ping pong[23]）を経

---

[19] “Privacy and Trust” ：議会インテリジェンス・保安委員会報告書、 “A Question of Trust” ：David Anderson による報告書、“A Democratic License to Operate”： Royal United Services Institute(RUSI)による報告書

[20] 政府提出法案が正式に議会の提出される前に、議会の委員会が審査を行うことを事前審査という。法律の質を高めるために行われるもので、どの法案を対象にするかは政府が決定する。2017 年議会期では、政府提出法案総数は 60 件であるが、事前審査されたのはそのうち 7 件である。出典：小熊美幸「イギリス議会の立法前審査」国立国会図書館 調査と情報 第 1106 号（2020.7.16）

[21] 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”

[22] “Report of the Bulk Powers Review” David Anderson, August 2016

[23] ping pong：両院の意見が対立した場合、わが国の両院議員協議会に相当する仕組みは特に設けられていない。同一会期中両院の意見が一致するまで両院間を往復する可能

て、11 月 16 日に可決された。
　ついで、11 月 29 日に女王の裁可（royal assent）を得て成立した。施行日は、国務大臣が規則（regulation）によって定める日になる。

(5) IPA2016 の成立によって、DRIPA2014 および RIPA2000 1 編（1 章・2 章）は廃止された。なお、RIPA2000 の 2 編（監視及び内密の人的情報源）、3 編（暗号化等によって保護される電子データの調査）など他編の規定は依然として効力を有している。

2. IPA2016[24]

2.1 条文構成と調査権限の種類

　本法は 272 条（1 編から 9 編）及び 10 の細則から構成されている。調査権限は 2 編から 7 編とおよび 9 編に規定されている。
　調査権限には、令状、許可、通知の 3 種類がある。令状(warrant)としては、特定対象の通信傍受令状（2 編）、特定対象の機器干渉令状（5 編）、バルク令状（通信傍受、通信データ取得、機器干渉）（6 編）、バルク・パーソナル・データセット令状（7 編）、許可(authorisation)としては、特定対象の通信データ取得許可（3 編）、通知(notice)としては、通信データの保存通知（4 編）、National security notices および Technical capability notices（9 編）がある。

＊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)等

性がある。この往復をピンポンという。下院が上院の修正を受入れ内ない場合、上院は下院の意見を尊重するのが通例とされる。出典：濱野雄太「イギリスの議会制度」国立国会図書館 調査と情報第 1056 号 (2019.5.28)

[24] 英国の正式名称は、the United Kingdom of Great Britain and Northern Ireland である。2021 年の国勢調査では人口は全体で 6700 万人であるが、そのうちイングランドが 84.3%、スコットランドが 8.2%、 ウエールズが 4.6%、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する規定があるが、本稿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：Census2021、Office for National Statistics

＊2 編：合法的（特定）通信傍受

通信傍受は通信内容を取得する行為である。

＊3 編：通信データ取得許可

＊4 編：通信データの保存（通知）

＊5 編：（特定）機器干渉（Equipment Interference）

5 編の機器干渉は、特定のコンピュータなどの機器に保存されている、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。

＊6 編：バルク令状（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）

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、通信データの取得を認める規定である。

但し IPA 2016 には、バルク・データの定義はない。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.)］であると述べられている。

＊7 編：バルク・パーソナル・データセット令状

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調査権限であり、インテリジェンス機関が求めている情報は、収録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。

＊8 編：監督の仕組み（Oversight Arrangements）

これまでの法律でも、インテリジェンス機関や法執行機関の権限行使の監督に関して、6 つのコミッショナー職が置かれていた。IPA 2016 においては、分散して規定されていたこれらのコミッショナー職を廃止して、調査権限コミッショナー（Investigatory Powers Commissioner）に一元化した（240 条）。

但し、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）。なお、法案とともに提出された付属文書の一つである“Operational Case for Bulk Powers”には、統合前の調査権限の根拠法が掲載されている。

＊9 編：雑則および一般的規定

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 を発出できる規定や用語の定義などの規定などがある。

＊細則：細則 1～10

2.2 議会における審議状況と法案修正

(1) 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[25]。

・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。
・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。
・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。

(2) 法案審議[26]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（令状等発出権者の国務大臣と、司法コミッショナーによる 2 重チェック） 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。

(3) 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
・報道資料に関する通信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

---

[25] 出典：“A Response to Pre-legislative Scrutiny” 法案提出時に併せて提出された文書

[26] 英国議会の審議プロセス：下院の場合：第 1 読会（本会議で法案の題名の朗読）、第 2 読会（本会議で基本方針の審議、通常 1 日約 5 時間）、委員会段階（法案毎に設置、委員数は 16～50 人、逐条審議）、報告段階（本会議で修正案が提出された条文についてのみ討論・評決）、第 3 読会（通常、報告段階直後に、本会議で法案への賛否についてのみ討論・評決） 出典：濱野、前掲注 23 p15

2.3 IPA2016 によって強化された調査権限と調査権限行使に対する制限

(1) 強化された調査権限

インターネット接続記録（ICRs：Internet Connection Records）の取得・保存が可能になった。この規定の新設によって、政府は人々の通信の方法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。またバルク機器干渉が可能になった。

(2) 調査権限の行使に対して強化された制限

まずプライバシー保護の規定が強化された。1 編では、プライバシーに関する一般的保護義務（2 条）が規定されて、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ける要配慮事項となった。

一方で、調査権限の必要性の根拠なども規定されていて、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となっている。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) 令状・許可・通知における保護措置

プライバシー保護強化の観点から、調査権限の行使に際して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。

1)特定の人・情報に関する保護措置の例

- 議会の議員（2 編、5 編）
- 法的特権に関する規定（2 編、5 編、6 編 1~3 章、7 編）
- ジャーナリストの保護に関する規定（2 編、5 編、6 編 1 章・3 章）
- 海外への情報の開示（2 編、5 編、6 編 1 章、3 章）
- 医療・健康記録（7 編）
- 保護されたデータ（7 編）

2)令状等の執行に関する制限規定の例

- 情報(material)の保存と開示（2 編、5 編、6 編 1~3 章）
- 無権限開示の罪（2 編、5 編、6 編 2 章）
- 検証(examination)に関する保護措置侵害の罪（6 編 1~3 章、7 編）
- フィルタリングの関する規定（3 編）
- 通信傍受で得られた情報の訴訟手続きからの除外（2 編、6 編 1 章）

(4) 監督体制の強化

新たに調査権限コミッショナー職および司法コミッショナー職が創設され、令状等の発出時の司法コミッショナーによる事前審査など、調査権限行使に関

する監督体制が強化された。

1)両コミッショナーの選任方法と地位保障

・高位の司法上の地位（high judicial office[27]）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。
・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。但し、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、全体的な監督の役割を担い、司法コミッショナーは、令状発出の承認の判断を行う。
・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。
また、調査権限コミッショナーの多くの監督事項は、229 条に詳細に規定されている。同条(1)では、監査(audit)、監察(inspection)、捜査(investigation)を含む審査(review)を行うと規定されている。
・また、調査権限コミッショナーは、同条(3)(e)で RIPA2000 の 2 編と 3 編の調査権限を監督することが規定されている。
・調査権限コミッショナーは、年次報告書を作成することとされている(234 条)。
・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・保安委員会の求めに応じて、インテリジェンス活動について指示することができる。（230 条(3)）

　またこの指示は公益などに反すると判断される場合を除き、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を、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に関しては、委任することができない。

---

[27] high judiciary office の意味は、憲法改革法 2005 の 3 編と同じ。

2.4 バルク令状

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、（通信データ）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。

性格の異なる BPD 令状を除く、通信傍受、取得、機器干渉の 3 つを比較すると、3 令状に共通する事項と違いがある事項がある。

(1) バルク 3 令状に共通する事項

バルク令状の申請権者は、インテリジェンス機関の長とその代理人であり、法執行機関の長には認められていない。申請できるインテリジェンス機関は、保安部(MI5: Security Service)、秘密情報部(MI6:Secret Intelligence Service)および GCHQ(General Communications Headquarters) の 3 機関[28]に限定されていて、国防 Intelligence には申請権限は認められていない。

発出根拠・理由は、① 国家安全保障、② 重大犯罪の防止・探知、③ ①に係る経済的利益があること、の 3 つである。

検証令状の場合には、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)」を要すると規定されている。

(2) バルク 3 令状で違いのある事項

1）通信傍受および機器干渉に関しては、調査権限対象が海外関連であるのに対して、取得に関してはその規定はない。

2）発出権者は、通信傍受と取得は国務大臣自身で代理人の規定がないのに対して、機器干渉に関しては例外的に代理人による発出も認められている。

3）通信傍受と取得の場合は常に司法コミッショナーの事前承認を要するのに対して、機器干渉の場合は緊急時には事前承認が不要となっている。

(3) バルク令状に関する議会における議論

バルク調査権限は、調査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、法案審議でもっとも議論が行われた分野の一つである。

インテリジェンス・保安委員会委員長は、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調査権限は必要である、また膨大なバ

---

[28] MI5 は Security Service Act 1989 によって、また MI6 と GCHQ は Intelligence Services Act 1994 によって、その設立根拠が与えられたインテリジェンス機関である。

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。

2.5 特定令状・特定通信データ取得許可とバルク令状の比較

本項では、特定対象令状・許可とバルク令状の規定の比較を行う。また、比較対象がない BPD 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。なお比較表は、後述する IPA2016 を改正した 2018 年規則後の内容で比較しているが、2023 年に議会に提出された IPA2016(Amendment)Bill の内容は入っていない。

以下の比較表を見ると、特定令状・許可とバルク令状では、バルク令状の方が令状申請権者、令状発出者、発出根拠・理由、承認権者などの手続き要件が厳しくなっている。これはバルク令状が、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いえる。

なお、多くの令状や許可の発出が規定されているが、248 条の規定により、国務大臣は令状等を発出する際に、令状および許可を組合せて（combination of warrants and authorisations）一つの文書で行うことができる。この組合せについては細則 8 に 9 ページにわたる詳細な規定が置かれている。

(1) 特定通信傍受令状（2 編）とバルク通信傍受令状（6 編 1 章）の比較

	特定通信傍受令状	バルク通信傍受令状
令状の種類	通信傍受、相互支援、検証（バルク令状で取得されたデータが対象）：15 条	通信傍受：136 条
調査権限	通信傍受、伝送中とシステムに蓄積されている 2 次データの取得、開示：15 条、16 条(3)、郵便事業者・サービスにも適用：45 条、47 条	海外関連（受発信者の一方が海外）の通信傍受、2 次データの取得、検証のための選択（語）、開示：136 条、137 条
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の長およびその代理人：18 条	インテリジェンス機関（MI5、MI6、GCHQ）の長とその代理人：138 条
発出権者	国務大臣：19 条、Scottish Ministers：21 条、例外的にその代理人：30 条(4)	国務大臣：138 条 代理人の規定はない：141 条
発出根拠	国家安全保障、これに係る経	左欄に加えて、検証には特

・理由	済的利益および重大犯罪の防止・探知：20 条(2)	定の運用目的があること：138 条
承認権者（更新・修正・取消の場合も同じ）	緊急時を除き、司法コミッショナーの事前承認：23 条、24 条	司法コミッショナーの事前承認：140 条 緊急時の規定はない
有効期限	6 か月：32 条、更新時 30 日：33 条(5)	6 か月：143 条(1)、更新時 30 日：144 条(3)

注：2 次データ：① identifying data：人物、装置、システムまたはサービスおよびイベントまたは人・イベントの位置を識別するデータ、② systems data：郵便、電気通信システム・サービスの機能を可能に、容易に、識別または記述するデータ：263 条（9 編）

(2) 通信データ取得許可（3 編）とバルク取得令状（6 編 2 章）の比較

	通信データ取得許可	バルク取得令状
種別	許可：60A 条、61 条、61A 条：但し、62 条、76 条などによる制約あり	令状：158 条
調査権限	通信データ取得および通信データの取得・開示 ：60A 条、61 条、61A 条 郵便事業者・サービスにも適用：84 条	電気通信事業者が保存しているまたはこれから取得できる通信データの取得、開示、取得したデータの検証 ：158 条
申請権者	細則 4 にある機関：60A 条、70 条、地方自治体：60A 条	インテリジェンス機関の長とその代理人：158 条
発出権者	調査権限コミッショナー：60A 条、申請機関の指定上級者：61 条、61A 条	国務大臣：158 条 代理人の規定はない ：160 条
発出根拠・理由	調査権限コミッショナーの場合：国家安全保障、これに係る経済的利益、犯罪目的など 7 事由、指定機関の上級者：国家安全保障など 3 事由：61 条、緊急時：犯罪目的、公共安全など 5 事由：61A 条、地方自治体：犯罪目的のみ：73 条	国家安全保障、これに係る経済的利益、重大犯罪の防止・探知に加えて、検証には特定の運用目的があること：158 条

承認権者	報道の情報源を対象とする場合には、司法コミッショナーの事前承認：77 条	司法コミッショナーの事前承認：159 条 緊急時の規定はない
有効期間	1 か月、更新時 1 か月：65 条	6 か月、162 条、更新時 30 日：163 条

注：細則 4 にある機関の場合には、承認権者は申請権者と同じ機関に所属しているので、いわば内部許可で良いことになっている。

(3) 特定機器干渉令状（5 編）とバルク機器干渉令状（6 編 3 章）の比較

	特定機器干渉令状	バルク機器干渉
令状の種類	機器干渉、検証：99 条	機器干渉：176 条
調査権限	機器に蓄積された通信および機器データの取得・開示、バルク機器干渉令状で取得したデータの検証：99 条	海外関連の機器に蓄積された通信、機器データおよび他の情報の取得、検証のための選択（語）、開示：176 条
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および細則 6 の 1~2 編の表にある法執行機関の長とその代理人 ：102~106 条	インテリジェンス機関の長とその代理人：178 条
発出権者	国務大臣・Scottish Ministers（例外的に代理人）、上記法執行機関（機器干渉令状のみ）の長と（例外的に）その代理人 ：102~106 条	国務大臣：178 条 例外的にその代理人 ：182 条
発出根拠・理由	国家安全保障、これに係る経済的利益および重大犯罪の防止・探知：102 条~106 条	左欄に加えて、検証には特定の運用目的があること：178 条
承認権者（更新・修正・取消の場合も同じ）	司法コミッショナーの事前承認：108 条、緊急時は事前承認なし：109 条	司法コミッショナーの事前承認：179 条、緊急時は事前承認なし：180 条
有効期間	6 か月：116 条、更新時 30 日 ：117 条	6 か月：184 条、更新時 30 日：185 条

(4) BPD 令状（7 編）

令状の種類	クラス BPD（bulk personal dataset）令状、 特定 BPD 令状：200 条(3)
調査権限	BPD の保存と検証：199 条、200 条（クラス BPD の利用には制限あり：202 条）
申請権者	インテリジェンス機関の長とその代理人 ：204 条、205 条
発出権者	国務大臣：204 条、205 条
発出根拠・理由	検証の場合に特定の運用目的必要：204 条、205 条、212 条
承認権者（更新・修正・取消の場合も同じ）	・特定 BPD 令状：司法コミッショナーの事前承認：208 条、国務大臣が緊急と判断する場合：事前承認なし：205 条（6）、209 条 ・クラス BPD 令状：司法コミッショナーの事前承認：208 条
有効期間	6 か月：213 条、更新時 30 日：214 条

2.6 通知制度

調査権限には、2-1 で述べたように上記の令状と許可の他、以下の 3 つの通知制度がある。

(1) 保存通知（4 編）

調査権限	事業者に通信データの保存を求めることができる。 ：87 条、通信データ：通信の受発信者、通信の日時と長さ、通信のタイプ・方法・パターン、電気通信システム、そのシステムの所在地：87 条(11) 郵便事業者にも適用：96 条
発出権限	国務大臣：87 条
発出根拠・理由	国家安全保障、それに係る経済的利益、犯罪目的、公共の安全など 6 事由：87 条
承認権者	司法コミッショナー：89 条
有効期間	個々の通知で指定。但し、最長 12 か月：87 条

注 1：通信データを保存している電気通信事業者の義務としては、データのセキュリティとデータの保護を確保すること、特に権限のある人だけがデータにアクセスできるように

技術的・組織的な保護手段を講ずること、事故や不法な棄損、事故による滅失、無権限・不法な保存・処理・アクセス・開示からデータを保護することが規定されている（92 条、93 条）。

注 2：4 編のデータの完全性、セキュリティまたは破壊（destruction）に関する要求事項や制約については、Information Commissioner に監督権限がある（244 条）。なお、Information Commissioner は、UK-GDPR やデータ保護法 2018 を所管している。

(2) National security notice (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 を交付する。

通知を受取った電気通信事業者の義務は、①IPA2016 以外の法律[29]の下での、インテリジェンス機関の活動の支援を行うこと、②非常事態（Civil Contingencies Act 2004 の 1 編[30]の意味と同じ）に対処すること、③インテリジェンス機関が、より安全にまたはより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行うことである。

(3) Technical capability notice （253 条）

National security notice が、 IPA 2016 以外の法律の下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、その行為による達成される目的と事業者に求める行為が比例的である場合で、支援の提供能力の確保が必要であり、かつ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。

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

---

[29] Intelligence Service Act1994、RIPA2000、RIP(Scotland)A2000

[30] Civil Contingencies Act 20041 の 1 編 1 条において非常事態（emergencies）として以下の 3 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

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、電気通信事業者に加えて、郵便事業者またはこの 2 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議しなければならない。

(4) 両方の notice に共通する事項

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。

2.7 電気通信事業者および郵便事業者の協力・守秘義務

通知における電気通信事業者および郵便事業者等の義務については、2.6 に述べた通りであるが、令状および許可においても協力義務が規定されている。

電気通信事業者と郵便事業者の両方が協力義務を負うのが、2 編特定通信傍受令状、3 編通信データ取得許可である。一方、電気通信事業者だけが協力義務を負うのが 2 編特定機器干渉令状、6 編 1 章バルク通信傍受令状、6 編 2 章バルク取得令状および 5 編特定機器干渉、6 編 3 章バルク機器干渉令状である。

また、義務には協力義務と守秘義務があり、事業者のこれらの義務違反行為に対しては、刑事罰と民事訴訟の二つの対抗手段がある。

一方で事業者が協力するための費用については、国務大臣が適切と考える額の費用を負担することが規定されている（249 条)。

2.8 令状・許可件数[31]

既に述べたように調査権限には、いくつもの種類があるが、調査権限コミッショナーが 234 条の規定によって作成する年次報告書の中に、実際に発出され

---

[31] 出典：Annual Report of the Investigatory Powers Commissioner 2021(2023 年 3 月公表)　この報告書では、調査権限コミッショナーが IPA2016 の監督権限だけではなく、229 条(3)(e)によって RIPA2000 の監督権限を有していることから、IPA2016 の規定以外に関する事項についても記述されている。

た令状および許可件数の一部が報告されている。

(1) 特定令状・通信データ取得許可件数　：単位件数

	2021 年	2020 年	2019 年
通信傍受（2 編） (UKIC+LEAs)	3,630 (このうち検証令状 36)	3,648	3,329
機器干渉（5 編） ・UKIC ・LEAs	 2,030 1,915 （このうち検証令状 36）	 1,139 1,039	 1,071 848
通信データ（3 編） ・UKIC ・LEAs ・WPAs ・Local ・Prison	 10,536 (3.7%) 273,193 (95.9%) 749 237 217	 11,444 (4.5%) 239,086 (94.9%) 969 212 155	

・UKIC：the United Kingdom Intelligence Community
・LEAs：Law Enforcement Agencies
・WPAs：Wider Public Authorities
・49 条~51 条において、刑務所、精神病院および入国拘留施設において、通信傍受が認められている。

(2) バルク令状件数

	2021 年	2020 年	2019 年
通信傍受（6 編 1 章）	33	31	30
通信データ（6 編 2 章）	14	14	18
機器干渉（6 編 3 章）	13	12	10
BPD（7 編） ・クラス ・特定	 111 66	 108 76	 101 85

この統計から読取れる特徴点は以下の通り。

1) 特定令状がバルク令状より極めて発出件数が多い。令状件数と許可件数を比較すると、許可件数が圧倒的に多い。これらの特徴は、それぞれの令状なり許可手続きの違いを反映したものと考えられる。
2) 特定通信傍受に関してはインテリジェンス機関と法執行機関を併せた件数であるが、特定機器干渉ではインテリジェンス機関と法執行機関の件数がほぼ同数になっている。
3) 通信データはほぼ法執行機関による取得である。なお、IPA2016 の 2018 年改正によって、60A 条で発出権限者に調査権限コミッショナーが追加されたが、この統計では調査権限コミッショナーと申請機関の指定上級者のそれぞれの発出件数の内訳は記載されていない。
4) 時系列では、それほどの変化はないが、機器干渉だけは 2 年間で倍になっている。
5) 司法コミッショナーの拒否件数については、特定通信傍受 4 件、特定機器干渉 8 件であるが、バルク令状では拒否した例はない。
6) 緊急令状は特定機器干渉で、282 件と全体の 7%程度となっている。

3. IPA2016 成立後の経過と IPA2016 の改正

3.1 EU 司法裁判所の DRIPA2014 違法判決(2016 年 12 月 21 日)

(Case C-203/15、C-698/15)

IPA2016 成立した 2016 年 11 月 29 日の約 1 か月後の 12 月 21 日に、EU 司法裁判所は DRIPA2014 の違法判決を下した。

3.1.1 付託事項、関係法条文、争点および付託された質問

(1) 先決判決付託事項(judgment)

先決判決の求めは、基本権憲章 7 条、8 条および 52 条(1)に照らした、2009 年 11 月 25 日の指令 2009/136/EC によって改正された 2002 年 7 月 12 日のプライバシー・電子通信指令（2002/58/EC）15 条(1)の規定の解釈である。

付託要請は、以下の 2 つの審理においてなされたものである。

（ア）スウェーデンの Tele2 Sverige AB（電気通信事業者）とスウェーデン郵便・電気通信機構(PTS)間での、後者から前者に送付された、前者の加入者・登録利用者のトラフィックおよび位置データの保存命令に関

する訴訟である。(Case C-203/15)

(イ) Tom Watson 氏らと英国内務省間での、DRIPA2014 の 1 条の EU 法との適合性に関する訴訟である。(Case C-698/15)

審理は、この 2 つの訴訟を併合して行われた。

(2) 関係法条文（legal context）

・EU 法：改正プライバシー・電子通信指令（Directive 2002/58）、データ保護指令(Directive 95/46)、データ保存指令（Directive 2006/24/EC）
・スウェーデン法：電子通信データの保存および国の機関による当該データへのアクセスに関する法律
・英国法：DRIPA2014（(2)(3)では以下 DRIPA）[32]、RIPA、データ保存指令規則 2014、通信データ取得・開示に係る Code of Practice

(3) 先決判決付託に至る争点

ここでは、英国の争点について述べる。（Case C-698/15）

Watson 氏らは、DRIPA1 条（通信データの保存）が基本権憲章 7 条・8 条および人権条約 8 条違反であると主張して、DRIPA1 条の適合性（legality）審査の訴えを High Court of Justice [33](高等法院)へ提起した。

2015 年 7 月 17 日[34]に High Court は、EU 司法裁判所の Digital Rights 判決（データ保存指令無効判決）において、データ保存指令が比例性原則に反しているので、その指令と同じ規定を含んでいる国内法は、同様にその原則に反していると判決した。

Digital Rights 判決の基礎にある論理では、通信データ保存に関する権利について十分な保護措置規定がない国内法は、基本権憲章 7 条・8 条で保障されている権利の侵害になる。従ってデータへのアクセスに対して明確かつ詳細な規定がない限り、また当該データへのアクセスに対する、裁判所または独立行政組織

---

[32] DRIPA の成立経過については、「1.3」参照。

[33] 地方裁判所の 1 つである High Court of Justice は、民事の第一審裁判所で、この判決は契約違反や一般不法行為事件等の一般民事裁判を管轄する Queen' s Bench Division で行われた。裁判所組織の出典：馬場真由美「英国司法制度の現状」神奈川ロージャーナル 4 号、神奈川大学、2011 年

[34] DRIPA の成立が 2014 年 7 月 17 日なので、本判決はちょうど 1 年後になる。また議会の事前審査を受けるための調査権限法草案が、議会に提出されたのが 2015 年 11 月なので、DRIPA に代わる草案の審議が始まる前に、本判決が下されたことになる。

による事前承認がない限り、DRIPA1 条は基本権憲章 7 条・8 条に適合的ではない。

国務大臣は、この判決を不服として控訴した。控訴審は、EU 司法裁判所はデータ保存指令判決の適合性についてはしたものの、保存されているデータへの国の機関によるアクセスの適合性を判断していないとして、審理を中断して先決判決を求めて EU 司法裁判所に付託した。

(4) 先決判決に付託された質問

1) スウェーデンの質問（Case C-203/15）

① すべての人とすべての電子通信のトラフィックデータ、および犯罪と戦う目的のためにいかなる区分、制限または例外も設けないトラフィックデータの全体的な保存義務は、基本権憲章 7 条・8 条・52 条(1)の規定に照らして、プライバシー・電子通信指令 15 条(1)と適合的か？

② もし質問 1 への回答がネガティブであるとすれば、データ保存は以下の場合に認められるか？

ア. 保存データへの国の機関のアクセスが命令の 19～36 項によって決定される場合

イ. データ保護とセキュリティ要件が命令の 38～43 項によって規制されている場合

ウ. すべてのデータが、通信が終了してから起算して 6 か月保存する義務、および命令の 37 項での消去義務が規定されている場合

2) 英国の質問（Case C-698/15）

① Digital Rights 判決は、基本権憲章 7 条・8 条を遵守するために、保存データへのアクセスを規律する加盟国の国内法に適用される EU 法の拘束力のある要求条件を定めているか？

② Digital Rights 判決では、EU 基本憲章 7 条・8 条の適用範囲を、人権条約 8 条を超えて拡大しているか？

3.1.2 審理および判決

(1)付託された質問についての審理

質問の審理については英国からの質問について述べる。

1) 英国の第 1 質問およびスウェーデンの第 2 質問

この付託された質問は、基本権憲章 7 条・8 条・52 条(1)に照らして、プライバシー・電子通信指令 15 条(1)は、国の機関の保存データへのアクセスを規定す

る以下の国内法は、排除していると解釈しなければならないか？

① 国内法が権限ある国の機関のアクセスを重大犯罪と戦うためだけに限定していない場合

② アクセスが裁判所または独立行政機関による事前承認を得ていない場合

③ 保存されるデータが EU 域内で保存されるべきとの規定がない場合

2)審理

電子通信の秘匿性原則を緩和する国内法を正当化できる目的に関して、プライバシー・電子通信指令 15 条(1)の第 1 文において規定されている目的は網羅的であること、保存データへのアクセスはそれらの目的の 1 つに真にかつ厳密に対応していなければならないことに留意しなければならない。

さらに法目的はアクセスに伴う基本権への干渉の重大性に対して、比例的でなければならない。このため犯罪防止・捜査・探知・訴追の領域では、重大犯罪と戦う目的だけが、保存データに対するアクセスを正当化することができる。

比例性原則に沿うことに関しては、国内法はアクセスが厳密に必要な限度を超えないようにしなければならない。

プライバシー・電子通信指令 15 条(1) でいう国内法は、適切な保護措置が必要なので、権限を有する国の機関が、データ保存に関してどのような状況と条件があれば、電子通信事業者はデータにアクセスを認めなければならないかについて、明確かつ詳細な規律を定めなければならない。同様にこの種の措置は、国内法のもとで法的な拘束力を持たなければならない。

当該国内法には権限ある国の機関が、アクセスを認められる客観的な基準を設定しなければならない。全ての保存データへの一般的なアクセスは、厳密に必要なものに限定しているとは見做せない。一般的なルールとしては、犯罪と戦う目的に関しては、重大犯罪を計画、関与または関与したと疑われる個人のデータにのみアクセスができる。

しかし例えば重大な国家安全保障、防衛または公共安全が、テロリストの行動によって脅かされている場合のように特別の状況があり、その行動と戦うのに役立つとの客観的な証拠があれば、他の人のデータへのアクセスも認められる。

これらの条件が尊重されるようにするために、権限ある国の機関の保存データへのアクセスは、緊急時を除き、裁判所または独立行政機関の事前承認を得るべきである。

また、権限ある国の機関は保存データへのアクセスの対象となる人に対して、通知が捜査を阻害しなくなったら、すみやかに本人に通知しなければならない。その通知は、その本人が自分の権利が侵害された場合に、法的救済の権利を実行できるようにするために必要である。

データのセキュリティと保護に関するルールに関しては、保存データの誤用

のリスクやデータに対する不法なアクセスから効果的に保護するために、事業者に対して適切な技術的・組織的な措置を求めている。

特に機微データについては、特別に高いレベルの保護措置を保障しなければならない。また国内法はデータを EU 域内に保存すること、およびデータの保存期間終了時に不可逆的なデータの破壊することを規定しなければならない。

上記のすべてを考慮すると、英国の第 1 質問とスウェーデンの第 2 質問への回答は、基本権憲章 7 条・8 条・11 条および 52 条(1)に照らすと、プライバシー・電子指令 15 条(1)は、トラフックおよび位置データの保護およびセキュリティ、特に権限ある国の機関が保存データへアクセスを規律する国内法は、以下のような場合を排除していると解さなければならない。

① アクセスの目的が、犯罪と戦う場合に、重大犯罪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の事前承認を得ていない場合
③データが EU 域内に保存すべき要件を課していない場合

3）Case C-698/15（英国）の第 2 質問

第 2 質問は、Digital Rights 判決において、EU 司法裁判所が基本権憲章 7 条・8 条の規定を、人権条約 8 条の規定する範囲を拡大するように解釈したかの確認を求めるものである。

EU 法 6 条(3)の規定によって、人権条約による基本権は EU 法の一般原則を構成すると認めたものの、人権条約は EU 法に組入れられた法的な規定ではない。

従ってプライバシー・電子通信指令は、基本権憲章によって保障される基本権のみを参照して、解釈されなければならない。

さらに基本権憲章 52 条(3)は、基本権憲章と人権条約の整合性を図る必要性から規定されたものであり、この規定は EU 法および EU 司法裁判所の自律性にマイナスにならないように置かれたものである。

52 条(3)の第 2 文が明確に規定しているように、第 1 文は人権条約をより拡大して保護することを、EU 法が規定することを排除していない。基本権憲章 7 条の規定とは区別される 8 条の権利は、人権条約にはそれに見合う規定がないことも付け加えておきたい。

EU 司法裁判所の判例によれば、先決判決を求める正当性は、一般的または仮定の質問に助言的な意見を求めるものではなく、EU 法に関する紛争の効果的な解決のために必要だからである。

この第 2 質問は、Case C-698/15 の紛争において、プライバシー・電子通信指令の解釈に影響を与えるものではない。

従って、Case C-698/15 の第 2 質問は肯定できない（inadmissible）。

(2)判決

1) 基本権憲章 7 条・8 条・11 条および 52 条(1)に照らすと、プライバシー・電子通信指令 15 条(1)は、犯罪と戦うために、すべての電子通信手段に関してすべての加入者・登録利用者の、すべてのトラフィックおよび位置データの一般的かつ無差別の保存を規定する国内法を排除していると解さなければならない。
2) 基本権憲章 7 条・8 条・11 条および 52 条(1)に照らすと、プライバシー・電子通信指令 15 条(1)は、トラフィックおよび位置データの保護とセキュリティ、特に権限ある国の機関の保存データへのアクセスを規律している国内法が、以下のような場合には排除するように解釈されなければならない。
すなわち、アクセスの目的が犯罪と戦う場合に重大犯罪のみに限定されていない場合、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、およびデータを EU 域内の保存する規定がない場合。
3) 英国高等法院からの第 2 質問は、容認できない（inadmissible)。

3.1.3 本判決の論点

1.2 で述べたデータ保存指令無効判決では、データ保存を加盟国に義務付ける指令そのものの EU 法との適合性が問われた判決である。

EU 法では基本権憲章などが一次法に、指令などが二次法に位置付けられている。従って一次法[35]に対する二次法の適合性の評価を行っているのが、データ保存指令無効判決である。

しかしこの判決では、データ保存に関する適合性の判断がなされただけで、保存されているデータへの国の機関によるアクセスの適合性については判断していないというのが、付託裁判所（控訴審）の判断であり、本判決はアクセスの適合性についても審理が行われた。

スウェーデンからの第 1 質問は、トラフィックの全体的な保存を規定している国内法が、基本権憲章と適合的かとの質問であり、データ保存に関する質問で

---

[35] 「EU 法における一次法とは、（中略）EU 条約および EU 機能条約、EU 基本権憲章、EU 司法裁判所の判例法において発展させられた法の一般原則、EU 司法裁判所のより確立され、EU 法秩序の基礎をなす EU 法の直接効果および優越性の原則などから成り、広義の EU 憲法を形成している。」「二次法また派生法とは、狭義には基本条約規定に基づき EU 諸機関により採択された「立法行為」を指す（以下略)」出典：庄司、前掲注 4 p198。

「規則、指令および決定などの第二次法は、EU 条約および EU 運営条約などの第一次法に適合する形で解釈されなければならない。」出典：中西、前掲注 2 p102

ある。

これに対して英国の第 1 質問およびスウェーデンの第 2 質問は、プライバシー・電子通信指令 15 条(1)は、国の機関の保存データへのアクセスを規定する国内法が以下の場合に、その国内法を排除していると解すべきかを問う質問である。

① 国の機関のアクセスが、重大犯罪と戦う場合に限定されていない場合
② 裁判所または独立行政機関の事前承認を得ていない場合
③ 保存データの EU 域内の保存を規定していない場合

この質問に対して、以下の判決がなされている。

1) プライバシー・電子通信指令 15 条(1)は、すべての電子通信に関して、すべての加入者・登録利用者の、すべてのトラフィックおよび位置データの、一般的かつ無差別な保存を規定する国内法を、排除していると解さなければならない。
2) 指令 15 条(1)は、重大犯罪との戦いに限定していない場合、裁判所または独立行政機関の事前承認を得ていない場合、および保存データの EU 域内保存を規定していない場合の 3 つの場合に該当する国内法を、排除していると解さなければならない。

従ってデータ保存指令無効判決は、データ保存自体の基本権憲章との適合性に対する判決であるが、本判決はこれに加えて、基本権憲章に照らして、国の機関のアクセスが認められない場合がどのような場合なのかを示した判決であることに意義があると考えられる。

3.2 英国国内裁判所の IPA2016 違法判決（Liberty 判決）

（2018 年 4 月 27 日、Case No :CO/1052/2017）

3.2.1　訴訟のテーマと本訴訟までの経過

(1)訴訟のテーマ

本判決は、Liberty（The National Council of Civil Liberty）が内務省と外務省に対して、IPA2016（3.2 では以下 IPA）の EU 法と人権条約との適合性について、2017 年 2 月 28 日に High Court に提起した訴訟に対する判決である。

本判決においては、その訴えの中での IPA4 編（保存通知）の適合性について審理が行われた。

(2)本訴訟までの経過

この問題の始まりは、EU 司法裁判所のデータ保存指令の無効判決である。英

国では、データ保存指令の国内実施法がデータ保護規則 2009 であったが、EU 司法裁判所の無効判決を受けて DRIPA2014(3.2 では以下 DRIPA)が制定された。

High Court がその DRIPA1 条の無効判決を下したが、政府側が控訴。これに対して控訴審は、EU 司法裁判所に先決判決を求め付託した。スウェーデンの訴訟と併合審査が行われ、EU 司法裁判所は、2016 年 12 月 21 日に DRIPA の違法判決を下した。

これを受けて、控訴審は審理を再開。2018 年 1 月 30 日には既に DRIPA は廃止されていたが、以下の 2 点において EU 法と不適合との宣言を行った。

1)保存データへのアクセスが、重大犯罪と戦う目的に限定されていない。

2)保存データへのアクセスが、裁判所または独立行政機関の事前承認を得ていない。

3.2.2 審理および判決

(1)審理

審理の中で政府側は、原告側の IPA4 編の以下の主張については争わないと述べた。

① 刑事犯罪の分野において、保存されている通信データへのアクセスとその利用が重大犯罪と戦うとの目的に限定されていない。

② 保存データへのアクセスが、事前審査に服していない。

また審理では双方の主張と裁判所の判断が示されたが、その主要争点についての裁判所の判断について述べる。

1) Liberty 側は、IPA61 条(7)(e)、(f)および(j)の許可申請事由[36]は、e-Privacy 指令[37]15 条(1)[38]が定める適用除外に該当しないと主張した。

---

[36] (e)公衆衛生（public health）、(7)税金事案（tax matters）、(j)金融サービス・市場規制および金融の安定（regulation of financial services/markets and financial stability）

[37] 本判決では e-Privacy 指令との用語が使われているが、これまでの裁判ではプライバシー・電子通信指令と呼ばれている指令のことである。

[38] e-Privacy 指令 15 条(1)は、本指令の 5 条（通信の秘匿性）、6 条（トラフィックデータ）、8 条（発信者番号表示）および 9 条（位置データ）の適用を加盟国は制限できるとの規定である。また 15 条における全ての方策は、EU 条約 6 条(1)(2)を含み EU 法の一般的原則に合致するものでなければならない。

EU 条約 6 条(1)は、基本権憲章の権利、自由および原則は、条約と同等の法的価値を有すること、(2)は EU は人権条約に加入するが、その加入は EU の権限に影響を与えないこと、および人権条約が保障する基本的権利が EU 法の一般的原則を構成することを定めている。

政府側は提案中の改正法では、これらの申請事由は削除されていると主張した。両者の主張を受けて裁判所は、現時点では不適合宣言をする必要性はないと判断した。

2) EU 法の国家安全保障に関する国内法への適用の可否

EU 司法裁判所判決は刑事事件に関する判決であるが、政府側は EU 条約 4 条(2)、e-Privacy 指令 1 条(3) の規定を根拠に、IPA の国家安全保障に関する規定は、EU 法の適用対象外であると主張した。

この問題について裁判所は、EU 司法裁判所へ先決判決を付託している Privacy International 訴訟で同様の質問がなされているので、その結果がでるまで審理を停止するとした。

3) データの一般的かつ無差別な保存

EU 司法裁判所の DRIPA 違法判決では、e-Privacy 指令 15 条(1)は、犯罪と戦う目的で、すべての電子通信手段に関して、すべての加入者・登録利用者の、すべてのトラフィックおよび位置データの、一般的かつ無差別な保存を規定する国内法を排除しているとしている。この判決部分は、3.1.3 で述べたようにスウェーデンの質問に対する判決である。

これに対して本判決では、IPA4 編の規定は一般的かつ無差別な通信データの保存を規定しているものではないとして、以下の 7 つの理由を挙げている。

① IPA4 編は一般的かつ無差別な通信データの保存を義務付けていない。国務大臣が通知を発出し、電気通信事業者にデータの保存を求める規定である。
② 国務大臣は必要性と比例性を考慮して、保存通知を発出している。
③ 原告（liberty）は 87 条(2)の全てのデータの保存を求めるとの規定を重視しているが、必要性と比例性のテストを満たすこととの法的規定を見過ごしている。
④ 保存期間は、12 か月を超えないことになっている。
⑤ 88 条(1)では通知を発する前に、国務大臣は通知により得られる便益、通知に係る利用者数、通知を遵守するための技術的可能性とコストを考慮しなければならないと規定している。
⑥ 87 条(1)では国務大臣が通知を発出するためには、司法コミッショナーの事前承認が必要と規定している。
⑦ 電気通信事業者は、90 条・91 条の規定によって、正規の審査手続きを求めて、国務大臣に通知を返却できる。

以上の理由に基づいて、IPA4 編は一般的かつ無差別な通信データの保存を認めていないので、IPA4 編が EU 法と適合しないとの原告の主張は認められないと判決している。

4）EU 域内でのデータ保存

EU 司法裁判所の DRIPA 違法判決において、データは EU 域内に保存すべきと判決したが、EU 域内の保存が絶対的なものか、保護措置に従う場合に域外に移転することを認めるのかが、本訴訟で提起された。

この問題について裁判所は、EU 司法裁判所へ先決判決を求めている Privacy International 訴訟で同様の質問がなされているので、その結果がでるまで審理を停止するとした。

5）データ保存の対象となった人への通知

EU 司法裁判所の判決では、データへのアクセスが認められた場合に、捜査に支障がなくなったら、速やかに本人に通知しなければならないと判決した。

控訴審では、この言明は裁判所の本論ではないとしたので、原告は判決を明確にするために先決判決を求めるべきと主張した。

原告は通知がなければ、データにアクセスされた人が救済を受けることができないからであると主張している。

EU 司法裁判所の判決は、アクセスされたデータに関する通知である。裁判所はすべての保存データの通知を一般的な法的要件とすることは現実的ではないと判断している。

この問題についても裁判所は、EU 司法裁判所へ先決判決を求めている Privacy International 訴訟で同様の質問がなされているので、その結果がでるまで審理を停止するとした。

（2）判決

1）IPA4 編は、刑事事件の分野において、以下の理由によって EU 法の基本権に対して不適合である。

① 保存データへのアクセスが、重大犯罪と戦う目的に限定されていない

② 保存データへのアクセスが、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

2）合理的な期間内に法を改正しなければならないし、またその合理的期間は本判決から 2018 年 11 月 1 日までである。また適切な救済措置は、不適合宣言[39]である。

---

[39] 不適合宣言は、1998 年人権法 4 条に規定されている。国内法が人権条約に適合していないと判断される場合に出される。この宣言は国内法を無効にする効力はなく、宣言の対応は議会などに任されている。また EU 法違反の場合には、order of disapplication という方法もある。出典： “The Enforcement of the ECHR and EU Charter in national

3.2.3　本判決の論点

3.1 は EU 司法裁判所による DRIPA1 条の違法判決であるのに対して、本判決は英国国内の裁判所による、IPA4 編の EU 法との適合性に関する判決である。

本判決では 3.3 で述べる Privacy International 訴訟で同様の質問がなされているので、EU 司法裁判所の判決待ちとの理由で、原告の訴えのいくつかの点について審理を停止するとした。

本判決では、IPA4 編は EU 法と適合的ではなく、違法であるとの判決ではあるが、その理由は DRIPA 違法判決の理由と同じである。

本判決で最も注目すべき論点は、IPA4 編は DRIPA 判決で違法と判断された一般的かつ無差別な通信データの保存を命ずる規定ではない、と判決されたことである。

一般的かつ無差別な通信データの保存との問題は、本稿での英国法やフランス法など EU 加盟国の国内法の規定を巡り、EU 司法裁判所の判決で審理されている問題であり、この問題について High Court が IPA4 編のその該当性を否定したことは注目すべき判決であると考えられる。

この論点は、7.6 で述べる欧州委員会の英国に対する十分性認定の実施決定文書でも言及されている。

3.3　IPA2016 の 2018 年改正

(1) The Data Retention and Acquisition Regulation[40]（データ保存および取得規則）2018 による改正

2016 年 12 月 21 日の EU 司法裁判所の DRIPA 違法判決に対して、IPA を改正するための本 Regulation が 2018 年 6 月に議会に提出された。

改正内容は、判決内容を反映して、ほぼ IPA2016 の 3 編と 4 編についての改正である。

(2) 本規則の議会提出までの経過

政府は EU 司法裁判所の 2016 年 12 月 21 日の DRIPA2014 無効判決へ対応

---

law" House of Lords- The UK. The EU and a British Bill of Rights-European Union Committee (parliament.uk)

[40] 国内法が EU 法違反であるとの判決があった場合に、ヨーロッパコミュニティ法 1972 の 2(2)の規定によって、Regulation により国内法が改正される。（EU 離脱前の規定）

するため、2017 年 11 月に通信データ保存についての諮問（日本のパブコメに相当）、および 2017 年 2 月に Codes of Practice についての諮問を行い、その結果に関する政府の対応方針をそれぞれ 2018 年 6 月および 2017 年 12 月に公表した。

通信データの保存についての政府方針では、8 項目が取り上げられている。

主な項目としては、①e-Privacy 指令のトラフィックデータ・位置データと IPA の entity データ・event データの関係、②独立した許可、③（通信データ）取得の重大犯罪へ制限、④英国法は一般的かつ無差別な保存の規定ではなく、このことは国内裁判所も認めていること、⑤保存データのセキュリティ、⑥自身の保存データにアクセスされた場合の本人への通知(notification)のあり方、がある。

なお、英国政府は国家安全保障に関するデータ保存なりアクセスに関しては、EU 法の適用外であると述べているが、EU 司法裁判所において係争中であるので、諮問事項には入れていないと述べている。

(3) 改正内容

改正内容は、EU 司法裁判所の判決および保存通知に関する諮問事項について、政府方針を反映したものとなっている。

1）3 編は 61 条から 86 条までの 26 条構成であるが、60A 条と 61A 条が追加され、74 条と 75 条が削除されたほか、19 条に亘り改正されている。

2）60A 条では、内部許可に対する批判を受けて、調査権限コミッショナーにも国家安全保障など 7 つの理由がある場合には、また指定機関の上級者は 3 つの理由がある場合に許可権限が付与されている。

3) 保存データへのアクセスが重大犯罪に限定されていないとの判決に対応するために、重大犯罪の定義が 263 条において 3 年以上の罪に該当する場合と規定されている。

政府方針ではこの 3 年以上の罪に該当しない犯罪でも保存データへのアクセスは必要であるとして、保存データへのアクセス根拠として、国家安全保障目的などと並んで犯罪目的との根拠が入っている。

この犯罪目的の規定では、EU 司法裁判所の判決でいうトラフィックおよび位置データは、IPA における events data に含まれるので、重大犯罪に限定されているのに対して、他の場合には犯罪防止・探知または騒乱防止を申請根拠として認めている（60A 条(7)(8)）。

なおこの犯罪目的を根拠とする規定は、61 条、61A 条など他の条文においても規定がある。

4)新たに追加された 61A では、指定上級者に緊急時に 5 つの理由がある場合

に、許可権限を付与している。また地方自治体への許可は犯罪目的のみである（73 条）
5)4 編では、許可の理由が、Liberty 判決でも述べられたように、公衆衛生などの理由が削除されて、10 から 7 つとなった（87 条)。また、国務大臣が保存通知を発出するときに考慮すべき事項が追加されている（88 条）
6)細則(Schedule4)の表が全面改正されているほか、8 編 227 条の調査権限コミッショナーの条文に軽微な条文が追加されている。

(4) 他の Regulation などによる IPA2016 の改正

4 編（保存通知）の改正はすべてデータ保存および取得規則 2018 による改正であるが、3 編（取得許可）はこの他、通信データ取得規則 2019 などによっても改正されている。

また、1 編から細則 1-10（細則 7 は除く）は、2017 年から 2023 年にかけて約 20 の Regulation などによって改正されている。

(5) 英国・米国間のデータアクセス協定

同協定は 2019 年 10 月に調印され 2022 年 10 月に発効したが、重大犯罪の防止・捜査・起訴の目的で、相手国の電気通信事業者が保存する通信データ（バルクデータを除く）を直接請求できるようにする協定である。

この協定の履行状況に対する監督権限が、調査権限コミッショナーの監督権限に追加された(229 条 3A、改正手続きは 239 条(1))。

またこの協定の締結によって、IPA2016 の他の条項や他の法律も改正されている。

3.4 EU 司法裁判所の Privacy International 判決（2020 年 10 月 6 日）（Case　C-623/11）

IPA2016 を改正した The Data Retention and Acquisition Regulation（データ保存および取得規則）2018 成立後においても、EU 司法裁判所における本判決および 3-6 で述べる人権裁判所の RIPA2000 に対する違法判決がなされている。

本項では、Privacy International が英国の IPT（調査権限行政審判所）へ訴訟提起をして、IPT が EU 司法裁判所に先決判決を求めて付託した事案について述べる。なお本判決は、3.5 で述べる La Quadrature du Net と同じ日になされた判決である。

3.4.1 付託事項、関係法条文、争点および付託された質問

(1)先決判決付託事項（judgment）

1) EU 条約 4 条(2)および EU 基本権憲章 7 条、8 条および 52 条(1)の規定に照らした、プライバシー・電子通信指令 1 条(3)および 15 条(1)の解釈

2) Privacy International と外務大臣・内務大臣・GCHQ・MI5・MI6 の間での、インテリジェンス機関によるバルク通信データの取得および利用を許可する法律の EU 法との適合性

(2) 関係法条文（Legal Context）

・EU 法：データ保存指令、プライバシー・電子通信指令、GDPR

・英国法：1984 年電気通信法 94 条、RIPA2000 の 21 条(4)(6)、65 条から 69 条

(3)先決判決付託に至る争点

2015 年始めに、インテリジェンス機関（GCHQ、MI5、MI6）によるバルク通信データの取得および利用慣行が公になった。2015 年 6 月 5 日、Privacy International がこれらの慣行の適合性に関して、IPT に訴えを提起した。

IPT は 2016 年 10 月 17 日の審決で、バルク・パーソナル・データセットがおそらく秘密裏に取得され、分析され、他の人や機関に開示され、外国のパートナーと共有されていると認定した。

またインテリジェンス機関は、1984 年電気通信法 94 条に基づき、国務大臣の指示（directions）によって、電気通信事業者からバルク通信データも取得していたことは、国内法および人権条約 8 条と適合的と判決した。

IPT は、取得および利用手法の EU 法のもとでの適合性に関しては、2017 年 9 月 8 日の判決において、バルク通信データに関しては EU 法においては適合的としたが、上記の法的手続きを経ていないデータ取得は適合的ではないと判決した。

IPT はこの判断に基づいて、現在の制度が EU 法に適合的との判断を求めて、EU 司法裁判所へ先決判決付託を行った。

なお付託裁判所は、バルク・データ取得の有効性について、2016 年 8 月 19 日のアンダーソン報告書に言及している。またバルク通信データの利用に関する保護措置は、人権条約の要求事項と適合的であると判断している。

さらに政府側がデータへのアクセスと利用は、EU 条約 4 条(2)を根拠に EU は権限外であると主張したことも付言している。

(4)先決判決へ付託された質問

＊第１質問：EU 条約 4 条(2)およびプライバシー・電子通信指令 1 条(3)に関して、国務大臣が電気通信事業者にバルク通信データをインテリジェンス機関に提供することを指示する要件は、EU 法および同指令の適用範囲内にあるか？

＊第２質問：もし第１質問が是であれば、DRIPA2014 判決で示された保存されている通信データに適用される要件、または人権条約による要件は国務大臣の指示に適用されるか？　もし適用されるとすれば、いかにまたどの程度それらの要件は適用されるか？

3.4.2　付託された質問についての審理

(1)第１問

Privacy International の主張は、1) 1984 年電気通信法 94 条の基づき、インテリジェンス機関が事業者からデータ取得およびそれを利用する行為は、プライバシー・電子通信指令（以下本項では指令）の対象となる。2) 指令 15 条(1)に国家安全保障が適用外になるとの文言は、指令が国家安全保障に適用されないことを意味せず、この規定は EU 条約 4 条(2)によって影響されない。

一方、英国を含む 9 つの政府は、EU4 条(2)に国家安全保障は加盟国の責任であると規定されているので、指令は国家安全保障に関する国内法には適用されないと主張した。

指令 1 条は指令の目的の規定であるが、その(1)では電子通信部門の個人データの取扱いに関して、基本的人権の保護、特にプライバシーや秘匿性に関して加盟国間で同等の水準になるように、各国間の規定の調和を図ることであると規定している。

また、指令 1 条(3)、3 条、15 条の解釈についても審理を行っている。

これらの審理から、第 1 問への答えは以下の通りと述べている。

EU 条約 4 条(2)に照らして、指令 1 条(3)、3 条および 15 条(1)は、国の機関が電気通信事業者にトラフィックおよび位置データを、国家安全保障目的でインテリジェンス機関に引渡すことを可能にする国内法は、同指令の対象となると解さなければならない。

(2)第２問

EU 条約 4 条(2)、基本権憲章 7 条、8 条、11 条および 52 条(1)に照らして、指令 15 条(1)は、電子通信事業者に一般的かつ無差別なトラフィックおよび位置データを、国家安全保障目的で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を排除していると解されるべきかの確認を求めるものである。

指令 5 条(1)は、加盟国は通信および関連するトラフィックデータの秘匿性を、保障すると規定している。

しかし指令 15 条(1)では、加盟国が国家安全保障などのために、指令 5 条(1)の例外規定を導入することを可能にしている。このため加盟国は一定の期間、データ保存をできるようにする法的措置を採用できる。

但し、指令 5 条、6 条および 9 条の権利の制限は例外的なものであって、それがルールになることは認められない。従って、指令 15 条(1)の解釈としては、基本権憲章 7 条のプライバシー、8 条の個人データの保護、11 条の表現の自由の重要性を考慮しなければならない。

一方で、基本権憲章 7 条、8 条および 11 条は、絶対的な権利ではなく、社会におけるそれらの役割との関係で考慮されなければならない。

基本権憲章 52 条(1)は、これらの権利の制限は意図する目的に対して厳密に比例的でなければならないと規定している。この厳密な比例性を充足するためには、権利を制限する国内法に明確かつ詳細な規定を置かなければならない。

国内法が指令 15 条(1)の要件に合致しているかについては、基本権憲章 7 条、8 条、11 条および 52 条(1)の規定に照らして、インテリジェンス機関にトラフィックおよび位置データを引渡すことは、秘匿性原則から逸脱していることに留意すべきである。

本件のように、一般的かつ無差別な方法による運用は、データの秘匿性に対する例外をルールにするものであり、例外は例外で留まるべきである。

トラフィックおよび位置データのインテリジェンス機関への引渡しに伴う基本権憲章 7 条の権利への干渉は、特に重大であると見做さなければならない。この引き渡しによって、当該データの対象になっている人のプロファイリングができるので、通信データは通信内容に劣らずセンシティブである。

(3)判決

1)指令 1 条(3)、3 条および 15 条(1)は、EU 条約 4 条(2)に照らすと、国家安全保障目的でインテリジェンス機関に、トラフィックおよび位置データの引渡しを電子通信事業者に求めることを可能にする国内法は、指令の対象であると解さなければならない。

2)指令 15 条(1)は、国家安全保障目的で一般的かつ無差別なトラフィックおよび位置データのインテリジェンス機関への引渡しを、電子通信事業者に求めることを可能にする国内法を排除している、と解さなければならない。

3.4.3　本判決の論点

DRIPA 違法判決と本判決は、いずれもプライバシー・電子通信指令の規定に対して、国内法の適合性を判断した判決である。

本判決では指令の規定の下で、国家安全保障目的で一般的かつ無差別に保存されたデータを、インテリジェンス機関へ引渡すことの適合性が問われている。

本判決では、指令はそのような国内法を排除していると解さなければならないとしている。

但し排除される国内法の規定が、インテリジェンス機関に保存データを引渡す規定なのか、また一般的かつ無差別なデータ保存の規定なのかは、判決文そのものからは読み取りにくい。

しかしインテリジェンス機関に保存データを引渡す規定が、指令で排除されているとは考えにくく、一般的かつ無差別なデータ保存の規定が指令から排除されていると考えれば、本判決はデータ保存無効判決および DRIPA 違法判決と同様の判決であると考えられる。

本判決で注目されるのは、指令は国家安全保障に関する国内法に適用されると原告(Liberty)が主張し、EU 条約 4 条(2)において国家安全保障は加盟国の責任との規定があるので、指令は国家安全保障に関する国内法に適用されないと政府側が主張したことに対して、指令は国家安全保障に関する国内法に適用されると判決したことである。

この問題は Liberty 判決では、Privacy International 判決待ちとして、審理を停止していた問題に対する回答にもなっている。なお、本判決では Liberty 判決で審理を停止していた保存データの EU 域内での保存、およびデータ保存の対象となった人への通知に関しては、言及されていない。

3.5 EU 司法裁判所 La Quadrature du Nez 判決（2020 年 10 月 6 日）

（Case C-511/18、C-512/18、C-520/18）

3.5.1 付託事項、関係法条文、および付託された質問

(1)先決判決付託事項（judgment）

1）基本権憲章 4 条、6 条、7 条、8 条、11 条、52 条(1)および EU 条約 4 条(2)に照らして、改正プライバシー・電子通信指令（Directive2002/58）15 条(1)および e コマース指令（Directive2000/31）12 条～15 条の解釈

2）Case C-511/18：La Quadrature du Net、フランス・データ・ネットワークなどとフランスの首相、内務大臣、国防大臣との間の訴訟では、2015-1185 号デクレ（2015 年 9 月 28 日）、2015-1211 号デクレ（2015 年 10 月 1 日）、2015-

1639 号デクレ（2015 年 12 月 12 日）、2016-67 号デクレ（2016 年 1 月 29 日）の適合性（lawfulness）
3）Case C-512/18：フランス・データ・ネットワーク、La Quadrature du Nez などとフランスの首相、司法大臣などとの間の訴訟では、郵便・電子通信法典（CPCE）10-13 条、2011-219 号デクレ（2011 年 2 月 25 日）の適合性
4）Case C-520/18：ベルギー企業とベルギー閣僚評議会（Council of Ministers, Belgium）との間の訴訟では、2016 年 5 月 29 日法の適合性

(2)関係法条文（legislative framework）
・EU 法：指令 95/46（データ保護指令）、指令 97/66[41]、指令 2000/31(e コマース指令)、改正プライバシー・電子通信指令（2002/58）、GDPR（2016/679）
・フランス法：国内安全法典（CSI）、郵便・電子通信法典（CPCE）、2004-575 デジタル経済信頼促進法（2004 年 6 月 21 日）、2011-219 号デクレ
・ベルギー法：2005 年 6 月 13 日電子通信法、刑事手続法典、1998 年 11 月 30 日インテリジェンス基本法

(3)先決判決付託質問
1)Case C-511/18
＊質問 1：改正プライバシー・電子通信指令（以下本項では指令）15 条(1)を根拠に、一般的かつ無差別な保存義務を事業者に課すことは、基本権憲章 6 条が保障する安全の権利および EU 条約 4 条の国家安全保障が、加盟国だけの責任であるとの規定によって正当化される干渉とみなされるか？
＊質問 2：指令は特定人物のトラフィックおよび位置データを、リアルタイム収集する立法措置を認めていると解されるか？
＊質問 3：指令は捜査上支障がなくなったら、データ主体に接続データの収集を通知することが、手続きの適合性の前提であると解されるか？　または救済が効果的であることを保障する他の保護措置を考慮すると、このような手続きを適合的とみなし得るか？
2)Case C-512-18
＊質問 1：Case C-511/18 の質問 1 と同じ。
＊質問 2：基本権憲章 6 条、7 条、8 条、11 条および 52 条(1)に照らして、e コ

[41] 電子通信部門における個人データの取扱いおよびプライバシー保護指令。プライバシー・電子通信指令により廃止され、同指令に置き換えられた指令。

マース指令（Directive 2000/31）は、オンライン通信サービスを提供する者、および無料であってもオンライン通信サービスを公衆に提供するために、サービス利用者が発信する信号、文字、画像、音声などを保存している自然人および法人にその保存を求め、民事・刑事責任の規則を遵守するために司法当局が必要とする場合に、そのデータを要求できるとする国内法を認めていると解すべきか？

3)Case C-520/18

＊質問１：指令 15 条(1)は基本権憲章 6 条、7 条、8 条および 52 条(1)と併せて読むと、重大犯罪事案の捜査などの目的だけではなく、GDPR23 条(1)が例示している、国家安全保障、領土防衛、重大犯罪以外の捜査・探知・訴追、電子通信システムの禁止されている利用の防止のために、指令の範囲内でトラフィックおよび位置データの一般的かつ無差別な保存義務を排除していると解さなければならないか？

＊質問２：指令 15 条(1)は、基本権憲章 4 条、7 条、8 条および 52 条(1)と併せて読むと、もしその立法が基本権憲章４条および７条に規定されている積極的な義務を遵守するため、特に年少者の性的搾取（abuse）に対する効果的な犯罪捜査、処罰および犯罪加害者を特定することを目的として、電子通信サービスの運用者および提供者に対して、指令の範囲内でサービス提供によって生成または取扱われるトラフィックおよび位置データの一般的保存義務を課す国内法を排除していると解さなければならないか？

＊質問３：第１および第２質問への回答の基礎として、もしベルギーの憲法裁判所が訴訟の対象となっている法律が、これらの質問対象の規定から生ずる 1 または複数の義務を果たしていないと判断するならば、法的不安定性を回避することおよび事前に収集され保存されているデータを、法目的のために利用を継続することを可能にするために、2016 年 5 月 29 日法の効力を一時的に維持して良いか？

3.5.2 付託された質問についての審理

本裁判では、付託裁判所からの質問に対して、多面的かつ詳細な審理を行っている。

(1)Case C-511/18、Case C-512/18 の第 1 質問および Case C-520/18 の第 1 および第 2 質問

指令 15 条(1)は、電子通信事業者に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を義務付ける国内法を排除していると解すべきかについて、付託裁判所は確認を求めている。

すべての利用者に適用されること、および保存期間が 1 年間であること、またフランス国務院とベルギー憲法裁判所は、トラフィックおよび位置データの保存と、国の機関によるそのデータへのアクセスを定めた国内法は指令の対象になるとの前提から審理を行っているが、審理に参加している当事者および 9 つの加盟国政府[42]から特に指令 1 条(3)の解釈に対して反対していることを踏まえて、まず当該国内法が同指令の適用対象になるかを検討する必要があるとして、指令の適用範囲の問題および指令 15 条(1)の解釈について審理している。

審理において EU 条約 4 条(2)は、国家安全保障目的の措置を講ずるとの事実だけで、EU 法が適用できないとか、EU 法の遵守義務を加盟国が免除されるとはならないとして、適用対象になると判断している。

ついで、個人データの保存を求める立法は、保存されるデータと立法目的の間のつながりを示す客観的な指標（criteria）を常に満たさなければならないとして、以下について審理している。

① 国家安全保障目的のために、予防的にトラフィック及び位置データの保存を規定する立法措置
② 犯罪との戦いおよび公共安全目的のために、予防的にトラフィックおよび位置データの保存を規定する立法措置
③ 犯罪との戦いおよび公共安全目的のために、予防的に civil identity[43]に関連する IP アドレスの保存を規定する立法措置
④ 重大犯罪との戦いの目的で、優先処理される（expedited） トラフィックおよび位置データの保存を規定する立法措置

この審理の結果、これらの質問への回答としては、15 条(1)は、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を義務付ける立法措置は、予防的措置としては排除されると解釈しなければならないが、指令 15 条(1)は以下の立法措置を排除していないとして、後述する判決文において、許容される立法措置の内容について述べている。

(2)Case C-511/18 の第 2 および第 3 質問

この質問は指令 15 条(1)が、電子通信事業者に対して、第 1 にトラフィック

---

[42] 以下の 9 つの加盟国政府は、国内法は安全保障目的の立法なので、同指令はその国内法には適用されないとの意見を提出している。チェコ、エストニア、アイルランド、フランス、キプロス、ハンガリー、ポーランド、スウェーデン、英国。

[43] civil identity の例としては、氏名、郵便番号、e メールアドレス、パスワード、口座番号、支払い方法、決済金額と日時などが示されている。

および位置データの自動分析およびリアルタイム収集、第 2 に使用されて端末機器の位置データに関する技術的データのリアルタイム収集を命ずる場合に、その収集対象の個人および収集の通知に関する規定がない国内法を排除するように解釈されなければならないかを問う質問である。

ここではトラフィックおよび位置データの自動分析、同データのリアルタイム収集、データ収集および分析の対象となっている人への通知についてそれぞれ審理されていて、後述する判決文において、許容される立法措置の内容について述べている。

(3)Case C-512/18 の第 2 質問

この質問は、e コマース指令（Directive 2000/31）が、オンライン通信サービスへのアクセスを提供する事業者およびホスティングサービス事業者に対して、個人データを一般的かつ無差別に保存することを求める国内法を排除するように解釈しなければならないかを問う質問である。

これらについての審理を行い、後述する判決文の内容について述べている。

(4)Case C-520/18 の第 3 質問

違法宣言を一時的に制限する権限を与える国内法条項が、基本権憲章 7 条、8 条、11 条および 52 条(1)に照らして、国内法が指令 15 条(1)に反している場合に、適用して良いかを問う質問である。

この質問については、EU 法を優先させる観点から審理を行っていて、一時的にせよ国内法を EU 法より優先させることは、EU 法の優位性と統一的な適用を損なうものであるとして、後述する判決文の内容について述べている。

3.5.3 判決

(1)指令 15 条(1)は、予防的措置として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を規定する立法措置を、排除していると解しなければならない。一方指令 15 条(1)は、次のような立法措置を排除していない。

1)国家安全保障目的で電子通信事業者に対して、トラフィックおよび位置データの一般的かつ無差別な保存を求めることは、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、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、およびその指示が真に必要である期間にのみ限定されている場合は許される。なお脅威が継続しているならば、期間延長は可。

2)国家安全保障、重大な犯罪との戦いおよび公共安全への真の脅威を防止する目的で、客観的で無差別な要因（factor） に基づいて、当該人物の類型または

地理的な指標に従い、厳に必要な期間に限定して、特定対象のトラフィックおよび位置データの保存について規定すること
3)国家安全保障、重大犯罪との戦いおよび公共安全への重大脅威の防止目的で、真に必要な期間に限定して、インターネット接続に割当てられた IP アドレスの一般的かつ無差別な保存を規定すること
4)国家安全保障、犯罪との戦いおよび公共安全への重大脅威の防止目的で、電子通信システムの civil identity に関する一般的かつ無差別なデータの保存を規定すること
5)重大犯罪およびとりわけ国家安全保障目的で、効果的な司法審査に服する権限ある機関の決定によって、電子通信事業者に対して、特定の期間トラフィックおよび位置データの優先保存（expedited）を求める指示を行うこと
　これらの措置は、明確かつ詳細なルールによって、当該データの保存が実体的かつ手続き的な条件に従っていて、当該人物が濫用リスクから効果的に保護されている場合に認められる。

(2)指令 15 条(1)は電子通信事業者に対して、第 1 にトラフィックおよび位置データの自動的分析およびリアルタイム取得を、第 2 に端末機器の位置に関する技術的データのリアルタイム収集を求める国のルールを、以下の場合には排除していないと解さなければならない。
1)自動的分析が、当該加盟国が現在または予見できる将来に、国家安全保障への真に重大な脅威に直面している状況に限定される場合
2)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
3)トラフィックおよび位置データのリアルタイム取集が、何らかのテロ活動に関わっているとの疑いに確固たる理由がある人物に限定されていて、かつそのようなリアルタイム収集が真に必要な期間の限り認められることを保障するために、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

(3) e コマース指令は、通信の秘匿性および情報社会サービスにおける自然人の保護の分野には適用されないと解さなければならない。
　これらの保護は、指令または GDPR によって保護される。GDPR23 条(1)は、オンライン通信サービスへのアクセス事業者およびホスティングサービス事業者に対して、そのサービスに関する個人データを一般的かつ無差別的に保存することを求める国内法を排除していると解さなければならない。

(4) 電子通信事業者へ国家安全保障および犯罪との戦いに関して、指令 15 条(1)に反する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を義務付ける国内法に関して、違法宣言の効力を一時的に制限する権限を与える国内法の規定を、国内裁判所は適用しないものとする。

指令 15 条(1)は、EU 法に反して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よって得られた情報や証拠を、国内刑事裁判所が採用しないように求めている。

3.5.4 本判決の論点

EU 司法裁判所の DRIPA2014 無効判決および Privacy International 判決が、英国国内法の EU 法との適合性に関する判決であるのに対して、本判決はフランスおよびベルギーの国内法の EU 法との適合性に関する判決である。

これら 3 つの判決では、いずれも一般的かつ無差別なデータ保存を、基本憲章に照らしたプライバシー・電子通信指令の解釈とは不適合であるとしている。

データ保存指令無効判決では、一般的かつ無制限なデータ保存を規定している指令そのものが、基本権憲章と不適合であるとされている。

これら 4 つの判決では、すべて一般的かつ無差別なデータ保存を義務付ける国内法なり指令は、認められないとする点では共通している。

一方で 3.5.3(1)(2)で述べたように、本判決ではプライバシー・電子通信指令 15 条(1)は、国家安全保障、重大な犯罪との戦いおよび公共安全に対する真の脅威がある場合には、いくつもの例外を認めていて、DRIPA2014 無効判決および本判決と同じ日の判決である Privacy International 判決とは、かなりトーンが異なるように考えられる。

但し例外を認める条件として、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こと、および真に必要な期間に限定していることを挙げている。これに加えて明確かつ詳細なルールによって、当該人物が濫用リスクから効果的に保護される場合に限り、認められるとしている。

この他保存データのなかで、IP アドレスと civil identity の一般的かつ無差別な保存する規定を認めている。

本判決では予防措置として、一般的かつ無差別なデータ保存を認めていないが、国家安全、重大犯罪との戦いおよび公共安全の防止する目的で、特定対象のトラフィックおよび位置データの保存を認めている。

また判決(4)で、EU 法が国内法に優先して適用されるべきことを明確にしている。

4. 欧州人権裁判所の Big Brother Watch 判決と英国政府の対応

4.1 欧州人権裁判所の Big Brother Watch 判決

（2021 年 5 月 25 日、nos.58170/13、62322/14、24960/15）

4.1.1 経過および争点

(1)人権裁判所大法廷への付託までの経過

スノーデンの暴露を契機として英国では 16 団体が、英国政府の調査権限に関して IPT（調査権限行政審判所）へ提訴した。IPT はそれらの提訴を 3 つのグループに分けて審理した。まず 2014 年 12 月 5 日の第 1 判決において、外国のインテリジェンス機関によって傍受された通信の情報を受取ることについては適合的とした。

また 2015 年 2 月 6 日の第 2 判決において、RIPA2000 8 条(4)（バルク通信傍受）の域外規定については、傍受の仕組みの公表後の傍受については適合的とした。

さらに 2015 年 6 月 22 日（2015 年 7 月 1 日の修正）の第 3 判決において、一部不備があったが是正されているので、RIPA2000 8 条(4)は適合的とした。

これを不服として、16 団体が人権裁判所[44]に訴訟提起を行った。小法廷第 1 部の判決では、16 団体の訴えについて、RIPA2000 8 条(4) および同法 1 編 2 章（通信データ取得）に関しては人権条約 8 条および 10 条違反と判決、またインテリジェンス情報の共有については人権条約 8 条違反ではないとの判決を下した。

この判決について、大法廷への移送の申請があって、受理されたために大法廷での審理が行われた。

(2) 訴訟の争点

この訴訟は、スノーデンの電子監視プログラムに関する暴露を契機として、

---

[44] 人権裁判所は人権条約 26 条において、単独判事(single-judge formation)、委員会（committee)、小法廷（原則判事 7 人)、大法廷（判事 17 人）の 4 部構成となっていて、27 条、28 条、29 条および 31 条でそれぞれの権限・役割が規定されている。また、小法廷から大法廷への付託については 30 条、43 条に規定されている。また人権裁判所への提訴は個人、非政府組織または個人のグループによる提訴（34 条）と加盟国間の訴訟（33 条）とがある。

提起されたものである。訴訟提起者は彼らの通信が、英国のインテリジェンス機関によって傍受されているか、外国政府が傍受して英国のインテリジェンス機関がその情報を受領しているか、および/または、通信事業者から英国の機関によって取得されていると信じていた。

この訴えに対して、人権裁判所はまずインターネットの秘密の監視スキームについて、英国のバルク通信傍受、インテリジェンス情報の共有、通信事業者からの通信データの取得、米国のプリズムプログラムおよびアップストリームプログラムについて審理している。

4.1.2 法的枠組みおよび慣行

以下のように詳細な調査が行われている。

(1) 英国国内法

①通信傍受：RIPA2000

＊令状：1 条(1)、8 条(4)。

＊保護措置：15 条、16 条

＊通信傍受実施規則（Code of Practice）

②インテリジェンス共有

＊英米通信インテリジェンス協定

＊インテリジェンス活動の法的枠組み

＊通信傍受実施規則（Code of Practice）

③通信データ取得：RIPA2000 1 篇 2 章

④IPT の慣行と手続き

＊RIPA2000

＊IPT 規則

⑤監督

⑥インテリジェンス機関の通信傍受活動に関する報告書など

＊議会のインテリジェンス委員会の 2013 年 7 月の声明（statement）

＊テロの立法に関する調査権限報告（アンダーソンレポート[45]）などの報告書

また、IPA2016 の規定についても審理が行われている。Liberty 判決において、政府側は IPA2016 の 4 編は EU 法に反していることを認め、（国内）裁判所は刑事法分野での保存データへのアクセスが重大犯罪に限定されていないこと、および保存データへのアクセスが裁判所または独立行政機関の事前審査を

[45] アンダーソンレポートは、2015 年の調査権限草案の議会の事前審査において提出された報告書である。

受けていないことを理由に、4 編は EU 法の基本権に反しているとの判決を下したと述べている。

⑵国際法
①国連：2013 年 12 月 18 日の総会によって採択された決議 68/167 号
②欧州評議会
＊欧州人権条約
＊2001 年 11 月 8 日の個人データの自動処理に関する個人の保護条約への追加議定書[46]（CETS No.181）
＊電気通信サービス分野における個人データ保護に関する閣僚委員会の勧告
＊シギント機関の民主的監督に関する欧州委員会の 2015 年レポート（1995 年 2 月 7 日採択）

⑶EU 法
①基本権憲章
②データ保護指令および GDPR
関連する判例法として以下の EU 司法裁判所の判決内容の論旨について述べられている。
＊Digital Rights Ireland（データ保存指令無効）判決（2014 年 4 月 8 日）
＊Tele2 Sverige AB・Tom Watson（DRIPA 違法判決）（2016 年 12 月 21 日）
＊Ministerio Fiscal 判決（スペインから付託された先決判決）（2018 年 10 月 2 日）
＊Schrems I（セーフハーバー無効）判決（2015 年 10 月 6 日）
＊Schrems Ⅱ（プライバシー・シールド無効）判決（2020 年 7 月 16 日）
＊Privacy International 判決および La Quadrature du Nez 判決（両判決とも 2020 年 10 月 6 日）

4.1.3 審理および判決
3 件の合同訴訟における訴えは、RIPA2000（本項では以下 RIPA）8 条(4)、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および通信事業者からの通信データの取得の 3 つの事項について、人権条約 8 条および 10 条との適合性（compatibility）について審理が行われた。

---

[46] 欧州評議会の第 108 号条約（1985 年 10 月 1 日発効）に関する追加議定書（2001 年 11 月 8 日署名、2014 年 7 月 1 日発効）出典：石井夏生利[2017]『新版 個人情報保護法の現在と未来』pp248-249

(1) 8 条(4)（通信傍受）の規定の適合性[47]

1）人権条約 8 条違反の主張

小法廷では権限濫用のリスクを避けるための次の 6 つの最小保護措置が示された : 通信傍受命令によって生ずる犯罪の性質、通信傍受の対象となる人の類型、通信傍受期間、傍受に引続く取得されたデータを利用し蓄積する検証手続き、他の機関へデータを伝える際に取られるべき予防策、通信傍受されたデータを消去または破壊しなければならない状況（この最小保護措置は、判例として適用されるのが通例であった。）

その上で小法廷では英国の通信傍受規定に関して、この 6 つの措置の適用について審理している。その結果、8 条(4)は通信傍受の選別語についての監督を規定していないこと、および通信データの検証に関して保護措置がないことを指摘したうえで、英国は通信傍受権限の濫用はしていないとしたものの、上記の欠陥があるために、英国の通信傍受制度は法的な質の要件（quality of law requirement）に合致していないこと、およびこの通信傍受を民主主義社会における必要性に止めていないと判決した。

大法廷はバルク通信傍受について、以下の判断を示した。

① バルク通信傍受は、加盟国が自国の安全保障への脅威を判定するために、不可欠な重要性を有していることを認める。
② しかしバルク通信傍受には、かなりの濫用の可能性がある。
③ 8 条(4)は十分な「エンド・ツー・エンド」の保護措置規定を含んでいない。特に独立した許可制度がないこと、令状申請において選択語類型がないこと、事前の内部許可に対して個人を結びつける選択語がない欠陥がある。
④ 通信傍受コミッショナーが独立した効果的な監督を行っていること、

[47] 審理の中では、バルク通信傍受は外国のインテリジェンス情報の収集および既知または未知の人物による新たな脅威に対処するために利用されていること、グローバルなインターネットの通信量が増大するにつれて脅威も増大していること、敵対国および非国家アクターにより探知されずに、デジタル領域でサイバー攻撃、国家安全保障への重大な脅威が生じていること（322~323 項）、人権条約 8 条は、国家安全保障や他の国益を対外的な脅威から守るための通信傍受を禁止していない。加盟国はどのような通信傍受を行うかの裁量を有しているが、その裁量はより狭いことおよび多くの保護措置がなければならない（347 項）と述べている。

およびIPTが強力な司法的救済手段を提供しているものの、これらの重要な保護措置の仕組みは、上記の欠陥を補うには不十分である。

以上の欠陥があるので、8条(4)は人権条約8条違反である。

2）人権条約10条違反の主張

小法廷は、訴訟提起者はジャーナリストおよびNGOに必要な通信の10条違反を主張しているが、国内法の救済措置を尽くしていないので認められないが、ジャーナリズムに関する10条の規定は大法廷に付託の範囲内と判決した。

大法廷では、小法廷の判決、関係者の主張および訴訟参加した第3者の主張について、またジャーナリスト保護の一般原則、通信傍受の文脈での10条の規定、本訴訟に採用されているアプローチなどを審理している。

これらの審理に基づき、大法廷は8条(4)の10条違反を認めた。

(2)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

大法廷に付託されるまでの経過について述べた後に、政府の反対に対する小法廷の判決について、ついで小法廷の実体審理の経過について述べている。

これらの審理に基づいて、大法廷は人権条約8条および10条違反はないと認定している。

(3)通信事業者からの通信データの取得

1)人権条約8条違反の主張

小法廷の審理中に、英国政府は現行法に代えて、新しい法律の立法過程にあった。新しい法律における通信事業者による通信データの保存規定に関しては、Libertyによって国内で訴訟提起されていた。

その審理において、英国政府はIPA4編が、EU法に反していると認めた。国内裁判所は刑事分野において保存データへのアクセスが重大犯罪に限定されていないこと、また裁判所または独立行政機関の事前審査を受けていないとの理由で、4編はEU法に違反しているとした。

小法廷は、同様の理由で人権条約8条違反と判定した。当事者はこの点について、大法廷では新たな提起を行わなかった。

大法廷は、RIPA1編2章の下での運用は、人権条約8条違反であると考える。

2)人権条約10条違反の主張

小法廷は、RIPA2章はジャーナリストの情報源を特定する場合に高度の保護を規定していると認めたものの、不十分なので人権条約10条違反であると考えた。当事者はこの点について、大法廷では争わなかった。

大法廷はRIPA1編2章の下での運用は、人権条約10条違反であると考える。

(3)判決

1）8 条(4)の人権条約 8 条違反は全員一致の判決

2）2 章の人権条約 8 条違反は全員一致の判決

3）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りは 12 対 5 で人権条約 8 条違反ではないと判決

4）第 2 訴訟での提起に関しては、8 条(4)および 2 章については、人権条約 10 条違反と全員一致の判決

5）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りは 12 対 5 で人権条約 10 条違反ではないと判決

6）3 つの訴訟提起者に、英国政府は 3 カ月以内に、それぞれ 227,500 ユーロ、90,000 ユーロ、36,000 ユーロを現地通貨で支払うことを全員一致で判決

7）訴訟提起者の公正な賠償[48]（just satisfaction）に関する残余の請求は、全員一致で棄却

4.1.4 本判決の論点

欧州人権裁判所（以下人権裁判所）は、欧州評議会（Council of Europe）が制定した欧州人権条約（以下人権条約）に基づく裁判所である。英国は欧州評議会の当初からのメンバーであり、EU 離脱後もその地位を継続しているため、人権裁判所の判決の対象となっている。

秘密裏に行われていた NSA 活動に関するスノーデンの暴露を契機として、英国の 16 団体が RIPA1 編に規定されているバルク通信傍受と通信データ取得の規定の人権条約 8 条および 10 条との適合性を問う訴訟を IPT に提起した。

判決では RIPA の当該規定は、人権条約 8 条および 10 条違反であることを全員一致で認めた。

結論だけをみると人権条約違反にはなってはいるものの、バルク通信傍受は加盟国が自国の安全保障への判定するために、不可欠な重要性を有していると認めている。また通信傍受コミッショナーが独立した効果的な監督を行っていること、および IPT が強力な司法的救済を提供していることも認めている。

しかし通信傍受規定には十分なエンド・ツー・エンドの保護措置規定がないこと、独立した（事前）許可制度がないこと、令状申請において選択語類型がないこと、事前の内部許可に対して個人を結びつける選択語がないことが、上記の効果的な監督および強力な司法的救済を上回る欠陥であることを理由とし

[48] 国内法が一部の賠償しか認めない場合に、人権裁判所が被害を受けた当事者に認める賠償のこと。人権条約 41 条に規定がある。

て、違法と判断したものである。

また通信データの規定が違法と判断された理由も、EU 司法裁判所の DRIPA2014 無効判決および英国国内裁判所の Liberty 判決と同様に、重大犯罪に限定されていないことおよび裁判所または独立行政機関の事前審査を受けていないことを理由としているが、これらの理由は既に IPA2016 では是正されている。

従ってバルク通信傍受の重要性を認めていること、および効果的な監督と強力な司法的救済を認めていることを考慮すれば、違法判決であるとはいうものの、人権制約に関する規定の見直しをすれば、適法になる可能性があることを示唆する判決であるように考えられる。

判決に対するこの受止めが正しいとすれば、この判決を受けた「4.2~4.4」および「5」に述べる英国政府の判決への対応が、違法判決に対する対応だけではなく、現在の IPA2016 の規定について法目的を達成するために適した規定（fit-for-purpose）に改正するとの視点も頷けるものと考えられる。

4.2　Big Brother Watch 判決に対する英国政府の声明（2022 年 3 月 31 日）

判決では、バルク通信傍受自体は人権条約違反ではなく、国家安全保障への脅威を判断するための手法としては、極めて重要と述べている。

RIPA2000 の規定における欠陥のいくつかは、IPA2016 によって既に是正されている。残りの課題についての政府の対処方針は以下の通り。

第 1 に、バルク通信傍受の申請において、令状を承認するために選択語(selectors)のタイプや類型を定めるべきとの判決に関しては、通信傍受によって取得したデータの検証のための現行の運用目的リストは裁判所の求めを満たすものと考えるが、裁判所の求めを考慮して運用目的の審査を行う。

第 2 に、e メールアドレスや携帯電話番号のような強い選択語の利用には、事前の内部許可を得るべきとの裁判所の判断に関しては、インテリジェンス機関は 6 編 1 章のバルク通信令状において、特定個人に対して強い選択語を適用する場合には、裁判所の判断に従う。

第 3 に、人権条約を遵守するために、バルク通信傍受において強い選択語の利用によって、ジャーナリストを特定またはジャーナリストの資料を取得・保存することになる場合には、事前の司法許可を求めるべきとの裁判所の判断に関しては、追加的な保護措置によってジャーナリストとその情報源の保護を強化する。インテリジェンス機関と調査権限コミッショナーと協議して、まもなく法律および実施規則の必要な改正を行う予定である。

4.3 調査権限コミッショナー年次報告書 2021（2023 年 3 月 20 日）

本報告書 3 章において、英国に係る人権裁判所の裁判案件が、Big Brother Watch 判決を含め 4 件記載されている。

Big Brother Watch 判決に関して、インテリジェンス機関と調査権限コミッショナーが協議している事項として、以下の項目が記載されている。

(1)人権条約違反とされたことに照らして、バルク令状の各段階における必要性と比例性および令状申請手続きを正当化するために、GCHQ の体制をどう変える必要があるか？

(2)秘匿性のあるジャーナリストの資料の検証のための選択語の利用、およびそれにより取得されたデータの保存について、事前承認を得るために、何を変える必要があるか？

(3)人権裁判所は、2 次データに対しても必要な保護措置が必要としているので、通信内容だけではなく 2 次データの規定に関しても、どの程度変える必要があるか？

4.4 IPA2016（Remedial）Order [49]2023

Big Brother Watch 判決では、RIPA2000 の規定に基づきバルク通信傍受によって取得したジャーナリストの資料とその情報源の検証と保存に関する保護措置が、人権条約 10 条に違反とされた。これに対して本命令の冒頭において、国務大臣は IPA2016 の 154 条（秘匿性のあるジャーナリストの資料に対する追加的保護措置）が人権条約と不適合であると判断して、この命令の手続きによって改正すると記載されている。

改正内容は、IPA2016 の 154 条の全面改正、および 154A 条の新設である。154 条では、バルク通信傍受によって取得された情報を検証した結果、その中に秘匿性を有するジャーナリストの資料とその情報源の情報があった場合に、速やかに検証者は調査権限コミッショナーに通知することが定められていた。

全面改正された 154 条(1)~(10)では、秘匿性を有するジャーナリストの資料とその情報源を明らかにするために検証を行う場合には、事前に調査権限コミッショナーまたは緊急時には国務大臣の代理人の承認を要することなどが規定されている。また新設の 154A 条では、154 条の国務大臣の代理人が承認する場合には、事後的に調査権限コミッショナーが関与することを規定している。

これらの改正規定は、ジャーナリストに関する保護措置を強化する内容とな

---

[49] この是正命令による改正は、1998 年人権法細則 2　パラグラフ 3 を根拠とする法改正方式である。

っている。また、これらの調査権限コミッショナーの監督権限強化に伴い、同コミッショナーの権限を定めている 229 条も改正されている。

5. 英国政府の IPA2016 の改正検討

5.1 IPA2016 改正に関する検討視点と検討事項

(1) 改正に関する英国政府の検討視点

「4」では、欧州人権裁判所の Big Brother Watch 判決に対する、IPA2016（Remedial）Order に至る英国政府の対応について述べた。

本章では、この判決に対する対応とは別の視点から、2023 年 11 月 8 日の IPA2016 (Amendment) Bill の議会提出に至る経過と法案内容について述べる。

IPA2016 の 2018 年改正は、EU 司法裁判所の DRIPA2014 違法判決や国内裁判所の IPA2016 違法判決に対応する改正であった。

これに対して今回の改正検討は、IPA2016 の成立から 6 年が経過して、その間の調査権限に関する脅威の変化や技術進歩を踏まえて、IPA2016 の規定が法目的達成にふさわしいのかとの視点（fit for purpose）から、改正検討を行ったものであり視点が異なる。

とはいうものの、IPA2016 (Amendment) Bill では、法目的達成のための調査権限強化の規定とともに、プライバシーなどの人権を尊重する視点から、調査権限行使に際しての保護措置および監督の仕組みの強化の規定が併せて盛り込まれている。

これは IPA2016 の立法趣旨が、調査権限を統一的に規定したことに加えて、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図った経過と整合的である。

(2) 内務省の「IPA2016 の運用に関する報告書」における検討事項

（2023 年 2 月）

本報告書は同法 260 条で作成が義務付けられている報告書であり、その作成目的は IPA2016 の規定が、法目的の達成にふさわしい規定になっているかを評価することである。

評価事項としては、監督、令状・許可手続き、保護措置、用語の定義、通知の有効性、BPD（バルク・パーソナル・データセット）、インターネット接続記録およびデータの証拠としての利用である。

またこの評価に当たっての運用環境の変化としては、技術、暗号、新技術、外国にあるデータ、英米データアクセス協定などが挙げられている。

この検討結果として、以下の事項が挙げられている。
1)通信データ、通信傍受、機器干渉に関する現在の権限および監督機関の統合については、IPA2016 の成立によって実現されている。
2)権限行使のための監督および保護措置の強化も実現しているようである。この強化には、監督機関の創設、調査権限に関する幅広い統計や情報収集、また（調査権限の行使に関する）重大な誤りを年次報告で公表し、その誤りに影響を受けた人への通知制度などが整備されている。
3)現在および将来の保障（future proofing）
IPA2016 は法目的達成を維持できるようにするために、意図的に技術中立的な規定にしている。しかし、BPD の規定、通信データの定義の複雑さなど評価を通して、法執行機関やインテリジェンス機関が重大犯罪と戦うことおよび国家安全保障のために必要な能力を効果的に生かすために、改革が必要であることが明らかになった。
これらの評価に基づいて、IPA2016 の改正提案を行っている。

(3) IPA2016 に対する独立報告書（David Anderson Report）（2023 年 6 月）
この報告書は、内務省報告書を補完するために、内務省が政府とは独立した立場から、以下の事項に関してアンダーソン氏に報告書を作成するように依頼したものである。
1）依頼した検討事項
BPD の仕組みは効果的か、インターネット接続記録取得の基準は良いか、いくつかの用語の定義は適切か、令状手続きおよび監督の仕組みにレジリアンスと迅速性があるか
2)内務省報告書の提案に対する本報告書の要旨
① 7 編（BPD）に、プライバシーへの期待がないか、または低い場合に取得手続きを簡素化する規定を追加する提案に賛成。
② 62 条のインターネット接続記録の利用を容易にする提案に賛成。ただ 3 条件の一部を改正するより、1 条件を追加して、インテリジェンス機関だけが国家安全保障および重大犯罪目的のために利用できるようにする方が良い。
③ 87 条に技術的変化に対応するため、国務大臣および司法コミッショナーが同意すれば、外国の SIM カードに関するインバウンド・ローミングの通信データの保存を、英国の電気通信事業者に求めてもよいとする改正提案に賛成。
④ 令状および監督手続きをよりレジリアントにするために、いくつかの用語の定義を明確する提案についてコメントしている。

⑤ 私が賛成した提案は、IPA2016 の中核的な仕組みを温存している。もし私が推奨している形で立法がなされるならば、インテリジェンス機関、法執行機関および調査権限コミッショナーオフィスに、重要な分野で有効な agility を与えることになるはずである。

⑥ この報告書は、脅威の状況の変化および技術的な発展の観点から作成されているが、これらの脅威および AI を含む技術の変化は、2030 年代に IPA を全面的に書きかえる必要が生ずるかもしれない変化である。

（4）法案検討過程における諮問結果

英国では法案検討過程で、日本のパブコメに相当する諮問を発出し、提出された意見の概要と政府側の回答を行っている。

本法案においても、通知制度改正について諮問を行い、政府側の回答を、議会への法案提出日の 2023 年 11 月 8 日に公表している。

諮問の直接の対象になっていないが、エンド・ツー・エンドの暗号について、多くの意見が提出されたようである。政府側の回答は、エンド・ツー・エンドの暗号は、調査権限機関の能力を弱化させていると述べているが、エンド・ツー・エンド暗号化は、公共安全と矛盾しない形で、サービス提供は可能であるとも述べている[50]。

この問題に対する政府の基本方針は、国民と国民のプライバシー、サイバーセキュリティと人権を守ること、および技術的イノベーションを支持するような合理的な提案を政府とテクノロジー企業の間で深めることに努めているというものである[51]。

5.2 IPA2016 (Amendment)Bill（2023 年 11 月 8 日議会提出）

5-1 の検討を経て、IPA 改正法案が議会に提出された。

本法案は、Part1 から Part5 から構成されている。主な改正内容については、IPA2016 の Part1 から Part9 の構成順ではなく、法案の構成順に従って述べる。

---

[50] 出典： “Government response to the Home Office consultation on revised notices regimes” November 8, 2023

[51] 出典： “International statement：End 2 end encryption and public safety” Home Office Guidance January 16, 2023。なお 2020 年 10 月 11 日に、当初署名国としてファイブアイズ、インドおよび日本が、「エンド・ツー・エンド暗号化および公共安全に関する国際声明」を公表していて、英国政府は英国の基本方針とこの国際声明は同趣旨の内容であるとしている。出典：“International Statement on End-to-End Encryption and Public Safety” October 11, 2020。

(1) Part1：BPD :IPA2016 Part7

Part1 における主な改正事項は、プライバシーへの期待が低いか、もしくは既に公知のデータでプライバシーへの期待がない規定を Part7A として、またインテリジェンス機関が自身以外の第三者の保持している BPD に関する規定を、Part7B として追加したことである。

「2.5(4)」に BPD 令状の主な規定を表として述べたが、同様に新たに提案されている規定についても、以下の表として述べる。

1）BPD 許可(authorisation)（7 編 7A）

許可の種類	個別(individual)許可：226B 条 類型（category）許可：226BA 条
調査権限	BPD 令状と同じ
申請権者	インテリジェンス機関
発出権者	インテリジェンス機関の長またはその代理人：226B 条、226BA 条（但し、BPD の保存などは当面国務大臣の承認）
発出根拠・理由	インテリジェンス活動に必要場合：226B 条、226BA 条
承認権者（更新・修正・取消の場合も同じ）	緊急時を除き司法コミッショナーの事前承認：226BB 条
有効期間	12 か月：226C 条 更新時 3 か月または 30 日：226CA(5)条

注：大量の公知の BPD を、バイアスを除く利用を含め機械学習を利用することで、人間の意思決定を支援できることが期待されている。

2）TPB（Third Party BPD）令状（7 編 7B）

令状の種類	検証令状
調査権限	第 3 者の保持する BPD の検証：226F 条
申請権者	インテリジェンス機関の長またはその代理人：226F 条
発出権者	国務大臣：226G 条(4)、代理人の規定はない：226GC 条
発出根拠・理由	安全保障、重大犯罪の防止または探知、国家安全保障に係る経済的利益：226G 条(4)
承認権者（更新・修正・取消の場合も同じ）	緊急時を除き司法コミッショナーの事前承認：226GA 条

有効期間	12 か月、更新時 30 日

注:一般的にはアクセスできない BPD に、電子的にアクセスできるようにする令状である。例えば、インテリジェンス機関が、政府の保有する移民関連のデータをチェックすることで、入国者に安全保障上のリスクがないことを確認できるようになる。

3) BPD 令状の有効期間を現行の 6 か月から 12 か月に延長する。
7A、7B の有効期間と同じに合わせた改正。(213 条の改正)

(2) Part2 監督の仕組み：IPA2016Part8

主な改正として、調査権限コミッショナーおよび司法コミッショナーの業務繁忙を軽減するために、以下の改正案が提案されている。

1)調査権限コミッショナーは、副調査権限コミッショナーを 2 人まで指名できる。(227 条 6A)

2)調査権限コミッショナーは、1 人またはそれ以上の臨時の司法コミッショナーを指名できる。各任期は 6 か月を超えないことおよび合計でも 3 年以内。(228A 条) 3 年以内としたのは、司法コミッショナーの任期が 3 年で再任可となっている(228 条)ので、このことを考慮して 3 年以内としたものと考えられる。

また、調査権限コミッショナーの権限に、インテリジェンス機関の国外のヒューミントなどの監視活動に対する監督権限が加えられた。(229 条の改正)

(3) Part3 通信データ関連：IPA2016Part3

主な改正事項としては、

1) 11 条（不法な通信データの取得の罪）に、合法的な通信データの取得の例を 3A として追加。

2) 62 条（インターネット接続記録に関する制限）の制限を緩和
インターネット接続記録を取得できる目的の範囲を拡大。
5A ではインテリジェンス機関と国内犯罪庁がインターネット接続記録を利用できる理由を、前者の方が後者よりも広くしている。5B では内部許可の場合を規定。

(4) Part4 通知：IPA2016Part4 および Part9

1) 国務大臣の事業者への保存通知（IPA2016 の 4 編）、Technical Capability Notice および National Security Notice（IPA2016 の 9 編）

主な改正事項としては、以下のような事項がある。

・87 条（データの保存を求める権限）に 4A を追加して、ローミング・サービ

スを保存対象として追加。
・95 条(5)に当該人物が英国外にいても、民事手続きを執行できる規定を追加。
・90 条の規定で、国務大臣が事業者に通知を行った場合に、事業者がその通知の再考を求めることができるが、その間に事業者が通知に支障が生ずるような電気通信サービスやシステムの変更を行わないことを求める規定を追加(4A)。257 条の通知でも同様の規定を追加[52]。
・通知の更新（有効期間 30 日）を繰り返した場合でも、原則 2 年間で有効期限が終了する規定を追加。（87 条）また 9 編の通知についても同様の規定を追加。（255 条 5A、5B）
・電気通信サービスを変更しようとする場合に、電気通信事業者が国務大臣に報告する義務を課す規定を新設。（258A 条）
・256 条 A 条（通知の更新）の規定を新設。
2）261 条(10)の電気通信事業者の定義を以下の事業者にも拡大。
・電気通信システムの制御または提供の一部ないし全部を英国内で行っていないが、英国内の人に電気通信サービスを提供する他の者が、利用している電子通信システムを制御または提供している事業者

これは、英国内で海外事業者の提供するサービスが拡大していることに対して、調査権限が及ぶようにするための改正。

(5) Part5 その他の改正

主な改正事項としては、以下のような事項がある。

1）議会の議員[53]に関する特定通信傍受と通信内容の検証（26 条）および特定機

---

52 この通知に支障が生ずるような変更の一つとして、エンド・ツー・エンド暗号化が想定されるので、この暗号化について多くの意見が提出されたものと考えられる。実際にこの改正によってどのような変化が生ずるかは、今後の推移を見守る必要がある。

暗号の法的規定として英国法では、IPA2016 253 条（Technical capability notice）(5)(c)に、「電子的保護の取り外し（the removal (中略) of electronic protection)」との規定がある。また RIPA2000 に 3 編「暗号などで保護されている電子データの捜査」の規定もあるが、実際の運用については把握できていない。

この暗号化については、今後も大きな議論のテーマとなると考えられる。以下の文献を参照。湯淺懇道[2017]「第 1 章 各論Ⅲ サイバー空間におけるテロ対策」大沢秀介・新井誠・横大道聡編著『変容するテロリズムと法』、湯浅懇道[2020]「第 6 章 6-1 暗号化された内容へのアクセスと法」小山剛・新井誠・横大道聡編『日常のなかの＜自由と安全＞』、小西葉子「暗号化通信の傍受に関する憲法上の課題」Nextcom Vol.42 2020 Summer

53 対象となる議員は、英国議会の上下両院、スコットランド・ウエールズ・北アイルランド

器干渉（111 条）

他の令状の場合には、国務大臣の令状発出と司法コミッショナーの事前承認が必要とされていて、これがダブルロックと呼ばれているが、議員に対する令状の場合にはこれに加えて首相の事前承認が必要とされていて、これはトリプルロックと呼ばれている。

この規定に関して、首相が何らかの理由によって事前承認できない場合で、緊急と判断される場合に、他の国務大臣が承認することができる規定を追加。

2) 令状発出を迅速化するための、緊急時には代理人が行える規定を追加。

例：BPD（7 編）202 条、219 条、220 条

6.EU 市民の個人データを米国に移転する取決め（その 1）

～セーフハーバー成立からプライバシー・シールド発効まで～

6.1 セーフハーバー成立までの経過と欧州委員会の決定文書

(1) セーフハーバー成立までの経過

1995 年に EU のデータ保護指令（以下、本項では指令）が採択され、指令の国内法化の期限が 1998 年 10 月 24 日に定められたことを契機として、データ保護指令 25 条(5)[54]の規定に基づき、EU 市民の個人データを米国への移転に関する EU-米国間の交渉が開始された。

個人データに関する米国と EU の法制度の違いもあって交渉は難航したが、移転された個人データの保護について米国の登録組織が自己認証し、FTC（Federal Trade Commission：連邦取引委員会）と運輸省が履行状況を監督するというスキームについて、欧州委員会は指令 25 条(6)に規定に基づき、米国が十分な保護レベルにあるとの認定を行った（2000 年 7 月 26 日）。

とはいうものの、「セーフハーバー協定は、EU 及び米国双方に火種を残す形で押し切られて合意である」、（米国に関する決定は）「部分的な十分性判断である[55]。」との指摘があるように、この合意は EU の最大の貿易相手国である米国との経済的つながりや政治的な考慮から、欧州委員会が行った決定であって、特

議会議員および英国選出の欧州議会議員である。

[54] 指令 25 条では、当該第 3 国が適切な保護レベルを保障していると、欧州委員会が認める場合に限り行うことができると規定されている。認められた場合には、追加的な保障を必要とせずに、加盟国から個人データを移転できる。

[55] 出典：石井、前掲注 46　p296、p477

に EU 側に不満の多く残る合意であったと考えられる。

(2) 欧州委員会のセーフハーバーに関する決定文書の構成と内容

決定文書（2000/520/EC）は、まず委員会決定の前文と 1 条から 6 条までの EU 側の決定内容と米国側が作成したⅠ～Ⅶまでの付属文書から構成されていて、量的には付属文書が約 90%を占めている。

これは、十分性認定に資するデータ保護制度および保護レベルに関する米国側の説明に対して、EU 側がその内容を審査して、十分性認定を行うとの形式を採っているためと考えられる。

1 条(1)では付属文書Ⅰの 7 項目からなるプライバシー原則[56]、同Ⅱのそのガイダンスとしての FAQ など付属文書の内容が記載されている。

また、付属文書Ⅰの第 4 パラグラフでは、a）国家安全保障、公共利益または法執行に必要な限度で、b）法律、政府規則または判例法によって相反する義務が生ずる場合には、これらのプライバシー原則は制限されると述べられている。なおこの b）については、付属文書Ⅳ B 項に詳細が述べられている。

6.2 セーフハーバー見直し交渉の契機および経過

6.2.1 セーフハーバー見直しの契機と EU 側の対応

2013 年 6 月にエドワード・スノーデンが米国 NSA（National Security Agency）の秘密文書を暴露し、NSA などの大規模なシギント活動に関して大きな反響を巻き起こした。

この NSA の活動が拡大した背景としては、2001 年 9 月 11 日の同時多発テロの発生以来、テロ対策を強化するために愛国者法の制定、FISA（Foreign Intelligence Surveillance Act：外国諜報監視法）や大統領命令 12333 号の改正など法的整備が行われたことがある。

このスノーデンの暴露を契機として、「3」と「4」で述べたように EU 司法裁判所や欧州人権裁判所などへ、いくつもの訴訟が提起されると共に、米国の個人データの保護レベルについて EU 側の懸念が高まった。

欧州委員会は 2013 年 11 月 27 日に 2 つの文書[57]を公表して、セーフハーバーのプライバシー原則などの見直し提言や、米国側との議論を行う方針を表明し、

---

[56] 7 つの原則とは、notice、choice、onward transfer、security、data integrity、access、enforcement の 7 つである。6 番目のアクセスは、政府機関のアクセスのことではなく、自己の個人データへアクセスして、訂正または削除できるとの意味である。

[57] この 2 つの COM の内容の出典：セーフハーバー無効判決、11～25 項

2014 年に入ってから EU-米国間でセーフハーバーの見直し交渉が始まった。

この 2 つの文書において、欧州委員会はセーフハーバースキームには弱点があることを認めている。

まず COM[58](2013)846final「EU-米国間のデータフローにおける信頼の再構築」では、米国政府機関は米国に移転された EU 市民の個人データにアクセスしているが、個人データが収集される（法的）根拠と米国に移転した目的とは合致しない、またより直接的に監視プログラムに関わっているように思える大多数の米国のインターネット企業が、セーフハーバースキームの下で認証されていると述べられている。

欧州委員会は、セーフハーバーには、第 1 に認証を受けた企業の中にはプライバシー原則を遵守していない企業があり、透明性、強制力、国家安全保障の例外的運用に関する構造的な欠陥を改善する必要がある、第 2 にセーフハーバーが米国へ移転された EU 市民の個人データを、米国企業が米国のインテリジェンス機関に引渡す経路（conduit）になっているとの 2 つの弱点があるとしている。このため欧州委員会は、判明したこれらの欠点を米国と協議すると結論づけている。

また、この文書に併せて米国側と共同で作成した報告書も公表された。

その報告書では、監視プログラムと米国政府による個人データの収集・取扱いに関する米国法についての詳細な分析が行われている。

もう 1 つの COM(2013)847final「EU 市民と EU で設立された企業の視点からのセーフハーバーの機能」では、以下の点が指摘されている。

① セーフハーバーへは参加は任意であるが、参加すると法的に拘束力が生ずる。

② 2013 年 9 月 26 日現在、3,246 社が認証を受けている。これらの企業は主に EU 域内でサービス、特にインターネットセクターでサービスを提供している。

③ 米国に移転されたデータが、国家安全保障を守るための必要性と比例性を超えて、米国のインテリジェンス機関によって、アクセス・取扱われている。

④ 米国法において米国市民と米国在住者に認められている保護措置が、EU のデータ主体には認められておらず、また行政的・司法的な救済を求め

---

[58] COM というのは、欧州委員会の政策文書として、欧州議会および閣僚理事会へ送付される文書である。COM（2013）846final の正式名称は、Policy Document ; COM (2013) 846final; COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

る機会がない。

⑤ セーフハーバーによって米国に移転されたデータへの米国のインテリジェンス機関による大規模なアクセスは、ヨーロッパ人のデータ保護の権利と自由に関する重大な問題を提起している。

6.2.2 米国側の対応

一方米国では、スノーデンの暴露から 2 か月後の 2013 年 8 月に、サイバーセキュリティの専門家であるリチャード・クラークや憲法学者のキャス・サンスティーンなど 5 人からなる検討グループを立ち上げた。この検討グループが同年 12 月に公表した報告書[59]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結論付けて、46 の提言を行っている。

この提言を受けて、2014 年 1 月にオバマ大統領は PPD（President Policy Directive：大統領政策指令）28 号を発出した。また 2015 年 6 月には米国自由法（USA Freedom Act of 2015）が成立し施行された[60]。

これらの内容が、セーフハーバーに代えて合意されたプライバシー・シールドの内容に反映されている。

この見直し交渉が行われていた最中の 2015 年 10 月に、EU 司法裁判所がセーフハーバー無効判決(Schrems Ⅰ)を下したことで、見直し交渉が加速される状況になった。

6.3 EU 司法裁判所のセーフハーバー無効判決(Schrems Ⅰ)(2015 年 10 月 6 日)

(Case C-362/14)

6.3.1 付託事項、関係法条文、争点および付託された質問

(1)先決判決付託事項

基本権憲章 7 条、8 条および 47 条の規定に照らして、データ保護指令（95/46/EC）25 条(6)および 28 条の解釈を求めるもので、米国商務省によるセ

---

[59] 報告書 “Liberty and Security In a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies” December 2013

[60] 出典：鈴木滋「米国自由法：米国における通信監視活動と人権への配慮」外国の立法、267（2016.3）p8。以下も参照：林紘一郎・田川義博[2016]「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、情報セキュリティ大学院大学、pp15-18

ーフハーバー・プライバシー原則および関連する FAQ に規定されている、保護の十分性に関する欧州委員会決定（2000/520/EC）の適合性（validity）を問うものである。

(2)関係法条文

・データ保護指令：前文(2)、(10)、(56)、(57)、(60)、(62)、(63)、1 条、2 条、25 条、26 条、28 条、31 条

・Decision 2000/520 (セーフハーバー決定)：前文(2)、(5)、(8)、1 条～4 条、付属文書Ⅰ、Ⅱ、Ⅳ

・COM(2013)846final、COM(2013)847final

(3) 先決判決付託に至る原審での争点

Facebook を利用しようとする EU 居住者は、利用者の個人データの一部または全部を米国の Facebook のサーバーに移転して、そこで取扱うとの契約を Facebook Ireland と結ぶことを求められる。

2013 年 6 月 25 日にシュレムス氏は、米国では十分な個人データ保護の水準にないことを理由として、アイルランドのデータ保護コミッショナーに対して、彼の個人データの米国移転への禁止を Facebook Ireland に命ずるように求める訴えを起こした。シュレムス氏は、スノーデンの米国インテリジェンス機関、特に NSA の活動に関する暴露にも言及している。

これに対して、同コミッショナーは、米国のデータ保護の十分性の問題は、欧州委員会の 2000/520 決定に従って判断されるべきで、欧州委員会は米国では十分な保護水準にあると認定していること、およびシュレムス氏の個人データが NSA にアクセスされている証拠はないことを理由として、シュレムス氏の訴えを却下した。

これに対して、シュレムス氏は同国の地方裁判所に訴えを提起した。同裁判所は、EU から米国に移転された個人データに対する電子監視は、公益上必要で不可欠な目的に資するものであると認定した。一方でスノーデンの暴露は、NSA などの活動は相当な行過ぎ（significant over-reach）であることを示しているとも述べている。

同裁判所は、審理を停止して、先決判決を求めて、EU 司法裁判所に以下の質問を付託することを決定した。すなわち、欧州委員会の決定に対して、国内のデータ保護コミッショナーはその決定に拘束されるか、また欧州委員会決定が公表されて以降の事実の展開に照らして、データ保護コミッショナーは自ら調査を行わなければならないかとの質問である。

6.3.2 付託質問、審理および判決

(1)付託質問および審理

付託裁判所の質問は、データ保護指令（本項では以下指令）25 条(6)は、基本権憲章 7 条、8 条および 47 条の規定に照らして、第 3 国が十分な保護レベルを保証していると認定した欧州委員会決定が、加盟国の監督機関が同指令 28 条の権限内で、第 3 国に移転された個人データに対して、第 3 国の法律と慣行が十分な保護水準を保障していないと本人が訴える場合に、データ保護コミッショナーがその訴えを検証することを妨げていると解すべきかとの質問である。

1)指令 25 条(6)に基づき欧州委員会が決定を行った場合の指令 28 条の規定による国内監督機関の権限

欧州委員会の決定は、加盟国の監督機関が指令 28 条の権限内において、個人データに関する権利を侵害されたとの訴えを検証することを妨げない。

但し国内裁判所には EU 法の有効性を判断する権限はなく、EU 司法裁判所のみが EU 法の無効宣言をする権限を有する。

また国内の監督機関が訴えを却下した場合には、基本権憲章 47 条の規定に照らして解釈すると、救済を求めて国内裁判所に訴えを提起することができる。

2)Decision2000/520（セーフハーバー決定）1 条の適合性（79～98 項）

セーフハーバー・プライバシー原則は、自己認証企業のみに適用され、公的機関にはこの原則の順守義務はない。(82 項)

付属文書 I には、国家安全保障などのために、セーフハーバー・プライバシー原則の適用が制限されることが明記されている。また FTC と運輸省の監督も企業に対して及ぶだけである。

COM(2013)846final と COM(2013)final でも、現行のセーフハーバーの欠陥が述べられているように、国家安全保障を守るために厳密な必要性と比例性を超えて、米国政府の機関が米国に移転された個人データにアクセスすることが認められている。またデータ主体には、行政的・司法的な救済手段がない。

EU 内で保障されている基本的権利と自由の保護の水準に関しては、EU 法においては（干渉の）手段の範囲と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。保護措置によって、濫用のリスク防止およびデータへの違法アクセス・利用に対して、効果的な保護ができるようにしなければならない。

公的機関に一般的な基準で電子通信内容にアクセスすることを認める法律は、基本権憲章 7 条で保障されている私的生活の尊重の権利を損なうものと見做されなければならない。

また法的救済を規定していない法律は、基本権憲章 47 条を尊重していない。

欧州委員会は、第 3 国は国内法または国際的コミットメントによって、EU 法秩序において保障されている水準と本質的に同等（essentially equivalent）の保護水準を保障していることを、認定しなければならない。しかし、欧州委員会はこの決定においてこれについて述べていない。

従って、セーフハーバー・プライバシー原則の内容を検証するまでもなく、セーフハーバー決定 1 条は、指令 25 条(6)の規定を遵守しておらず、それ故に無効である。

3）Decision2000/520 3 条の適合性（99～106 項）

基本権憲章 8 条の規定に照らして、指令 28 条の下で、国の監督機関は、当人に係る個人データの取扱いに関する権利と自由の保護に関するいかなる訴えも、完全な独立性をもって検証できなくてはならない。

とりわけその訴えで、指令 25 条(6)に基づく欧州委員会決定の適合性に関する問題を提起する場合には一層妥当する。

しかし 3 条(1)の第 1 パラグラフは、この権限を否認していると解されなければならない。EU 法で欧州委員会には、国の監督機関の権限の制限する権限はなく、欧州委員会は 25 条(6)で与えられた権限を越えていて、それ故無効である。

1 条および 3 条は、2 条、4 条および付属文書から不可分であり、それが無効であることは決定全体の適合性に影響が及ぶ。

以上の理由から、セーフハーバー決定は無効である。

(2)判決

1)指令 25 条(6)は、基本権憲章 7 条、 8 条および 47 条の規定に照らして、欧州委員会は第 3 国が十分な保護水準を保証していると認定するセーフハーバーのような決定は、指令 28 条の範囲内で加盟国の監督機関が、加盟国から第 3 国に移転された個人データの保護に関して、第 3 国の法と運用が十分な保護水準を保障していないと主張する場合に、当該者の権利や自由の保護に関する訴えを、検証することを妨げていると解しなければならない。

2)セーフハーバー決定（Decision 2000/520）は無効である[61]。

6.3.3 本判決の論点

1-2 で取上げたデータ保存指令無効判決は、基本権憲章の規定に照らして、指令そのものが無効との裁定であった。これに対して、本無効判決はデータ保護

[61] 判決内容は(2)判決に述べられたことに加えて、審理の項で扱われているセーフハーバー 1 条および 3 条の適合性も判決内容であると考えられる。

指令の規定を基本権憲章の規定に照らして解釈すると、欧州委員会のセーフハーバー決定は、同指令違反であり無効としたものである。

無効の理由としては、大別すると次の 3 つの理由があると考えられる。第 1 に、EU 委員会の 2 つの COM 文書において、欧州委員会自身が認めているように、十分性認定に関する調査・審査に欠陥があった。第 2 に、セーフハーバー ・プライバシー原則にコミットメントを表明した自己認証企業のなかには、同原則を遵守していない企業があり、遵守状況を監視する FTC と運輸省の監督も不十分であった。第 3 に、米国のインテリジェンス機関がセーフハーバーの適用外であることに加えて、国家安全保障目的にとって必要かつ比例的である限度を超えて、大規模なアクセスと利用が行われている。また権利侵害されたとする個人に対する救済制度が EU 市民にはない。

これらの理由によって、米国の個人データ保護の水準が、EU 法の個人データの保護水準と本質的に同等ではないと判断されたものと考えられる。

6.4 セーフハーバー無効判決後の見直し交渉と欧州委員会のプライバシー・シールド実施決定

6.4.1 EU-米国間の見直し交渉

この第 3 の理由の米国のインテリジェンス機関による、米国に移転された EU 市民への大規模なアクセスと利用については、バルク・データの問題として、EU-米国間での交渉の焦点となっていた。

米国側の見直し交渉に対する対応としては、前述した PPD28 号や米国自由法 2015 において、バルク・データ収集について制限する方向で見直しが行われた。

主な見直し事項としては、第 1 に特定データ収集を原則として、バルク・データ収集を例外とするかまたは止める。第 2 に外国諜報のためのシギント活動では、識別子(discriminants)を利用して、収集対象データを限定する。第 3 にバルク収集を行う場合でも、その利用は 6 項目[62]の安全保障目的に限定する。

また 2016 年 2 月には、司法救済法[63]（Judiciary Redress Act of 2015）が成立した。この法律の適用対象に EU が指定されたことで、EU 市民が個人データ

---

[62] 6 項目の安全保障目的とは、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、である。

[63] この法律の 2 条では、1974 年プライバシー法の適用範囲を拡大して、司法長官が指定する国や地域の市民（covered person）は、訴訟提起に関しては米国市民と同じ権利を有することを規定している。

の不法な開示に対して、米国プライバシー法の規定に基づいて米国政府を訴えることができるようになった。

これらの米国側の対応に対して、欧州委員会は 2016 年 2 月 29 日に草案を公表した。その後 EU 内部の調整を経て、2016 年 7 月 12 日に欧州委員会はプライバシー・シールドの実施決定を行った。

6.4.2 欧州委員会の実施決定文書の構成

本文の構成は、「1.はじめに」では交渉経過、「2.プライバシー・シールド」では概要、「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的機関によるアクセスと利用」となっている。このうち「3」がその全体の半分を占めていて、セーフハーバー見直し交渉の焦点が、ガバメント・アクセスであることを如実に示していると考えられる。

この「3」では、第 1 に米国の公的機関による国家安全保障目的で行うアクセスと利用の制限に関しては、主としてバルク・データ収集に関する PPD28 号と米国自由法および FISA の規定について、また公的機関のアクセスと利用に関する効果的な保護のための監督の仕組み[64]が述べられている。第 2 に米国の公的機関による法執行および公益目的でのアクセスについて述べられている。

この他の項目としては、プライバシー・シールドの下での十分な保護水準、(加盟国の) データ保護機関の行動と欧州委員会への情報提供、十分性認定に関する定期的なレビュー、十分性決定の破棄についても述べられていて、EU 司法裁判所のセーフハーバー無効判決で指摘された内容が盛り込まれている。

付属文書として、米国政府作成の文書が添付されている。この中には、公的機関の適正執行を確保するためにオンブズパーソンの創設、およびオンブズパーソンが行うシギント活動に関する（監督の）仕組みについて述べられている（付属文書Ⅲ)。

また米国のインテリジェンス機関を統括している国家情報長官室（ODNI: Office of the Director of National Intelligence）から、プライバシー・シールドの米国側の代表である商務長官などへの手紙が添付されている（付属文書Ⅵ)。この中には、過去 2 年半に及ぶ EU-米国間の交渉において、プライバシー・シールド原則の例外として国家安全保障のために、米国のインテリジェンス機関が行うシギント情報収集活動に関して説明を行ってきたとして、改めて PPD28 号、FISA702 条、米国自由法、透明性、救済措置について詳細に述べている。

---

[64] 行政部門、議会および FISC（FISCR）の監督の仕組み

6.4.3 セーフハーバーとの比較

セーフハーバー決定文書では、EU 側作成の本文と米国側作成の付属文書から構成されているが、付属文書が全体の 90%の分量を占めているのに対して、プライバシー・シールド実施決定では、本文における米国側の説明に基づく欧州委員会の十分性認定のための審査の記述が、かなり詳しく述べられている。

プライバシー・シールドでは、EU 司法裁判所のセーフハーバー無効判決内容を反映し、米国の公的機関による EU 市民の個人データへのアクセスと利用について、米国側の見直し内容が盛り込まれている。

一方でセーフハーバーと同様に、米国企業による自己認証制度および FTC と運輸省が監督する仕組みは維持している。

またプライバシー・シールド原則[65]としては、7 項目が記載されている。

7. EU 市民の個人データを米国に移転する取決め（その２）

～プライバシー・シールド無効判決からデータ・プライバシー・フレームワーク発効まで～

6.3 で取上げたセーフハーバー無効判決は、2013 年 6 月のスノーデンの暴露を契機として始まった、EU-米国間でセーフハーバー見直し交渉の最中の 2015 年 10 月 6 日に下されたもので、これによって見直し交渉が加速されたものと考えられる。

これに対して、2020 年 7 月 16 日の EU 司法裁判所のプライバシー・シールド無効判決を契機として、EU-米国間での交渉が始まり、データ・プライバシー・フレームワークが発効したもので、同判決がなければデータ・プライバシー・フレームワークは存在しなかったと考えられる。

「7」では、EU 司法裁判所のプライバシー・シールド無効判決から、EU-米国間の交渉における米国側の対応、それを基礎とした 2023 年 7 月 10 日の欧州委員会のデータ・プライバシー・フレームワークの実施決定内容に加えて、欧州員会の新 SCC および対英国への決定について述べる。

7.1 EU 司法裁判所のプライバシー・シールド無効判決（Schrems Ⅱ）

---

[65] プライバシー原則は、以下の 7 項目である。notice、choice、accountability for onward transfer、security、data integrity and purpose limitation、access・recourse,・enforcement and liability

（2020 年 7 月 16 日 Case C-311/18）

7.1.1 先決判決付託事項、関係法条文および争点

(1)先決判決付託事項

・EU 条約 4 条(2)および基本権憲章 7 条、8 条並びに 47 条の規定に照らした、データ保護指令（Directive 95/46/EC）の 3 条(2)、25 条、26 条および 28 条（3）の解釈
・欧州委員会 SCC 決定の解釈および適合性
・欧州委員会のプライバシー・シールド決定の解釈および適合性

(2)関係法条文

・データ保護指令：3 条、25 条、26 条(2)(4)および 28 条(3)
・GDPR：前文 10 カ所、2 条(1)(2)、4 条、23 条、Ⅴ章（44 条～50 条）、51 条(1)、55 条(1)、57 条(1)、58 条(2)(4)、64 条、65 条(1)、77 条、78 条、94 条、99 条
・SCC 決定：前文 11、1 条、3 条、 4 条、付属文書
・プライバシー・シールド決定：前文[66]13 カ所、1 条、付属文書Ⅱ、Ⅲ、Ⅵ

---

[66] 本決定の前文では規定内容に加えて、以下のようなコメントも述べられている。まず米国のインテリジェンス機関に関する法令として、大統領令 12333 号、PPD28 号に言及されている。PPD28 号ではシギント活動に関して多くの制限が規定されていて、EU 市民のような非米国人にとって重要であり、その用語は使われてはいないものの、PPD28 号の原則は必要性と比例性の原則の本質を捉えている。

一方、FISA702 条では、プリズムやアップストリームプログラムのような監視プログラムを、FISC（Foreign Intelligence Surveillance Court:外国諜報監視裁判所）は個々の監視手段を許可するのではなく、年間で認証している。また FISC の認証には特定の人物に関する情報は含まれておらず、類型的な認証を行っている。

FISA は非米国人へも多くの救済策を規定している。但し、大統領令 12333 号に基づくインテリジェンス機関の行為には適用されないし、救済策がある場合でも利用できる訴因は限定されている。

付属文書Ⅲにおいて新たに創出したオンブズパーソンの仕組みは、PPD28 号で指名された国務省上級調整官で、米国のシギント活動に関して外国政府が懸念を伝える連絡者である。これらの審査結果から、欧州委員会は米国が十分な保護水準を保障していると認定している。

また欧州委員会は、米国の公的機関による同国に個人データを移転された者の基本権への干渉は、正当な目的達成のために厳に必要な限度に制限されており、およびこのような干

(3)付託裁判所（原審）における争点

2015 年 10 月 6 日の EU 司法裁判所のセーフハーバー無効判決後に、付託裁判所はデータ保護コミッショナーに決定を差し戻した。コミッショナーの審理において、Facebook Ireland は SCC（Standard Contractual Clauses）決定の付属文書に定められている標準データ保護条項に従って、大部分の個人データを米国の Facebook に移転していると説明した。このために、コミッショナーはシュレムス氏に訴えを再構成するように依頼した。

2015 年 12 月 1 日の再構成した訴えにおいて、シュレムス氏は SCC 決定によって個人データを米国に移転することを正当化することはできないので、自分の個人データを Facebook への移転を禁止するか中断するようにコミッショナーに求めた。

2016 年 5 月 24 日に、コミッショナーは暫定的な認定をまとめた決定草案を示した。この中で EU 市民の個人データが、基本権憲章 7 条および 8 条と不適合な（incompatible）方法で、米国の機関によって取扱われている可能性があり、米国法は基本権憲章 47 条に沿った法的救済を規定していないとの暫定的な見解を示した。

SCC が定める標準データ保護条項は、米国の機関を拘束するものではないので、これらの欠陥を是正することができないとコミッショナーは認定した。

2016 年 5 月 31 日に、コミッショナーは裁判所に訴えを提起した。

付託裁判所は、米国政府が参加した国内審理における証拠の検証を行った 2017 年 10 月 3 日の判決のコピーを付属文書として添付して、2018 年 5 月 4 日に、EU 司法裁判所へ先決判決を付託した。

付託裁判所の審理では、FISA702 条と大統領令 12333 号の規定内容および実際の運用状況についても説明が行われた。

付託裁判所は、米国は個人データの大量処理を行っているが、基本権憲章 7 条および 8 条による保障と本質的に同等の保護水準を保障していないと判断した。

また米国憲法修正 4 条は EU 市民に適用されないので、EU 市民は米国市民と同じ司法的救済を受けられないと述べている。

さらに大統領令 12333 号に基づく NSA の活動には司法的な監督が及ばない、またオンブズパーソンは基本権憲章 47 条の意味での裁判所（tribunal）ではないとも判断している。

欧州委員会のプライバシー・シールド決定のような第 3 国が保障する保護水

渉に対する効果的な法的保護があると認定している。

準の十分性認定は、SCC 決定における標準データ保護条項に従った個人データの移転についても、監督機関を拘束するとも裁判所は述べている。

以上の審理から付託裁判所は、SCC 決定の適合性について質問している。

本判決では以上の付託裁判所の争点を述べた後に、付託裁判所が先決判決を求めて、EU 司法裁判所に行った 11 の質問を記載しているが、これらの質問に対して 6 つにまとめて審理されているので、本稿ではこれに対応して質問と審理を分析する。

7.1.2 審理および判決

(1)本付託に関する容認性

質問に対する審理に先立って、EU 司法裁判所は、Facebook Ireland およびドイツ・英国両政府の先決判決の付託は認められない、との主張に対する審理を行っている。

Facebook Ireland は、質問の基礎となっているデータ保護指令は、GDPR によって廃止されたと主張している。この点に関しては、データ保護指令は 2018 年 5 月 25 日に廃止されたものの、EU 司法裁判所が付託を受けた 2018 年 5 月 9 日には、効力を有していた。

ドイツ政府は、コミッショナーは SCC 決定の有効性に疑問を表明しただけで、明確な意見を表明したわけではないことなどを、反対の根拠にしている。また英国政府は、付託裁判所はデータが実際に移転されたとの認定を行っていないので、仮定の質問であると主張している。

これらの主張に対して EU 司法裁判所は国内裁判所の質問は、妥当性の推定を受けるのが判例法であるとしている。

このため、EU 法の解釈や適合性に関する付託質問に対しては、EU 司法裁判所は原則として判決しなければならない。EU 司法裁判所が拒否できるのは、その解釈が訴訟対象の事実とは関連性がない場合、仮定の問題である場合、有用な回答をするために必要な事実または法的な資料を有していない場合に限られる。

本訴訟では、十分な事実および法的な資料があり、事実と関連がないとか、仮定の問題であるということではない。

Facebook Ireland はデータ移転を認めていて、これらの移転は SCC 決定の標準データ保護条項に従って行われている。またコミッショナーが SCC 決定の適合性について明確な意見を表明しなかったとの主張も、先決判決を求める付託の容認性に関して適切な主張ではない。

従って、先決判決の付託は容認される。

(2)付託質問についての審理

データ保護指令が GDPR によって廃止されたときには、コミッショナーがまだ最終決定を行っていない時であった。それ故に、付託質問に対してはデータ保存指令ではなく、GDPR の規定によって回答しなければならない。

＜第 1 質問＞

付託裁判所の質問は、EU 条約 4 条(2)との関連において、GDPR2 条(1)および 2 条(a)(b)(d)は、公共の安全、防衛および国の安全の目的で、当該第 3 国の機関によって処理される可能性がある場合に、加盟国の事業者(economic operator)から第 3 国の事業者へ個人データの移転に適用されると解釈されなければならないのか、ということである。

EU 条約 4 条(2)の国家安全保障は、各加盟国のみの責任であるとの規定について最初に明確にしなければならない。この規定は、GDPR の規定を解釈するためには適切ではない。

GDPR2 条などの規定を考えると、公共の安全、防衛および国の安全の目的で当該第 3 国の機関が取り扱う可能性があるからといって、加盟国から第 3 国への個人データの移転を、GDPR の適用外とすることはできない。（80~89 項）

＜第 2、第 3 および第 6 質問＞

これらの質問は、GDPR46 条の規定で求められる保護水準を明確にすることを求める質問である。具体的には、SCC に基づく第 3 国への個人データの移転に関して考慮すべきファクター、十分な保護措置を提供し、執行力のある（enforceable）データ主体の権利なり効果的な救済策の質問である。

これらの質問に対する回答として、① GDPR46 条(1)と(2)(c)は、適切な保護措置、執行力のある権利および有効な法的救済に関して、EU 法と本質的に同等の保護水準を保障しなければならない、と解さなければならない。② 保護水準の評価に当たっては、当事者間の契約条項と、当該第 3 国の公的機関による個人データへのアクセスに関する法的システムの両方を考慮しなければならない。（90~105 項）

＜第 8 質問＞

付託裁判所は、GDPR58 条(2)(f)(j)は、標準データ保護条項(standard data protection clauses)に従った第 3 国への個人データの移転について、権限ある監督機関がデータ保護が保障されていないと判断した場合に、中断または禁止することを求められると、解さなければならないかを問うものである。

EU 司法裁判所は GDPR の法解釈を行って、以下の裁定を下している。

GDPR58 条(2)(f)(j)は、欧州委員会の十分性認定がなく、標準データ保護条項

を当該第 3 国が遵守できない場合、および当事者自身が移転を中断または終了せず、他の手段ではデータの保護ができない場合には、権限ある監督機関はデータの移転の中断または禁止が、求められると解さなければならない。（106~121 項）

＜第 7 および第 11 質問＞

付託裁判所は、基本権憲章 7 条、8 条および 47 条の規定に照らして、SCC 決定の適合性を明確にするよう求めている。

標準データ保護条項が第 3 国の監督機関を拘束していないならば、SCC 決定が第 3 国に移転された個人データの十分な保護水準を保障することができるのかと、付託裁判所は問いかけている。

この問いに関して EU 司法裁判所は、以下のような詳細な審理を行っている。

＊標準データ保護条項は、EU 側の管理者および第 3 国の受取人を拘束するが、第 3 国の公的機関は契約当事者ではないので、拘束できない。

＊第 3 国の公的機関に対して拘束力がないとすると、標準データ保護条項が無効ではないかとの疑問が生ずる。

＊第 3 国の立法が十分な保護水準を保障している場合にのみ、欧州委員会は GDPR45 条(3)に基づく十分性認定を行うことができる。

＊これに対して、欧州委員会が SCC 決定のような標準データ保護条項を採択する場合には、欧州委員会が採択前に十分な保護水準を評価するように求められているとは、GDPR46 条(1)、(2)(c)からは推測できない。

＊この点については、EU 側の管理者または取扱者が、十分な保護措置を講ずることに留意しなければならない。

＊標準データ保護条項は、その性格上契約上の義務を超えて保障することを規定することができないが、EU 法が求める保護水準を遵守するために、管理者は追加的な措置を採ることを求められることがある[67]。

＊EU 側の管理者または取扱者が追加的な措置を講ずることができない場合で、管理者または取扱者が中断または終了できない場合には、権限のある監督機関は第 3 国への個人データの移転の中断または終了することが求められる。

第 3 国の法律が、EU からの個人データの受取人に、公的機関によるアクセ

---

[67] 欧州データ保護会議が公表したプライバシー・シールド無効判決に関する Q＆A では、SCC の有効性はケース・バイ・ケースの判断に基づいて、追加的保護措置を講ずることで、米国法が SCC の保障する十分なレベルな保護を損なうことを防止できるか否かにあると述べている。

スに対する契約上の十分な保護水準の保障と相反する義務を課している場合に、特に当てはまる。

以上の審理から、標準データ保護条項が第 3 国の公的機関を拘束しないとの事実だけでは、SCC 決定の有効性には影響しない。

＊その有効性は、EU 法で求める保護水準の遵守を保障することを可能にする、および条項違反の場合には個人データの移転を中断するか禁止する効果的なメカニズムがあるか否かによる。

＊加えて、第 3 国の個人データの受取人は、条項 5 条に従って、契約義務の遵守ができないような事由が発生した場合には、EU 側の管理者に通知し、また管理者はデータの移転を中断するか終了する義務がある。

＊国家安全保障、防衛および公共の安全を守るために、必要な限度を超えない強行規定は、標準データ保護条項とは矛盾しない。反対に、必要な限度を超える義務付けは、これらの条項の侵害として扱われなければならない。

＊第 3 国の立法が標準データ保護条項の遵守を認めない場合には、第 3 国の個人データの受取人は、既に第 3 国に移転されたデータの全部を返還または破棄しなければならないし、該当する個人は被害の補償を受ける権利がある。

＊第 3 国の立法が標準データ保護条項にマイナスの影響ありそうなことを、受取人が EU 側の管理者に通知した場合で、EU 側の管理者が移転継続を決定する場合には、監督機関に通知することを求められる。十分な保護水準を保障するために、通知を受けた監督機関は、移転の中断または禁止すべきかを見定めることができる。

＊SCC 決定 4 条の規定により SCC 決定があっても、監督機関が標準データ保護条項に従った第 3 国への個人データの移転を、中断または禁止することは妨げられない。

＊GDPR58 条(2)(f)(j)の規定によって、標準データ保護条項が第 3 国で遵守されず、移転されたデータの保護を他の方法では保障できない場合には、監督機関は移転を中断または禁止することを求められる。

＊以上の審理から、第 7 および第 11 質問に対する回答は次の通り。基本権憲章 7 条、8 条および 47 条に照らした SCC 決定の検証では、同決定の有効性に影響することは、何も明らかにならなかった。（122～149 項）

＜第 4、第 5、第 9 および第 10 質問＞

付託裁判所は、米国が十分な保護水準を保障しているとのプライバシー・シールドにおける十分性認定が、どの程度加盟国の監督機関に拘束力を有するかを知りたいと願っている。

また米国法についての認定から見て、標準データ保護条項に従った個人デー

タの移転が、基本権憲章 7 条、8 条および 47 条に規定された権利侵害に当たるか、およびオンブスパーソンの導入は基本権憲章 47 条に適合的かと質問している。

EU 司法裁判所は、基本権憲章の規定、プライバシー・シールドの内容および監督機関への拘束性の解釈を通して、以下の判断をしている。

プライバシー・シールドの拘束性については、EU 司法裁判所が同決定の無効を宣言しない限り、（加盟国の）監督機関は個人データの移転の中断または禁止をすることができない。

一方十分性認定の適合性を争う訴えがある場合に、監督機関は訴えに対して完全な独立性の下で、十分な根拠があると考えるならば、EU 司法裁判所に同決定の適合性に関する先決判決を求めるために、国内裁判所に訴えを移送しなければならない。

付託裁判所に回答するためにはプライバシー・シールド決定が、GDPR と基本権憲章の要件を遵守しているかを検証しなければならない。

＜プライバシー・シールド決定＞

EU 司法裁判所は、プライバシー・シールド決定における米国の保護水準の認定に関して、米国のインテリジェンス機関の権限行使に関する FISA702 条、大統領令 12333 号および PPD28 号の規定を調査している。その中で、シギント機関が特定の対象への選択語を利用できない場合には、大規模なバルク・データ収集を認めていることを指摘している。

同決定では以下の認定を行っている。①米国は十分な保護水準を保障している。②プライバシー・シールド原則は、国家安全保障などで必要な場合には制限される。③米国の公的機関による干渉は、厳密に必要なものに限定されていること、およびそのような干渉に対して効果的な法的保護もある。

この認定に対して、EU 司法裁判所は、以下の詳細な審理を行っている。

1)付託裁判所は、米国が十分な保護水準を保障している、との同決定の認定に疑問を持っている。(168 項)

2)公的な機関など第３者に個人データを渡すことは、基本権憲章の７条および８条に規定されている基本権への干渉である。また個人データの保存および公的機関によるデータへのアクセスも同様である。（171 項）

3)しかし基本権憲章７条および８条の権利は絶対的な権利ではなく、社会において果たしている機能との関連で考察されなければならない。（172 項）

4）基本権憲章８条(2)は、個人データは特定の目的、および関係する個人の同意または他の法的な根拠の下で、取扱われなければならないと規定している。(173 項)

5)基本権憲章 52 条によると、基本権を制限するには、法的根拠があることおよび基本権の本質の尊重が求められる。また比例性原則に従い、必要であり EU で認められている一般的利益に真に合致する場合のみ、基本権を制限することができる。（174 項）
6)干渉を認める EU の立法には、範囲と適用に関する明確で詳細な規定が必要である。また濫用のリスクを防止するために、個人データに対して効果的な最小限の保護措置を講ずることで、干渉が真に必要な限度に制限されるようにしなければならない。（176 項）
7)GDPR45 条(2)(a)は、第 3 国における十分な保護水準を評価する場合には、効果的で執行可能なデータ主体の権利を特に考慮すると規定している。（177 項）
8）欧州委員会の実施決定については、特に FISA702 条、大統領令 12333 号を根拠とする監視プログラムによる干渉が、比例性原則に従って、基本権憲章 52 条(1)と本質的に同等な保護水準になっているかが問われている。

このためそれらの監視プログラムがこの保障に従っているか、および当該第 3 国が本質的に同等な保護水準を遵守しているかを検証する必要がある。(178 項)
9）欧州委員会の認定では、FISC（Foreign Intelligence Surveillance Court:外国諜報監視裁判所）は個々の監視方法を許可するのではなく、プリズムやアップストリームのような監視プログラムを年次認証（annual certifications）している。

FISC はそれらの監視プログラムが、外国諜報監視目的に関連しているかを検証する役割であって、対象とされる個々人が適切かは審査対象となっていない。（179 項）
10)FISA702 条で明らかなのは、外国向けのインテリジェンスの監視プログラムの実施権限に制約がなく、またそのプログラムで監視対象となる可能性のある非米国人へ保障は存在していない。

従って 702 条は基本権憲章と本質的に同等の保護水準を保障できていない。比例性の原則要件を満たすためには、詳細なルールおよび最小限の制限の範囲を確定し、明確な保護措置を定めなければならない。（180 項）
11)監視プログラムは PPD28 号の要件に従っていて、その要件は法的拘束力があるものの、PPD28 号はデータ主体に裁判所に訴える権利を認めていない。

従って十分性認定では、データ主体が効果的で執行可能な権利を有しているかが問われるが、プライバシー・シールド決定では、GDPR45 条(2)の要件に反して、本質的に同等の保護水準を保障することができない。（181 項）
11)PPD28 号は、インテリジェンス機関が特定の対象と紐づける識別子を利用することができない場合に、大規模なシギント情報またはデータのバルク収集を認めている。（183 項）

12)従って FISA702 条または大統領令 12333 号は、PPD28 号と併せて解釈すると、それらは最小限の保護措置を講じておらず、結果としてこれらの規定に基づく監視プログラムは厳密に必要なものに制限されているとは言えない。(184 項)
13)基本権憲章 47 条は、権利と自由を侵害された人には、裁判所に効果的な救済を求める権利があることを規定している。(186 項)
効果的な司法審査があることは、法の支配に不可欠のものである。自身の個人データにアクセスし、そのデータの訂正や消去を求める法的救済策のない立法は、基本権憲章 47 条に規定されている効果的な司法的保護に関する基本権を尊重していないことになる。(187 項)
14)GDPR45 条(2)(a)は、第 3 国における十分な保護水準を評価するに当たり、特に効果的な行政的および司法的救済を考慮することを求めている。(188 項)
15)オンブズパーソンの導入によっては、欧州委員会自身が司法的保護に関して認定した欠陥を是正することはできないので、米国が基本権憲章 47 条と本質的に同等の保護水準を保障しているとの欧州委員会の認定が問題視されている。(190 項)
16) オンブズパーソンの仕組みは、データ主体が独立した公平な裁判所で、自身の個人データにアクセスし、そのデータの訂正や消去を求める法的訴えを提起できる可能性から検討を始めなければならない。(194 項)
17)オンブズパーソンは、国務長官によって任命され、国務省に組込まれていて、身分保障はないので、オンブズパーソンの独立性は損なわれている。(195 項)
18)オンブズパーソンにはインテリジェンス機関に対して、拘束力のある決定を行う権限がない。(196 項)
19) 欧州委員会は、米国が十分な個人データ保護水準にあるとの十分性認定において、GDPR45 条(1)の要件を無視している。(198 項)
20) プライバシー・シールド決定 1 条は、GDPR45 条(1)に適合的ではなく(incompatible)、それ故無効である。(199 項)
21) 同実施決定 1 条は、2 条、6 条および付属文書と不可分であるので、その無効は決定の適合性全体に及ぶ。(200 条)
22) 以上を考慮すると、プライバシー・シールド決定は、無効であるとの結論になる。(201 項)
23)法的な空白を避けるために同実施決定の効果を維持することが適切であるとの主張に関しては、十分性認定が無効になったとしても、そのような空白を生ずることにはならない。(202 項)

(3)判決
1) GDPR2 条(1)(2)は、データが移転時または移転後に、公共の安全・防衛およ

び国家の安全の目的で、第 3 国の機関によって取扱われるか否かに関わらず、加盟国の事業者から第 3 国の事業者へ、商業目的での個人データの移転に適用されると解釈しなければならない。
2)GDPR46 条(1)(2)は、適切な保護措置、執行可能な権利および効果的な法的救済に関して、標準データ保護条項に従って第 3 国に移転された個人データのデータ主体には、EU 法と本質的に同等な保護水準を与えなければならないと解さなければならない。
保護水準の評価に当たって考慮しなければならないのは、GDPR45 条(2)の規定によれば、当事者間の契約条項および第 3 国の公的機関による（個人データへの）アクセスに関する法的システムの両方である。
3)GDPR58 条(2)(f)(j)は、欧州委員会の十分性決定がなくて、標準データ保護条項に従うデータの移転に関して、もしこれらの条項が第 3 国が遵守できないか、他の手段では保障することができない場合には、権限ある監督機関が中断または禁止することを求めている。
4) 第 7 および第 11 質問に対する回答は次の通り。
基本権憲章 7 条、8 条および 47 条に照らした SCC 決定を検証した結果では、同決定の有効性に影響することは、何も明らかにならなかった。
5) 欧州委員会のプライバシー・シールド実施決定は、無効である。

7.1.3 本判決の論点
本判決では、かなり詳細な審理が行われている。判決要旨としては以下のような事項があると考えられる。
１）GDPR は、加盟国から第 3 国への個人データの移転に対して適用される。
２）GDPR46 条の SCC による個人データの第 3 国への移転においても、EU 法と本質的に同等の保護水準を保障しなければならない。
３）GDPR58 条は、データの保護水準が GDPR の求める水準にない場合には、加盟国の監督機関にはデータ移転の中断または禁止する権限があると規定している。
４）SCC 決定は、当事者間の契約であるので、公的機関のアクセス・利用には効力は及ばないことを理由に、その有効性がないとは言えない。
国家安全保障などの理由に基づく必要な限度を超えない強行規定は、SCC と矛盾しない。管理者が追加的な措置を講ずることによって、十分な保護水準にあれば、有効性は認められる。
５）EU 司法裁判所がプライバシー・シールドの無効宣言をしない限り、加盟国の監督機関は、データ移転の中断または禁止をすることができない。しかし十分性認定の適合性を争う訴えについて、十分な根拠があると考えるならば、EU 司

法裁判所に先決判決を求めるために、国内裁判所に訴えを移送しなければならない。
6）基本権憲章 52 条の規定では、基本権の制限には法的根拠があることおよび基本権の本質の尊重が求められる。比例原則に従い必要であり、EU 法で認められている一般的な利益に合致する場合にのみ制限できる。

基本権を制限する立法には、範囲や適用に関する明確でかつ詳細な規定が必要である。しかし米国法では監視プログラムの実施権限に制約がなく、最小限の保護措置を講じておらず、またオンブズパーソンによる救済の仕組みも不十分であり、EU 法と本質的に同等な保護水準にないため無効である。

この無効判決を受けて 7.2 で述べるように、EU-米国間データ・プライバシー・フレームワークの原則合意、および大統領令 14086 号の発出を経て、欧州員会の実施決定がなされた。

7.2 プライバシー・シールド無効判決後の EU-米国間の見直し交渉

7.2.1 見直し交渉の経過

2020 年 7 月 16 日のプライバシー・シールド無効判決後に、EU-米国間で判決内容を踏まえた見直し交渉が行われていたが、2022 年 3 月 25 日にデータ・プライバシー・フレームワークに関して、原則合意[68]がなされた。

この原則合意では、米国のシギント活動に適用されるプライバシーと市民的自由の保護を強化するための新しい保護措置として、①シギント活動が国家安全保障目的の遂行において必要で比例的であることを保障すること、②2 層の独立した法的拘束力のある救済制度を創設すること、③シギント活動の制限に関する遵守を保障するために、厳格で重層的に監督を強化することの 3 点が、基本的事項として謳われている。

また、この見直しの狙いは、市民の権利を保護することと共に、大西洋横断のデータ流通を促進することで、デジタル経済を促進することであると述べられている。

この原則合意に基づいて、米国は同年 10 月 7 日に大統領令 14086 号を発出した。これを受けて、同年 12 月に欧州委員会はデータ・プライバシー・フレームワーク草案を採択した。その後 EU 内部の調整を経て、2023 年 7 月 16 日に欧州委員会はデータ・プライバシー・フレームワークの実施決定を行い、即日施

[68] European Commission “European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework” 25 March, 2022

行された。

7.2.2 大統領令（Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities　October 7, 2022）14086 号

1 条（目的）においては、①インテリジェンスないしシギント活動の安全保障上の重要性を強調するとともに、その活動に当たってはすべての人を尊厳と敬意をもって遇すること、②個人情報を扱う際には、すべての人が正当なプライバシーの利益を有していることに配慮すべきこと、③そのためシギント活動に対する保護措置を創設することを、達成すべき目的としている。

2 条はシギント活動についての規定である。ここでは、EU-米国間での原則合意を反映した必要性、比例性や厳格な監督のあり方に加えて、以下の規定が盛り込まれている。

(1)シギント活動の目標として、外国政府などの能力・意図・行動を理解し評価すること、外国の軍事的能力や行動から米国を守ること、外国政府等によるインテリジェンス行動やサイバーセキュリティの脅威から米国を守ること、選挙や政治的プロセス・政府資産・インフラを守ることなどが挙げられている。

(2)禁止されるシギント活動としては、批判や言論の自由の抑圧、正当なプライバシーの利益の抑圧・制限、人種・性別・宗教などによる不利益扱い、および米国企業を競争上優位にするために、外国の商業的情報や営業秘密を収集することなどが挙げられている。

(3)プライバシーおよび市民的自由に関する保護措置に関する事項として、シギント情報のバルク収集に関して規定されている。ここでは、特定対象の情報収集が優先され、これにより難い場合にバルク収集が認められるとされている。

またバルク収集は、テロ対策、諜報、サボタージュ、暗殺、サイバーセキュリティの脅威などを目的とする場合に限定されている。

この他、シギント活動で収集した個人情報の扱いとしては、収集した個人情報の配布および保存に関する最小化原則とともに、データセキュリティやデータ品質、バルク収集した情報を扱う際のプライバシーおよび市民的自由への配慮、監督を容易にするための文書化、PCLOB[69]による監査などについて記載されている。

---

[69] PCLOB (Privacy and Civil Liberties Oversight Board)は、9/11 Commission Act of 2007 によって、行政府の独立行政委員会として設立された委員会である。その責務としては、連邦政府のテロ防止の取組とプライバシーおよび市民的自由のバランスを取ることである。

3 条では、シギント活動で権利を侵害された人への救済の仕組みが規定されている。原則合意で述べられているように、2 層の救済制度が新設されている。第 1 層は訴えに対する調査、監査、適切な救済策の命令を行う CLPO[70]（Civil Liberty Protection Office）を創設である。

第 2 層は、司法省の内部組織として創設された DPRC[71](Data Protection Review Court：データ保護審判所）である。この審判所は CLPO の決定に対して、不服がある場合の訴えの審判を行うもので、判決には法的拘束力があり、インテリジェンス機関には遵守義務がある。

さらに、救済措置に関して PCLOB が年次監査を行うことも規定されている。

4 条は用語の定義[72]であるが、バルク収集（bulk collection）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、大量のシギントデータの許可された収集」と定義されている。

7.3 欧州委員会のデータ・プライバシー・フレームワーク実施決定

この実施決定の内容は、EU 司法裁判所のプライバシー・シールド無効判決を受けて行われた EU-米国間の交渉のなかで、7.2.1 で述べた原則合意および 7.2.2 で述べた大統領令 14086 号の内容を反映したものとなっている。

7.3.1 データ・プライバシー・フレームワーク文書の構成

2023 年 7 月 10 日に実施決定された文書は、本文と付属資料とから構成されている。本文の主な構成としては、1）データ・プライバシー・フレームワーク 7 原則、2）実施の仕組み、監督、執行力、救済、3）米国の公的機関による EU から米国に移転された個人データへのアクセスと利用について、犯罪に関する法執行目的および国家安全保障目的に分けて、それぞれの法的根拠、制限、保護

---

[70] 国家情報長官室（ODNI：Office of the Director of National Intelligence）の内部組織として創設されている。その責務としては、国家情報長官室およびインテリジェンス機関の法令遵守状況を監督すること、インテリジェンスプログラムの濫用（abuse）に関する訴えを審査することなど、7 項目の責務が規定されている。出典：50U.S.C. §3029

[71] DPRC は、28CFR201 によって創設されたもので、この PART201 に設立目的、組織および権限・役割が規定されている。

[72] インテリジェンスの定義は、大統領令 12333 号と同じとされている。12333 号では、インテリジェンスはカウンターインテリジェンスと外国インテリジェンスの両方であると定義されている。

措置、監督、救済について、十分性認定の審査の内容が述べられている。

分量的には、国家安全保障目的に関する記述が犯罪の法執行に関する記述の 2 倍ほどあり、本実施決定の焦点が国家安全保障目的のための、公的機関による個人データへのアクセスと利用にあることが伺える。

ついで、結論、本決定の効果、データ保護機関の行動、本決定のモニタリングおよび審査の記述の後で、5 条からなる決定内容が記述されている。

付属資料は米国側が作成した資料である。付属資料 I は商務省作成のプライバシー7 原則、補足的 16 原則が記載されている。付属資料Ⅱと Ⅲは商務省からの説明文書、付属資料Ⅵと Ⅴは自己認証登録企業を監督する FTC 委員長（連邦取引委員会）と運輸長官の説明文書、付属資料Ⅵは司法省の本実施決定に係る米国法の簡単な説明文書、最後の付属資料Ⅶは国家情報長官室からの大統領令 14086 号、FISA702 条などの米国法の規定、およびシギント活動におけるバルク収集についての説明文書となっている。

7.3.2 データ・プライバシー・フレームワーク実施決定文書の内容

（1）自己認証登録企業に係る規定

1）プライバシー・シールドと同じく、データ・プライバシー・フレームワークでは、EU 市民の個人データの米国への移転先として自己認証登録企業制度を採用している。EU 側へは商務省が米国側を代表し、FTC と運輸省が自己認証登録企業のプライバシー原則等の遵守状況を監督するとの仕組みを採用している。

また自己認証については、毎年再認証する制度を新たに導入している。

2）データ・プライバシー・フレームワーク原則

同原則では個人の権利として、データへのアクセス、取扱いに反対する権利、データを訂正・削除させる権利、個人データの管理者または処理者に対する法的執行が可能であることが挙げられている。

3）救済

自己認証登録企業がプライバシー原則を遵守していない場合に、EU のデータ主体には救済を求めることのできる 6 つの方法が述べられている。

（2）公的機関による犯罪に関する法執行目的での個人データへのアクセスおよび利用（90～118 項）

1）同目的での個人データの収集・利用に関する制限

収集に関する法的な手続き（令状、召喚状、裁判所命令など）が、記載されている。また、Clinger-Cohen 法およびコンピュータセキュリティ法によって付与されている権限に従って、行政管理予算局（OMB）Circular No. A-130、連邦情

報セキュリティ管理近代化法（Federal Information Security Management Modernization Act）、E ガバメント法および連邦文書法（Federal Records Act）の規定が適用される。

2）監督

司法的な手続き、各省に配置されている PCLO（Privacy and Civil Liberties Officers）、FBI を含む司法省を監督している独立監察官（Inspector General）、テロ対策活動に関しては PCLOB および上院・下院の司法委員会によって重層的に監督されている。

3）救済

行政部門の救済としては PCLO、司法的救済としては、行政手続法（APA：The Administrative Procedure Act）、情報公開法（FOIA）、電子通信プライバシー法が挙げられている。

(3)国家安全保障目的での米国の公的機関によるアクセスおよび利用（119～200 項）

1）根拠法（120～126 項）

FISA（Foreign Intelligence Surveillance Act：外国諜報監視法）、NSL（National Security Letters）、米国外における収集については大統領令 12333 号、大統領令 14086 号が挙げられている[73]。

2）国家安全保障目的での個人データ収集に関する制約と保護措置（127~153 項）

この実施文書では、大統領令 14086 号の個人データ収集、利用、配布などに関する保護措置規定が、詳細に述べられている。

またバルク収集については、米国外でのみ行い得るもので、この場合でも特定対象の収集が優先されること、特定の目的に限定されることなどが述べられている。またバルク収集に係る FISA105 条の規定内容についても述べられている。

さらに FISA702 条において、司法長官と国家情報長官は、収集すべき情報類型を特定する年次認証請求を FISC に提出することされている。また FISC の決定について FISCR（Foreign Intelligence Surveillance Court of Review）へ控訴できること、最終的には連邦最高裁に上告できると述べられている。

この他 NSA の活動についても、述べられている。NSA の収集対象の選定に

---

[73] プライバシー・シールドで言及されていた PPD28 号は、国家安全保障メモランダム（National Security Memorandum/NSM-14）に基づき、大統領令 14086 号によって一部が廃止された。PPD28 号で廃止されていない規定は、3 条、6 条および秘密指定の付属規定である。実施は、大統領令 14086 号の発効日と同日付である。

関しては、司法省のインテリジェンス活動監督室の責任者が、NSA の法律違反を FISC と議会に報告することが義務付けられている。

加えて FISA の規定内容について、例えば 301 条、402 条、501 条の内容についても説明がある。

3）国家安全保障目的で収集された情報の利用に関する保護措置

シギント活動で収集された個人データ保護措置の主要事項

① 適切なデータセキュリティを保障すること、および許可を得ていないアクセスを防止すること。このために多段階認証（multifactor authentication）や暗号のような最小限の情報セキュリティ手法を講ずる。

② インテリジェンス機関は、インテリジェンス・コミュニティの正確性や客観性に関する標準を遵守しなければならない。

③ データ保存および配布の規定は、米国人と非米国人とは同じ扱いである。

4)行政部内による監督（162～168 項）

インテリジェンス機関の活動は、様々な機関により監督される

・各インテリジェンス機関の内部監査組織：上級レベルの法務、監督、コンプライアンス担当官、独立した監察官（Inspector General）

・国家情報長官室の監察官には、インテリジェンス・コミュニティ全体の監察権限がある。

・大統領インテリジェンス・アドバイザリー・ボードの内部組織として創設された IOB（Intelligence Oversight Board）は、インテリジェンス機関の憲法遵守状況を監督。

・PCLOB の監督にも服している。PCLOB はカウンターインテリジェンスの方針および実施に関して、プライバシーおよび市民的自由を保護する責任を担っている。

5)議会による監督（168～171 項）

① 議会（上下両院のインテリジェンス・司法委員会）は全ての米国の外国諜報活動に関する監督権限を有している。これらの委員会の議員は、秘密指定の情報およびインテリジェンスの方法や計画にアクセスする。

② 委員会は司法長官、国家情報長官、インテリジェンス機関および他の監督組織（例えば監察官）などから、インテリジェンス活動について定期的な報告を受ける。

③ 国家安全保障法は、大統領がこれらの委員会が十分な情報を得ることを保障する、と規定している。また大統領は、違法なインテリジェンス活動があった場合に、その是正措置と共に、インテリジェンス委員会に速やかに報告することとされている。

④ これらの報告の他に FISA は司法長官に、FISA の特定条項に基づく政

府の活動に関して、上下両院のインテリジェンス・司法委員会に十分な情報提供を行うことを求めている。

また FISA は、FISC または FISCR の全ての決定、命令または意見のコピーを提出することを、政府に求めている。

⑤ FISA702 条に基づく監視に関しては、半年ごとに司法長官が活動報告を行うことも含まれる。また各年の FISA 命令の件数や監視対象とされた米国人と非米国人の数も議会に報告することが、FISA に規定されている。

6)インテリジェンス機関による透明化の取組（172 項）

各インテリジェンス機関にインテリジェンス透明化責任者を指名。国家情報長官室の「IC on the Record」のウエブページへの掲載を含め、資料を公開。

7)FISC による監督（173～174 項）

(4)大統領令 14086 号で新設された 2 層の救済の仕組み（175～204 項）

1)第 1 に大統領令 14086 号によって、DPRC（Data Protection Review Court：データ保護審査裁判所）が創設された。EU 市民は、シギント活動を規律している米国法（例えば、大統領令 14086 号、FISA702 条、大統領令 12333 号）違反の疑いに関して、救済を求めて訴えを提起できる。

この救済の仕組みは、米国司法長官が「有資格国」と指定した国などの個人が利用できる。2023 年 6 月 30 日に、EU および欧州自由貿易加盟国 3 国が、大統領令 14086 号 4 条(2)に基づいて指定された。

2)EU のデータ主体は、EU 加盟国のデータ保護機関に訴えを提起することになる。これはデータ主体に訴えやすくするためである。訴えが受理されたら、当該データ保護機関は欧州データ保護委員会の事務局経由で、訴えを提起する。

訴えを提起する個人は、自身のデータが米国のシギント活動に利用されたことを証明する必要はないので、救済を求める訴えを提起しやすくなっている。

3)第 1 層の救済：国家情報長官室 CLPO による審査と決定（179~183 項）

①最初の訴えに対する調査は、国家情報長官室 CLPO（Civil Liberties and Privacy Officer）が行う。内部組織であっても、国家情報長官も CLPO への干渉は禁止されている。

② 訴えを審理するに当たっては、CLPO はシギント活動における国家安全保障の利益とプライバシー保護の両方に関して、法を公正に適用しなければならない。

③ 審理では CLPO は米国法違反があったか、もしあったとすれば適切な是正策を決定する。この決定は、当該インテリジェンス機関を拘束する。

④ CLPO は、違法行為の認定や適切な是正措置に関する決定を説明する秘

密指定された決定文書を作成しなければならない。

⑤ 審査が終了すると、(加盟国の) 機関経由で、訴えた人に審査結果を連絡する。国家安全保障上、行われた活動の秘匿性を保護することを認める一方で、個人に対しては訴えが正当に調査され裁定されたことを確認する決定を連絡する。この決定について、個人は不服申し立てができる。このため、DPRC へ上訴が可能であることの連絡がなされる。

4) 第 2 層の救済 (184～193 項)

①訴え人および各インテリジェンス機関は、DPRC に CLPO の決定の審査を求めることができる。この審査の訴えは、CLPO から審査終了の通知があってから 60 日以内に行わなければならない。EU 市民は、データ保護機関に訴えを提起できる。

② DPRC は、大統領令 14086 号の規定によって司法長官が創設した独立審判所である。司法長官が他の機関と協議して指名する最低 6 人で、4 年任期で再任可である判事 (judges) で構成される。全ての判事は、セキュリティ・クリアランス資格を有していなければならない。

③ DPRC への訴えは、3 人の判事のパネルで審査される。DPRC は CLPO の決定を審査する。審査の結論としては、インテリジェンス機関が訴え人の個人データを扱った証拠はないと決定するか、CLPO の決定は法的に正しく証拠によって裏付けられていると決定するか、または CLPO の決定を不服として、自身の決定をする。

④ 全ての決定では、DPRC は多数決で文書化した決定を行う。審査で適用法違反があるとした場合には、決定で適切な救済策を決める。この決定には拘束力があり、かつ最終決定である。

また、法違反を認定した場合の、安全保障担当の司法次官と FISC への秘密指定の報告書の扱いは、CLPO の決定の場合と同様である。

⑤ DPRC の決定は CLPO に伝達される。訴え人には決定内容について、国の機関を経由して通知される。

⑥ 透明性を高めるために、司法省は少なくとも 5 年毎に、当該インテリジェンス機関に、DPRC の審査に関する情報が秘密指定を解除されたかを確認しなければならない。秘密指定が解除された場合には、訴え人にその情報が利用できることが通知される。

5)他の救済制度 (194～200 項)

この 2 層の救済制度は、定期的かつ独立した形で評価される。すなわち、大統領令 14086 号の規定に従って、PCLOB が年次審査する。この中で、CLPO および DPRC が訴えをタイムリーに処理しているか、両者が必要な情報に十分にアクセスしているか、審査に当たって大統領令 14086 号の保護措置が適切に考

慮されているか、インテリジェンス機関が CLPO および DPRC の決定を全面的に遵守しているかを評価する。

この評価結果の報告書を、大統領や関係機関に提出する。また秘密指定していない版を一般に公開する。この報告書は、欧州委員会が行う実施決定の定期的な審査に反映される。この他当事者適格が証明できれば、一般の米国の裁判所でも救済を求めることができる。

FISA などでは一定の条件がある場合には、個人が金銭賠償を求めて、訴訟提起ができることが規定されている。また不法なガバメント・アクセスの場合には他の法律（コンピュータ詐欺・不正防止法、電子通信プライバシー法など）、およびより一般的な救済方法としては APA（Administrative Procedure Act：行政手続法）によって訴訟提起ができる。情報自由法によって、個人は連邦機関の文書にアクセスする権利を有しているので、それらの情報にアクセスすることで、通常の訴訟を提起しやすくなる。

(5)結論（201～204 項）

欧州委員会は、GDPR と本質的に同等の保護水準を、米国が保障していると考える。その根拠として、プライバシー原則の効果的な適用、監督制度および救済策が整備されていること、犯罪の法執行および国家安全保障目的での（個人データへの）干渉は、正当な法目的達成のために厳に必要である場合に限られていること、および干渉に対する効果的な保護措置があることも挙げている。

(6)本決定の効力およびデータ保護機関の行為（205～207 項）

加盟国が EU 法を遵守するために必要な措置を講ずることを求められるのは、EU 法は適合的と推定され、廃止または先決判決で無効とされるまでは、法的効果を有するからである。従って欧州委員会の十分性決定は、国の独立監督機関を含めてすべての加盟国の機関を拘束する。

GDPR58 条(5)および Schrems 判決で説かれているように、加盟国のデータ保護機関が欧州委員会の十分性決定の適合性を問題にする場合には、同機関が国内裁判所へ EU 司法裁判所に先決判決を求めるために提訴する規定を国内法に置かなければならない。

(7)本決定のモニタリングおよび審査（208～214 項）

欧州委員会は十分性認定を行った後に、第 3 国が本質的に同等の保護水準を維持しているかを、継続的にモニターしなければならない。

このモニターを容易にするために、米国政府は、認証企業と公的機関の個人データへのアクセスに適用される制限と保護措置の両方に関して、法的および実

際の運用の変化について、欧州委員会に通知すべきである。
加盟国は特にデータ主体からの質問や訴えに関して、データ保護機関の取った行為について、欧州委員会に通知すべきである。
GDPR45 条(3)によって、欧州委員会は米国によって保障された保護水準が、依然として事実レベルでも法的にも正当化できる水準かについて、定期的に審査しなければならない。
本決定の最初の審査は、本決定の発効後 1 年以内に行うことになっている。この審査結果に基づき、関係機関と協議して、将来の審査の周期を決めることになる。またこの審査に当たっての着目点についても述べられている。

(8) 本決定の中断、廃止または修正（215～220 項）
モニタリングや加盟国機関からの情報によって、本決定に基づき移転されたデータの保護水準が最早十分ではないと判明した場合には、米国に適切な期限内に適切な措置を取るように、迅速に通知しなければならない。
米国が期限内に適切な措置を取らないか、十分な保護水準であることを証明することができない場合には、本決定の一部または全部を中断または廃止することに関して、GDPR93 条(2)の手続きを開始する。
また他の手続きとして、データ移転について追加条件を付するか、十分な保護レベルが保障されると認定されるデータ移転に範囲を限るかという修正について、手続きを開始する。
どういう場合に中断または廃止する手続きを開始するか、また修正手続きを開始するかについても述べられている。
これらの審査を経て、1 条から 4 条の決定を行っている。

7.4 プライバシー・シールドとデータ・プライバシー・フレームワークの比較

プライバシー・シールド実施決定（本項では以下 PS）とデータ・プライバシー・フレームワーク実施決定（本項では以下 DPF）を比較すると、かなり類似の項目なり内容が多い一方で、異なる事項もある。PS と DPF を、決定文書の構成および内容の両面から比較してみることとしたい。

7.4.1 類似事項

（1）文書の構成
1）PS は欧州委員会作成の本文が 43 ページ、米国側作成の付属文書が 100 ページで合計 143 ページであるのに対して、DPF は本文が 64 ページ、付属文書が 67 ページで合計 131 ページである。

２）PS の本文は、Introduction が約 3 ページ、EU-US PS が約 12 ページで、公的機関のアクセスおよび利用が約 12 ページ、十分性認定やその定期的な点検、十分性認定の中断などが 5 ページ、条文が約 2 ページとなっている。

DPF の本文は、Introduction が 3 ページ弱、EU-US DPF が約 19 ページ、公的機関のアクセスおよび利用が約 36 ページ、そのうち法執行目的の部分が約 12 ページ、国家安全保障目的の部分が約 24 ページ、結論、決定のモニタリングと評価および決定の中断、廃止または修正が約 4 ページで、条文が 1 ページ強となっている。PS と比較すると、全体の分量がかなり多くなっているうえに、公的機関のアクセスおよび利用に関する審査の記述のウエイトが高く、そのなかでも国家安全保障目的の部分のウエイトが特に高くなっている。

これは特に国家安全保障目的のガバメント・アクセスが焦点となっていることの反映であると考えられる。

３）PS7 原則および補充的 16 原則は、DPF 原則と補充的原則と項目数および内容が同一である。

４）付属文書の作成省庁は、商務省、FTC、運輸省、司法省、国家情報長官室であり共通している。司法省は法執行目的について、国家安全長官室は国家安全保障目的の法規定について述べている。

（２）実施決定内容

１）EU-US PS および EU-US DPF とも、権限の制約、保護措置、監督の仕組み、救済の仕組み、透明性などの項目は共通している。

２）自己認証登録企業制度を採用していて、EU 側へは商務省が米国側の代表し、FTC と運輸省が自己認証企業の遵守状況を監督する仕組みは、セーフハーバー以降同じ仕組みが継続している。

３）ガバメント・アクセスについては、法的根拠、権限の制限、保護措置、監督の仕組みおよび救済の仕組みが規定されていることは、両者で共通している。

7.4.2 内容における相違事項

DPF では、EU-US DPF において、個人の権利[74]（individual rights）および説明責任[75]（accountability）の項目が加わっている。

---

[74] データ主体の権利として、データへのアクセス権、データの取扱いに反対する権利およびデータの修正および消去の権利があること、またアクセス原則などについて述べられている。これは救済に関係する記述である。（29～36 項）

[75] 説明責任について述べられているが、これも救済に関する記述であり、DPF が救済の仕組みの見直しに重点を置いていることが伺える。（44～46 項）

DPF では、国家安全保障目的でのガバメント・アクセスの個人データへの不法な侵害に対する、新たな 2 層の救済制度の内容ついて、かなり詳細に記述されている。

またバルク収集については、PS でも DPF でも記述されているが、内容が多少異なっている。PS 本文では、PPD28 号のバルク収集の制限および米国自由法について述べるとともに、FISA の規定にも言及していて、FISA702 条は特定対象の監視を行うもので、米国は無差別な監視を行っていないと米国政府は保障している、と述べている。

また国家情報長官室が作成した PS 付属文書Ⅵでは、PPD28 号に規定されている収集制限および保存期間の制限、FISA702 条に基づく収集について本文と同様、バルクでも無差別ではないこと、および米国自由法におけるバルク取集規定について、FISA でも NSL（国家安全保障書簡）でもバルク収集は行っていないと述べている。

一方 DPF ではバルク収集について、大統領令 14086 号の規定において、特別の保護措置があることが述べられている。（141 項）

また付属文書Ⅶでは PS 付属文書Ⅵと同様に、FISA でも NLS でもバルク収集は行っていないと述べている。

7.5 欧州委員会の新 SCC 実施決定(2021/914)（2021 年 6 月 4 日）

（1）新 SCC の実施決定までの経過

プライバシー・シールド無効判決（SchremsⅡ）では、欧州委員会のプライバシー・シールド実施決定が無効であるとされた一方で、SCC（Standard Contractual Clauses：標準契約条項）実施決定は有効とされた[76]。

この SCC 決定はデータ保護指令の下での決定であり、判決内容をも反映する形で、また GDPR との整合性を図るため、新しい（modernized）SCC 制定への検討が始まった。

欧州委員会は、判決 4 か月後の 2020 年 11 月に新 SCC 草案を公表、内部検討を経て 2021 年 6 月 4 日に新 SCC の実施決定を行った[77]。

---

[76] 判決では米国法により、SCC が保障する保護水準が損なわれることを防止するための追加的措置に言及している。

[77] Commission Implement Decision EU 2021/914of 4 June 2021
なお正確を期せば、GDPR46 条の文言は standard contractual clauses ではなく、standard data protection clauses である。しかし SCC の語が長く使われてきたため、欧州員会の実施決定文書でも SCC の語がそのまま使われている。

（2）新 SCC の内容

1 条では、本標準契約条項の目的は、個人データの第 3 国への移転に関して、GDPR の要件の遵守を保障することであると規定されている。

「第Ⅱ当事者[78]の義務」では、管理者(controller)から管理者への移転、管理者から処理者（processor）への移転、処理者から処理者への移転、処理者から管理者への移転の 4 つのモジュールに分けて、それぞれの義務を規定している。

処理者から管理者への移転を除く 3 つのモジュールに共通する義務としては、目的の制限、透明性、データの正確性、保存期間の制限、取扱いのセキュリティ、機微データ、再移転、文書化および遵守がある。処理者から管理者への移転については、データ輸入者からの指示、取扱いのセキュリティ、文書化および遵守が義務となっている。

10 条ではデータ主体の権利、11 条ではデータ主体の救済の規定、12 条は民事責任（liability）、13 条では監督（supervision）が規定されている。

また「第Ⅲ 公的機関によるアクセスの場合の第 3 国の法および義務」では、14 条は第 3 国の法と慣行[79]、15 条は公的機関によるアクセスの場合のデータ輸入者の義務が規定されている。

「第Ⅳ 最終規定」では、16 条は条項の不遵守および解除、17 条は準拠法（Governing law）、18 条は裁判管轄が規定されている。

（3）新 SCC で改正・強化された事項[80]

改正理由は(1)で述べたように、GDPR との整合性を図るため、また判決内容を反映するためである。

データ保護原則、セキュリティ義務、データ保護機関と裁判所など基本的な事項は維持されている反面、主な改正事項としては、第 1 に SCC のアーキテクチャがアップデートされている。①管理者、取扱者の間での 4 つのモジュール毎に当事者の義務が規定されている。②SCC へ新たな参加者を認める結合条項[81]

---

[78] controller と processor は、GDPR4 条にそれぞれ定義がある。

[79] 「両当事者は、輸入者による個人データの処理に適用される移転先第 3 国の法令・慣行が、輸入者による新 SCC の条項の義務を妨げると信ずべき理由がないことを保証しなければならない(a)項。」この保証のために、データ移転影響評価の実施が必要となるが、この評価の実施は実務上負担が大きいと指摘されている。出典：田中浩之・北山昇「欧州新 SCC の概説とデータ移転に係る実務対応」ビジネス法務 2021.10 条文の日本語訳はこの資料による。

[80] 出典：欧州委員会の “New Standard Contractual Clauses Q and A overview”

[81] SCC の締結後でもこの条項を通して、新しい当事者を加えた複数の当事者で使用できる。出典：前掲注 79　p16

（docking clause）を新設。③Annexes に具体的な情報が掲載されている。

例：Annex Ⅰ では当事者のリスト、AnnexⅡの技術的・組織的措置では、個人データの仮名化・暗号化措置など。

第 2 に多くの改正事項が挙げられている。①GDPR の新たな要求事項を反映させている。例：透明性義務の強化、データ主体の権利のより詳細な条項、データ侵害の通知および再移転の規定、②GDPR28 条の要求事項の SCC への組入れ、③SchremsⅡ判決内容を実行するために、SCC の当事者による影響評価を行い、移転先の法律および個人データを守るための追加保護措置の文書化、

④ 公的機関が移転されたデータへ、アクセスする場合の新たな義務設定
例：データ輸出元へ通知および不法な要求に異議を唱えること。

7.6 欧州委員会の英国に対する 2 つの実施決定

欧州委員会は 2021 年 6 月 28 日に、英国に対して個人データの保護に関する 2 つの実施決定を行った。

1 つは、GDPR（Regulation (EU) 2016/679）(2016 年 4 月 27 日)に基づく実施決定であり、他の 1 つは刑事司法指令[82]（Directive (EU)2016/680）(2016 年 4 月 27 日)の基づく実施決定である。

（1） GDPR と刑事司法指令の関係および規定内容

EU における個人データの取扱いに係る規律は、GDPR によって定められているが、その 2 条(2)(d)において、「犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行のために行われる場合」には、GDPR の適用対象外となっている。

この 2 条(2)(d)の分野における個人データの取扱いは、刑事司法指令によって定められている。

GDPR と刑事司法指令は、類似の規定が数多くあるが、その制定趣旨から一方にあって他方にない規定もいくつかある。

1) GDPR にあって刑事司法指令にない規定としては、データポータビリティ、行動規範や認証制度、一貫性の仕組み、行政上の制裁などがある。

2) 刑事司法指令にあって GDPR にない規定としては、刑事犯罪に係る者に関する異なる種類のデータ主体の区分（6 条）、事実に基づく個人データと人物評価に基づく個人データの区分（7 条）、ロギング（25 条）などがある。

ロギングについては、「1 加盟国は、少なくとも、自動処理システムを用いた

---

[82] 刑事司法指令については、以下の文献を参照した。石井夏生利[2020]『EU データ保護法』第 3 章、星周一郎「GDPR と刑事司法指令・NPR 指令の相関―データの越境移転を中心に」ジュリスト 2018 年 7 月号 pp20~25

次に掲げる取扱業務、すなわち、収集、修正、照会、移転を含む提供、結合および消去を行う際に、ログを保存するように定めなければならない。(以下略) 2 ログは、取扱いの適法性の確認、自己監視、個人データの完全性及び安全性の保障並びに刑事手続きにのみ用いるものとする[83]。」

一方で加盟国は個人データの消去や個人データの保存の必要性について、定期的な審査を行うことが定められている（5 条)。

（2） GDPR に基づく実施決定の構成および内容

1）実施決定は、前文と 229 項目および条文 4 条から構成されている。

十分性認定を行うために、英国の法制度[84]などを GDPR の観点から審査している。まず個人データの取扱いに適用される規律について、データ保護法（Data Protection Act）2018 と UK GDPR についての Brexit に伴う立法経過が述べられていて、EU GDPR と同様な内容であることが述べられている。

2）ついで保護措置、権利および義務の規定が述べられている。さらに監督と執行については、独立した監督制度、制裁を含む執行、救済についての規定が述べられている。

3）十分性認定において焦点となっている、公的機関の移転されたデータへのアクセスと利用について、犯罪に係る法執行と国家安全保障とに分けて、それぞれの（公的機関のアクセスと利用についての）法的根拠および適用される制限・保護措置、監督および救済に関するデータ保護法 2018 および IPA2016 の規定が

---

[83] 出典：日本語訳は石井、前掲注 82　pp301~302

[84] 英国の個人データ保護に関する法律には、データ保護法（DPA：Data Protection Act）2018 と UK GDPR がある。

EU 法の規則は、国内法化が必要な指令とは異なり直接適用可能（directly applicable）であり、「その制定により自動的に各国内法制度の一部となり、実施のためのいかなる国内立法も必要としない。」（出典：庄司 前掲注 4、p252）

しかし GDPR23 条には、12 条から 22 条、34 条および 5 条の規定に関して、加盟国が立法措置によって、国家安全保障など 9 項目については、適用範囲を制限できるとの規定がある。この GDPR23 条の適用制限に関する法律が、データ保護法 2018 である。

従ってデータ保護の基本法は UK GDPR であり、適用制限する場合であっても、「その制限が基本的な権利及び自由の本質を尊重するものであり、かつ（中略）必要かつ比例的な措置である場合（23 条(1)）」とされている。なお 23 条(1)は基本権憲章 52 条(1)とほぼ同一の表現となっている。

以下の英国政府のサイトも参照。https://www.gov.uk/data-protection

述べられている。特に IPA2016 の調査権限については、詳細に述べられている。

(3) 十分性認定理由

1)英国は EU を離脱したが、現在の個人データ保護の法制度は、EU にいたときと同じである。但し欧州議会や加盟国が懸念しているように、将来的に EU とは異なる法制度になる可能性に関しては、英国側に重要な保護措置に変化があれば介入する。

2)プライバシー・シールド判決を受けて、特に国家安全保障を理由とする公的機関の個人データへのアクセスについて、英国は強力な保護措置を定めている。特にインテリジェンス機関によるデータ収集は、独立した司法的組織による事前承認に従っている。いかなる手段も達成しようとすることに対して、必要性があり比例的であることが必要である。

3) 救済に関しては、不法に監視されたと考える人は、誰でも IPT（調査権限審判所）に訴えを提起できる。

4) また英国は人権裁判所の管轄内にあって、人権条約と個人データの自動処理に関する欧州評議会条約（108 号条約）を遵守する立場にある。

5) 初めて「サンセット条項」を取入れた。すなわち、4 年毎に十分性認定は期限切れとなり、その後は英国が個人データの十分な保護レベルを維持する限り、認定を更新できる。

6) この 4 年間の期間中であっても、英国の法制度の状況をモニターして、いつでも介入することができる。

7) IPA2016 の調査権限については、特定調査権限とバルク調査権限について個別の権限の内容、手続きなどを詳細に審査している。注目すべきは、バルク調査権限は、制限と保護措置のない大量監視（mass surveillance）とは同じではないと述べていることである（216 項）。

8) 「4.結論」では以下のように述べられている。

欧州委員会は、英国の GDPR およびデータ保護法 2018 は、EU の GDPR と本質的に同等の保護水準にあると考える。監督の仕組みおよび救済方法は、実際の侵害行為を判定し処罰することを可能にし、データ主体が自身の個人データにアクセスし、その訂正や削除できる救済策もある。

法執行および国家安全保障目的での、公的機関の個人データへの干渉は、達成すべき正当な目的に厳に必要で比例的であると考える。

この結論は、英国の国内法および国際的約束、特に人権条約の遵守および人権裁判所に従うとの両方に根拠を有している。

9) 「5.本決定のモニタリング、中断、廃止または修正」では、GDPR45 条(4)の決定に従って行うことを表明している。

10) 「6.本決定の期間および更新」では、5）で述べたことを再説している。

(4) 刑事司法指令に基づく実施決定の構成・内容および認定理由

1) この実施決定は、前文 181 項目および 5 条の条文から構成されている。内容としては、権限のある機関の刑事司法目的での個人データへのアクセスや利用に特化している。

2) しかし構成自体は、GDPR に基づく実施決定と同じような構成となっていて、調査権限とその制限と保護措置、監督および救済に関する英国の法制について審査を行っている。

3) 「3.結論」、「5. 本決定のモニタリング、中断、廃止または修正」、「6. 本決定の期間および更新」では、GDPR に基づく実施決定と同じ構成になっている。

4) 但し本実施決定では、「4.本決定の効果およびデータ保護機関の行為」において、EU の加盟国とその組織が必要な措置を講ずることが定められている。これは、本実施決定の名宛人が加盟国であること、および Regulation ではなく Directive による実施決定であるので、加盟国の行為が必要になるためである。

（5）EU-米国間における犯罪に関する個人情報を移転する協定

前(4)は刑事司法分野における、EU から英国への個人データの移転に関する十分性認定である。

これに対して EU-米国間でのテロを含む犯罪の防止、捜査、探知および訴追に係る個人情報の保護に関する EU-米国間の協定が、 “EU-US Umbrella Agreement[85]”である。

この協定の成立に必要な手続きが、EU 側では欧州議会の同意を経た閣僚理事会決定（Council Decision (EU)2016/920）であり、米国側は司法救済法に基づく（EU を covered country に）指定を行うことである。これらの手続きが終了したことで、協定は 2017 年２月１日に発効した。

但しこの協定自体が、米国への個人情報を移転する法的根拠とならず、既存の EU-英国および加盟国-米国の協定を補完するものである。

7.6 の欧州委員会の２つの決定は、EU から英国への個人データの移転である

---

[85] EU-US agreement on personal data protection/ EUR-LEX(Europa.eu)、Council Decision (EU)2016/920 of 20 May, 2016、Official Journal of the European Union L336/3, “Agreement”, 10 December 2016, European Commission-Fact Sheet “Q and A on the EU-U.S. Data Protection “Umbrella Agreement” 1 December , 2016

また英国-米国間では、UK-US Data Transfer Agreement によって、犯罪捜査に関する個人情報を、法執行機関が相手国の電気通信事業者に直接請求できる協定がある。

のに対して、この協定の特徴は EU-米国間および米国-EU 間の相互の個人情報の移転であること、および EU 側の決定が欧州委員会ではなく閣僚理事会決定であることである。なおこの協定では、個人データではなく個人情報との用語が使われている。

7.7 英国側の対応

7.7.1 EU に対する十分性認定

7.6 で述べたように欧州委員会は、Brexit 後の 2021 年 6 月 28 日に、英国に対する EU 市民の個人データの英国への移転に関する十分性認定を行った。

一方、英国はデータ保護法 2018 の 17A 条および 74A 条に基づいて、EU に対して Brexit 移行期間終了日の 2020 年 12 月 31 日に、国務大臣[86]が十分性認定を行っている。

7.7.2 英国の新 SCC：IDTA（International Data Transfer Agreement）および UK Addendum[87]

7.5 で述べたように欧州委員会は、データ保護指令において決定された SCC を GDPR とより整合的にするため、およびプライバシー・シールド無効判決内容を反映させるために、2021 年 6 月 4 日に新 SCC の実施決定を行った。

この時点で英国は既に EU を離脱していたため、この EU の新 SCC を利用して、英国市民の個人データを第 3 国へ移転することができない。

この状況に対応するために、ICO は 2021 年 8 月に IDTA と Addendum 草案の諮問を開始して、2022 年 2 月 2 日に国務大臣は議会へ提出した。この経過を経て、英国は EU の新 SCC の英国版である IDTA と UK Addendum を、2022 年 3 月 21 日付で発効させた。

IDTA[88]と UK Addendum は、十分性認定を行っていない第 3 国へ英国市民

---

[86] 国務大臣とは DCMS（文化、メディア、スポーツ省）大臣のことである。この十分性認定を行うためには、事前に ICO（情報コミッショナー室：DCMS に所属している独立行政委員会、データ保護法に ICO の規定がある。）と協議が必要である。出典：Alan Meneghetti and Stewart Duffy “Adequacy Decision Under the UK GDPR and Data Protection Act 2018” 17 May, 2021。

[87] UK Addendum の正式名称は、International Data Transfer Addendum to the EU Commission Standard Contractual Clauses である。

[88] IDTA と UK Addendum については、ICO の以下のサイトを参照。
“International data transfer agreement and guidance”

の個人データを移転する場合に利用される。UK Addendum は、多者間のデータ移転協定を創出するために、EU の SCC に追加する意図がある。英国と EU の両方で個人データの取扱いを行っているデータ輸出元に応えるものである。

8. 調査権限の人権制約に関する許容度

8.1 EU 司法裁判所、欧州人権裁判所および英国国内裁判所の判決分析

調査権限（ガバメント・アクセス）の人権制約に関する許容性を探る目的で、まず 8 つの判決分析を行う。いずれも違法または無効との判決であるが、不適合性、審理対象事項、不適合とされた判決理由および正当で必要と認められた調査権限について分析する。

8.1.1 分析対象の判決（本稿の記述順）

・CJEU：データ保存指令無効判決（2014 年 4 月 8 日）[EU 第 1 判決]
・CJEU：DRIPA2014 違法判決（2016 年 12 月 21 日）[EU 第 2 判決]
・英国 High Court：IPA2016 違法判決（2018 年 4 月 27 日）
[High Court 判決]
・CJEU：Privacy International 判決（2020 年 10 月 6 日）[EU 第 3 判決]
・CJEU：La Quadrature du Net 判決（2020 年 10 月 6 日）[EU 第 4 判決]
・ECHR：Big Brother Watch 判決（2021 年 5 月 25 日）[ECHR 判決]
・CJEU：セーフハーバー無効判決（2015 年 10 月 6 日）[EU 第 5 判決]
・CJEU：プライバシー・シールド無効判決（2020 年 7 月 16 日）
[EU 第 6 判決]

注：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）
以下判例の呼称は、EU 第何判決、High Court 判決および ECHR 判決と呼ぶ。

8.1.2 不適合性

・EU 第 1 判決：基本権憲章に対して、データ保護指令が不適合
・EU 第 2 判決：プライバシー・電子通信指令に対して、英国国内法が不適合
・High Court 判決：プライバシー・電子通信指令に対して、
英国国内法が不適合

・EU 第 3 判決：プライバシー・電子通信指令に対して、英国国内法が不適合
・EU 第 4 判決：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
・ECHR 判決：欧州人権条約に対して、英国国内法が不適合
・EU 第 5 判決：データ保護指令に対して、欧州委員会決定が不適合
・EU 第 6 判決：GDPR に対して、欧州委員会決定が不適合

EU 第 1 判決は一次法に対して二次法（指令）が不適合との判決である。

人権条約に基づく国内法の適合性を判断した ECHR 判決を除き、他の 7 つの判決は、EU の二次法である指令・規則に対する、国内法または欧州委員会決定の不適合である。一次法である基本権憲章の規定に照らして解釈された指令・規則に対する不適合とされている。従って EU の一次法に対しても、国内法および欧州委員会決定は不適合との判決であると考えられる。

8.1.3 審理対象事項

・EU 第 1 判決： 焦点は全ての人の全てのトラフィックデータを、一律に最長 2 年間の保存義務。一部国の機関のアクセス
・EU 第 2 判決： トラフィックデータの全体的な保存義務、
保存されたデータへの国の機関のアクセス
・High Court 判決：IPA2016 4 編（データ保存通知）
・EU 第 3 判決：インテリジェンス機関のバルク通信データの取得・利用
・EU 第 4 判決：プライバシー・電子通信指令を根拠に、一般的かつ無差別な保存義務を、電子通信事業者に課すこと。特定人物のトラフィック・位置データのリアルタイム収集など
・ECHR 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受取
・EU 第 5 判決：欧州委員会のセーフハーバー決定
・EU 第 6 判決：欧州委員会の SCC 決定
欧州委員会のプライバシー・シールド実施決定

EU 第 1 判決から EU 第 4 判決および High Court 判決の 5 判決は、加盟国の国内法または指令の EU 法との適合性が問われた判決である。

一方 EU 第 5 判決と第 6 判決は、とりわけガバメント・アクセスに関する米国法とその実践が、データ保護指令または GDPR ひいては EU の一次法の規定に反していると判断したうえで、十分性認定を行った欧州委員会の決定を無効

としたものである。

従ってこの 2 つの判決は、実質は米国のガバメント・アクセスに対して向けられたものであり、上記 5 判決とは性格が異なる。

8.1.4 不適合とされた判決理由

・EU 第 1 判決：全ての人の全てのトラフィックデータを、一律に最長 2 年の保存義務が、比例性原則を超えている。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。（職業上守秘義務を負う人の通信に例外規定がない。国の機関のデータへのアクセス・利用に関する制限規定がない。保存期間の客観的基準がない。セキュリティとデータに係る濫用のリスクに対する保護措置規定がない。）

・EU 第 2 判決：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。
保存データの EU 域内での保有規定がない。
（データへのアクセスについて、明確かつ詳細な規律を定めなければないない。）

・High Court 判決：国の機関のアクセスを、重大犯罪に限定していない、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。
（IPA4 編は、一般的かつ無差別なデータ保存規定ではないと認定）

・EU 第 3 判決：一般的かつ無差別なトラフィック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。
権利を制限する国内法には、明確かつ詳細な規定が必要

・EU 第 4 判決：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を義務付ける国内法は、予防措置としては認められない。

・ECHR 判決： 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。
独立した許可制度がない。令状申請に選択語類型がない。
事前の内部許可に関して、個人を結びつける選択語がない。

・EU 第 5 判決：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）手段の範囲と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。決定 1 条・3 条は、データ保護指令の権限を超えている。

・EU 第 6 判決：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、範囲と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。

8.1.5 正当で必要な調査権限とされた事項

・EU 第 1 判決：指令の目的は、重大犯罪との戦いに貢献する。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。

・EU 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、保存データに対するアクセスを正当化できる。

一般的には犯罪と戦う目的に関しては、重大犯罪の計画に関与または関与したと疑われる個人のデータのみにアクセスできる。重大な国家安全保障、防衛または公共の安全が、テロリストの行動によって脅かされているような場合に、その行動と戦うのに役立つとの客観的な証拠があれば、他の人のデータへのアクセスも認められる。

・High Court 判決：特に言及はない。

・EU 第 3 判決：特に言及はない。

・EU 第 4 判決：

1） 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。

2） 国家安全保障、重大な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て、特定対象のトラフィックおよび位置データの保存規定は認められる。

3） 国家安全保障、重大犯罪との戦いおよび公共の安全への重大脅威の防止目的で、真に必要な期間に限定して、インターネット接続に割当てられた一般的かつ無差別な IP アドレスの保存規定は認めら

れる。

4） 電子通信システムの civil identity に関する一般的かつ無差別なデータの保存規定は認められる。

5） 重大犯罪および国家安全保障目的で、効果的な司法審査に服する権限ある機関の決定によって、電子通信事業者に対して、一定期間のトラフィックおよび位置データの優先保存を求める指示は認められる。

これらの例外は、明確かつ詳細なルールによって、当該データの保存が実体的および手続き的な条件に従って、当該人物が濫用リスクから効果的に保護されている場合に認められる。

6） トラフィックおよび位置データの自動分析およびリアルタイム取得、端末機器の位置に関する技術的データのリアルタイム収集は、以下の場合に認められる。

① 自動分析が、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状況に限定される場合で、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

② トラフィックおよび位置データのリアルタイム収集が、何らかのテロ活動に関わっているとの疑いに確固たる理由がある人物に限定されていて、かつそのようなリアルタイム収集が真に必要な期間に限り認められることを保障するために、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。

・ECHR 判決：バルク通信傍受は、加盟国が自国の安全保障への脅威を判定するために、不可欠な重要性を有していることを認める。
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。

・EU 第 5 判決：特に言及はない。

・EU 第 6 判決：特に言及はない。

8.1.6 判決における主な審理・判決事項

（1）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

EU 司法裁判所のデータ保存指令無効判決を始めとして、国内法の不適合を認めた DRIPA2014 違法判決、Privacy International 違法判決においては、いずれもこの保存義務を規定した指令なり国内法は、認められないとの判決である。

しかし同じ EU 司法裁判所判決であっても、La Quadrature du Net 判決

では、予防措置としては認められないとしつつも、一般的かつ無差別なデータの保存を始めとして、8.1.5 で述べたように、かなりの例外を認めていて、他の EU 司法裁判所判決とは異質な印象を受ける。

またこの判決が 2020 年 10 月 6 日と一番後に出された判決であることを考慮すると、EU 司法裁判所のスタンスが調査権限の制約を緩和するような方向へ転換したとも考えられる。

上記 EU 司法裁判所の判決では、いずれも国内法ないし指令が、一般的かつ無差別なデータ保存を義務づけていると判断したのに対して、英国 High Court の Liberty 判決では、IPA2016 4 編は一般的かつ無差別なデータ保存を義務付けた法律ではないと、7 つの理由をあげて認定している。

この Liberty 判決は、7.6 における欧州委員会の英国に対する十分性認定に関する実施決定において、英国のバルク調査権限は制限と保護措置規定があるので、大量監視（mass surveillance）ではないと認定している論調と符合している。

（２）明確かつ詳細なルール

EU 司法裁判所のいずれの判決においても、明確かつ詳細なルールを定めるべきであると指摘されている。

明確かつ詳細なルールには、調査権限の内容と制約に関する規定を定めるとともに、人権を守る観点から保護措置、監督、救済の規定を定めることが要請されていると考えられる。

但し調査権限の人権制約度合いについては、調査権限の目的である国家安度合いも変化することが考えられる。また変化について国民の理解が得られるのかとの問題もあるため、変化に対する迅速性とともに、ルールの透明性ないし分かりやすさも求められると考えられる。

（３）安全保障目的の調査権限を規定する国内法は、EU 法の適用外とする論

EU 司法裁判所の DRIPA2014 違法判決、Privacy International 判決および La Quadrature du Net 判決のすべての判決において、この論を否定していて国家安全保障を規定する国内法へも EU 法が適用されると判断している。

なお Liberty 判決においても、政府側は適用外を主張したが、Privacy International 訴訟でも同様の質問がなされているとの理由で、この問題の審理は停止された。

（４）保存データの EU 域内保存

EU 司法裁判所のデータ保存指令無効判決では、無効理由の一つに保存デー

タの EU 域内保存の規定がないことが挙げられている。理由としては、基本権憲章８条３項によって明確に求められている保護とセキュリティに関する、独立したコンプライアンス機関によるコントロールが行えなくなること、およびこのコントロールは個人データの取扱いに関する個人の保護に関する必須の構成要件であるとしている。

また DRIPA2014 違法判決でも、理由の一つとしてデータを EU 域内に保存する規定がないことが挙げられている。

しかし Liberty 判決で、Privacy International で同じ質問が付託されているので、判決審理中断とされた EU 域内保存について、Privacy International 判決では言及がなく、それ以降の判決でも言及されていない。

（５）判決分析から得られる示唆

上記の分析によって、判決では正当で必要な調査権限の存在を認めている。しかしいずれの判決においても、調査権限の必要性は認めつつも、指令、国内法および欧州委員会決定を、人権保障が不十分であることを理由に基本権憲章または人権条約に不適合と判決したものである。

この問題を考えるうえで、第１に調査権限の目的である国家安全保障やテロを含む重大犯罪との戦いに対して、目的達成のために効果的かつ効率的な調査権限活動を行っているか、第２に濫用・誤用を避け法目的に従い、調査権限活動が適正に行われているか、の２つの課題があると考えられる。

8.2　調査権限の適正執行を確保する課題１：効果的・効率的活動

まず第１に調査権限の目的である安全保障や重大犯罪の防止・捜査・探知・訴追に役立つ、効果的・効率的な活動が行われているかとの課題がある。

5.で述べたように、人権裁判所の Big Brother Watch 判決を受けて、英国政府は判決内容に対応するために IPA2016(Remedial) Order2023 を成立させた。

また英国政府は、IPA 成立から 6 年が経過して、その間の調査権限に関する脅威の変化や技術進歩を踏まえて、IPA の諸規定が法目的達成にふさわしかとの視点（fit for purpose）から改正検討を行って、2023 年 11 月 8 日に IPA2016(Amendment) Bill を議会に提出した。

この法案は法目的達成のために調査権限強化の規定とともに、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の規定も盛り込まれている。

この改正には、国家安全保障やテロを含む重大犯罪を取巻く技術進歩や脅威の深刻化を踏まえ、調査権限の目的を達成するために、調査権限の対処力を強化

するとの問題意識が伺える。

調査権限活動のために人権制約をしたとしても、それだけで国家安全保障や重大犯罪に関する安全性が高まるものではない。あくまで法目的に沿った調査権限活動を効果的・効率的に行うことで、安全性が高まることを認識することが重要である。

8.3　調査権限の適正執行を確保する課題 2：濫用・誤用防止を含む人権保障

第 2 の課題は濫用・誤用防止し、適正に執行する課題である。

ここでは、調査権限活動に関する監督・統制の仕組みについて述べる。

（1）まず調査権限を担う組織および従事者が、法目的に沿った効果的・効率的な調査活動を行うとともに、コンプライアンス遵守のマインドセットが醸成され徹底されることが重要である。これに組織内部での適正執行に対する内部統制の仕組みと実践が加わって、組織としての適正施行が担保されるものと考えられる。

（2）英国における適正執行については、2.で述べたように IPA2016 の 1 篇にプライバシー保護重視の規定、および各編に特定の人・情報および令状等の執行に関する保護措置規定が置かれた。さらに監督の仕組みを強化するために、行政内部に調査権限コミッショナーや司法コミッショナーを新設する法整備が行われた。

（3）議会の統制としては、プライバシー保護などの視点から活発な論議が行われ、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に関する統制が行われている。

また調査権限の執行過程に関して、Justice and Security Act 2013 の規定によって、インテリジェンス・保安委員会の権限が強化されている。監督権限はインテリジェンス 3 機関（GCGQ、MI5、MI6）の他、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などに及んでいる。また各インテリジェンス機関の予算支出、維持管理及び政策評価に加えて、オペレーション等にも及んでいる[89]。

上記のように英国では政府と議会の相互連携の下で、調査権限の適正執行が図られていると考えられるが、この背景としては、「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）と呼ば

[89] 出典：小林、前掲注 11　pp283-286

れるインフォーマルかつ主体的な協力関係の文化が構築されている。[90]」と説かれている。

（４）司法的統制

Brexit によって EU 司法裁判所の管轄からは離脱したが、司法的統制としては、国内裁判所および欧州人権裁判所による統制がある。

1998 年人権法 10 条の規定では、欧州裁判所または国内裁判所が英国法の条項を人権条約と不適合と判断した場合、これに対して国務大臣は不適合を除去するために必要な立法を命令（order）で行うことができる。

8.4　バルク・データ収集・利用の必要性および人権制約

8.4.1 バルク・データの必要性

アンダーソンの「バルク権限レポート[91]」では、調査権限法案が審議されていた 2016 年 8 月に議会に提出されたこのレポートは、国際的なプライバシー保護の観点から、バルク収集と保存に関する人権制約の許容性について、以下のように述べている。

①バルク権限はその定義上、国家安全保障や重大犯罪への関与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も、国家がアクセスする可能性がある。

②バルク権限のいかなる濫用も、無実の人々へ特に幅広い影響を及ぼし得る。探知できないまま濫用が可能であるとすれば、大きな不信感が生じ得る。

③上に述べたことは、バルク権限を放棄する理由にはならない。しかしこのようなリスクがあるので、バルク権限はそれを不可欠とする運用事例があり、かつ適切で目に見える保護措置に従う場合に限り、是認されるべきである。

またバルク権限の実態については、次のように述べられている。

④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御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 と MI6(秘密情報部)が利用している

⑤大多数の事例では、バルク権限を特定令状やヒューミントなど他の手段では代替できない。

⑥GCHQ 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のデータに基づいている。

---

[90] 出典：小林、前掲注 14　pp246~247

[91] 出典：　“Report of the Bulk Powers Review by David Anderson Q.C. Independent Reviewer of Terrorism Legislation” August 2016

⑦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。バルク機器干渉権限は、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。

8.4.2 Big Brother Watch 判決におけるバルク通信傍受に関する審理

（1）バルク通信傍受の意義

判決では、バルク通信傍受は外国のインテリジェンス情報収集や新たな脅威の特定に利用されている、と認定している（322 項）。

次いでフランス政府および英国・オランダ政府からのバルク通信傍受が必要であるとの提出意見[92]を参照しつつ、バルク通信傍受は加盟国が国家安全保障に対する脅威を特定するために、極めて重要であることを認めている（424 項）

（２）人権制約段階論

恣意的運用および濫用に対する保護措置の存在によって、条約が遵守されているかについて、実際の運用に関する限られた情報に基づいて、裁判所はデジタル分野における新たな脅威を特定する、貴重な技術的能力である加盟国の通信傍受の評価を求められている（323 項）。

英国政府はバルク通信傍受が、人権条約に規定されている人権への干渉であることを争っていない（324 項）。

裁判所の見解では、バルク通信傍受の人権制約の程度は、プロセスが進むにつれて段階的に高まってくるとして、個々の違いはあるが、以下のように考えられるとしている（325 項）。

① 通信傍受および通信内容並びに通信データの最初の保存
② 保存された通信内容および通信データへの特定の選択語の適用
③ 選択された通信内容および通信データの分析官による検証
④ データ保存および第 3 者とデータ保存を含む最終プロダクトの利用

① の段階では大量の個人データが自動的に収集されるが、このうち多くの情報はインテリジェンス機関には関心がない情報である（326 項）。

---

[92] 以下の意見を提出している。バルク通信傍受はテロリストの活動だけではなく、国家または非国家のアクターによる、（国政選挙への影響力行使などの）民主主義への妨害であるサイバー攻撃に対する、探知および防止にとって必要である。さらに（水道、エネルギー、通信、交通、輸送、港湾および空港のような）重要な部門は、よりデジタルに依存しているので、サイバー攻撃に脆弱になっている。この妨害の結果は金銭的な損害をはるかに超えて、社会へ深刻な影響がある（303 項）。

② の段階では、異なる種類の（e-mail アドレスのような強い選択語を含む）選択語 and/or 複雑な手順が適用される。強い選択語を利用して個人が特定される（327 項）。

③ の段階では、分析官によって検証され、④の段階で通信傍受された情報が実際のインテリジェンス機関によって利用される。利用用途としては、インテリジェンス・レポートの作成、他の国内または外国のインテリジェンス機関への情報の配布があり得る（329 項）。

（RIPA2000 の）8 条(4)は、各段階に適用されると裁判所は考える。

まず第 1 段階の通信傍受とそれに引続く通信の破棄の段階では、特段の干渉に該当しない一方で、通信傍受のプロセスが進行するにつれて、8 条(4)の個人の権利への干渉度合いが高まる。それにつれて、保護措置の必要性も高まる。また個人データが自動的に取扱われる場合に、よりその必要性が高まる。

コード化され保存される情報は、コンピュータ技術の利用によってのみ解読でき（intelligible）、限られた人によってのみ解釈される事実は、この認定とは関係がない。

最終段階で特定の人物または通信内容が分析官によって分析される段階では、保護措置の必要性は最大になる（330 項）。

裁判所は干渉についてのこの理解に基づいて、8 条(4)の評価を行うと述べている（331 項）。これによる評価に従った審理によって、バルク通信傍受の必要性は認めつつ、エンド・ツー・エンドの保護措置がないことを理由に、4.1.3 で述べたような判断を行っている。

8.4.3 IPA2016 における各段階における保護措置

2.3(3)において述べたように、 IPA には多くの保護措置規定が置かれている。段階区分は、Big Brother Watch 判決の区分とは異なるが、以下のような保護措置規定がある。

そのうち情報収集段階の規定が圧倒的に多いが、検証段階、保存・破棄段階、開示・配布段階において以下のような保護措置規定がある。

・検証段階：6 編 1 章；152 条・155 条、6 編 2 章：172 条・173 条、6 編 3 章；193 条・196 条、7 編；221 条・222 条・224 条
・保存・破棄段階：5 編；92 条・129 条、6 編 2 章；171 条、6 編 3 章；191 条、7 編；223 条
・開示・配布段階：2 編；57 条・58 条・59 条、5 編；129 条・132 条・133 条・134 条、6 編 2 章；171 条・174 条、6 編 3 章；191 条

このそれぞれの段階における保護措置について以下考察する。

(1) 収集段階

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、本来的には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ものの、バルク権限自体は認められている。一方米国では、PPD 28 号、2015 年米国自由法、大統領令 14086 号においては、バルク・データ収集が大きく制限されるようになった。

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 下院の調査権限法案の審議において、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）は、莫大な量の個人情報の収集がプライバシーに影響することを認めながらも、コンピュータの自動化によりプライバシーが侵されたことにはならないので、プライバシーの問題は生じないという。」、また「スタンス（William J. Stuntz）のように、プライバシー権が問題になるのは公開の場面であって、収集の段階では問題にならないという見解もある。[93]」

しかしながら、仮に収集段階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と考えられる。

---

93 出典：大林啓吾[2015]『憲法とリスク』p199。原典は、Richard A. Posner “Our Domestic Intelligence Crisis” Wash. Post. Dec.21, 2005. At A31. William J. Stuntz “Secret Service: Against Privacy and Transparency, New Republic 12(Apr. 17, 2006) なお Richard A. Posner は 1981 年から 2017 年まで米国連邦第 7 控訴審判事。「法と経済学」の研究で著名である。

(2) 検証段階

この段階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) 保存段階・破棄段階

保存されているまたは破棄すべきデータに対する、サイバー攻撃、内部者の情報持ち出しおよび不適切な管理による情報漏洩リスクが考えられる。

(4) 開示・配布段階

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。

以上各段階におけるプライバシー侵害リスクを述べてきたが、各段階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ある。

8.4.4 各段階におけるプライバシー侵害リスクと保護措置規定

米国ではプライバシーと市民的自由と、英国ではプライバシーの用語で議論が行われている。大林啓吾は以下のように説明している[94]。

> 政府による監視の問題は、令状との関係が問題視されることから、修正 4 条に基づく主として令状主義の問題に収斂される可能性が高い。さらに自由な情報流通を阻害しかねないプライバシー権よりも、表現の自由の問題として構成した方が自由な表現空間を狭めなくてすむ。

国の機関による個人データの収集、検証、保存・破棄、開示・配布の各段階におけるプライバシー侵害リスクが存在することを考えると、この説明による米国のアプローチは収集段階の保護に偏重しているように考えられる。

IPA では 8.4.3 で述べたように、各段階において保護措置が規定されている。

---

[94] 大林、前掲注 93　p191

この問題に関してダニエル・ソローヴは、プライバシー侵害の多元性を理解するために、情報収集、情報処理、情報拡散、侵襲の 4 つの類型を提示して、各類型におけるプライバシー侵害リスクについて分析している[95]。

このソローヴのアプローチも、プライバシー侵害リスクを収集段階だけではなく、各段階で分析することの必要性を示していると考えられる。

8.5 EU 法における人権制約およびその限界に関する規定

EU 法には、人権制約を認める規定がある。しかしその人権制約には限度があることも規定されている。また欧州人権条約にも人権制約を認める規定がある。

（1）基本権憲章 52 条（Scope of guaranteed rights）

本条ではこの基本権憲章で認められている権利および自由の行使に対する制限は、法によって規定されなければならない。またこれらの権利や自由の本質を尊重しなければならない。

制限は比例性原則に従って、必要であり真に EU 法が認めている一般的利益目的または他の人の権利および自由を守るために限り行うことができる。

この規定は制約を認める一方で、比例性原則を逸脱した制約は認めないとの人権制約の限度も示している規定であると考えられる。

（2）プライバシー・電子通信指令 15 条(1)

この規定は本指令で規定している権利および義務に関して、制約を認める規定である。制約を認める規定は 5 条（通信の秘匿性）、6 条（トラフィックデータ）、8 条（発信者情報）(1)(2)(3)(4)、9 条（位置データ）である。

制約できるのは、国家安全保障、防衛、公共の安全および犯罪の防止、捜査、探知および訴追または電子通信システムの無権限利用に関して、必要であり、適切であり、比例的な手段である場合と規定されている。

また全ての手段は、EU 条約 6 条(1)(2)の規定を含め EU 法の一般原則に従ってなされるものとする。

この規定においても、指令が規定する保護を制約することを認めるとともに、制約の限度も示している規定と考えられる。

（3）GDPR23 条

「（前略）EU 法または加盟国の国内法は、その制限が基本的な権利及び自由

---

[95] 出典：ダニエル J. ソローヴ[2013]「第 5 章プライバシーの類型論」『プライバシーの新理論』

の本質的な部分を尊重するものであり、かつ、以下の対象を保護するために民主主義社会において必要かつ比例的な措置である場合、第 12 条から第 22 条に定める権利及び義務に対応するそれらの法律の条項範囲内で立法措置によって、第 12 条から第 22 条および第 34 条並びに第 5 条で定める義務及び権利の適用範囲を制限できる[96]」として、国家安全保障、防衛、公共の安全への脅威からの保護及びその防止を含め、犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行を理由とした制限を認める規定を置いている。

この規定も、国家安全保障や犯罪などを理由とする制約を立法によって行うことを認めているが、その制限が基本的な権利及び自由の本質的な部分を尊重するものであり、かつ必要であり比例的な措置であることを限度としていると考えられる。

（4）欧州人権条約 8 条（私生活及び家族生活の尊重についての権利）

本条では 1 項で私的及び家族生活、住居及び通信の尊重の権利を有すると規定しているが、2 項においてその制約される場合も次のように規定している。

「この権利の行使については、法律に基づき、かつ、国の安全、公共の安全若しくは犯罪の防止のため、健康若しくは道徳の保護のため、又は他の者の権利及び自由の保護のため民主主義社会において必要なもの以外のいかなる公の機関による干渉もあってはならない[97]。」

この 8 条においても 1 項で保障している権利を、2 項で制限できる理由を列挙しているが、制限の限度に関する規定はない。

但し人権条約 1 章が人権尊重義務、2 章が欧州人権裁判所、3 章雑則から構成されていることから考えても、人権制約について制限がないことを意味しないものと考えられる。

8.6　IPA2016 における調査権限とプライバシー保護の両立を図る規定

IPA2016 2 条（一般的保護義務）では、令状等の発出時にプライバシーに配慮するとともに、調査権限の必要性にも配慮すべきことを規定している。

また新設された司法コミッショナーが令状等の発出に関して事前承認審査をする場合に、令状等の発出根拠に必要性と比例性があるか、裁判所の司法審査と同じ原則を適用すること、2 条の義務の遵守に関して十分な配意をすることが規定されている（23 条など）

---

[96] 日本語訳は、個人情報保護委員会の仮訳による。

[97] 日本語訳は、『ベーシック条約集 2023』による。

さらに司法コミッショナーは、国家安全保障など令状発出の根拠・理由に関して公益に反する行動を取らないことが、229 条(6)に規定されている。

また 229 条(7)では以下の行動を取らない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、各省庁または軍隊の運用の有効性を不当に害すること

これらの規定も、調査権限行使とプライバシーの両立を求めている規定と考えられる。

8.7　調査権限の必要性と人権保障に関する基本的考え方

これについては、2014 年 1 月の PPD28 号発出時にオバマ大統領が述べた以下のことが基本であるように考えられる。

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 以降突然従来以上の役割を果たすことが必要となった。
② 現実の新たな脅威への対処において、政府の行き過ぎのリスクや核心的な自由の一部を失う可能性を、指摘されることが多くなった。
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。技術が法よりも進歩が速い場合は、とりわけ大きくなる。このため自由・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になる。
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。何故ならこの信頼は、歴史上数多く破られているからである。我々の自由は権力者の良き意図（good intention）に頼ることはできない。我々の自由は、権力者を制約する法律を頼りにしている[98]。

8.8　明確かつ詳細なルール

EU 司法裁判所判決において、無効または違法判決と判断した理由で共通しているのは、（人権制約に関して）明確かつ詳細なルールが定められていないということである。

明確かつ詳細なルールを定める意義としては、8.1.6(3)で述べたように、調査

---

[98] 出典：“Remarks by the President on Review of Signaling Intelligence” Department of Justice, January 17, 2014

権限の内容と権限に対する制約を規定するとともに、調査権限に関する保護措置、監督の仕組みおよび調査権限行使によって人権が不当に侵害されたと考える個人への救済の仕組みを規定することで、人権保障に資するからであると考えられる。

調査権限を行使する機関にとっては、明確かつ詳細なルールがあれば、これを遵守することで、人権制約の限度を超えた調査権限の行使を避けることできると考えられる。

また調査権限の対象となる側からは、調査権限が適正に行使されているかが判断しやすくなり、濫用・誤用に対する救済が求めやすくなると考えられる。

8.9 EU 司法裁判所の Schrems I および Schrems II 判決と IPA2016

Schrems I 判決を受けての EU-米国間の見直し交渉においては、米国法の個人データ移転に関する規定の見直しとともに、バルク・データ収集に関する PPD28 号、米国自由法によって、制限・縮小する見直しが行われた。

これらの見直しを行ったものの、Schrems II 判決では米国の公的機関による米国に移転された EU 市民の個人データへのアクセス・利用に関して、EU 法と本質的に同等の保護水準にないことを理由に、無効と判決された。

これを受けての EU-米国間の見直し交渉においては、オンブズパーソンに代わり 2 層の救済の仕組みとともに大統領令 14086 号で見直されたバルク・データ収集の規定が盛り込まれている。

EU 司法裁判所の「本質的に同等ではない」との判断は、バルク収集自体が問題であるというよりも、バルク・データ収集を行う監視プログラムの実施に制約がなく、米国法における国の機関による個人データへのアクセス・利用に関する権限の制限、保護措置、監督・救済の仕組みの規定が不十分であるとの理由によるものではないかと考えられる。

一方英国の IPA2016 では、バルク権限は縮小されていない。3.2.2 で述べた Liberty 判決においては、IPA2016 4 編の規定は一般的かつ無差別な通信データの取得の規定ではなく、必要性および比例性原則に従っているとされている。

人権制約をする場合であっても、濫用・誤用防止を含む適正執行を行うために、明確かつ詳細なルールを透明性もって設定することが、どのような人権制約がなされるか、その制約が必要性と比例性に沿ったものであるかを判断することに役立つので、極めて重要なことではないかと考えられる。

この検討に当たっては、どのような場合に人権制約が認められるかについての基本論[99]を踏まえて、詳細な制度設計が求められると考えられる。

---

[99] 数多くの文献がある。例えば、吉田俊弘・横大道聡「いつ人権の制約は正当化されるの

9　自由と安全

2001 年 9 月 11 日の米国同時多発テロ発生を契機として、欧米各国でテロ対策法が相次いで制定された。この法律には人権を制約する規定が含まれていたため、自由と安全の問題として多くの議論が行われた。

本稿の終わりに、この自由と安全の枠組みに基づいて、調査権限の人権制約の許容性について考察してみたい。

9.1 国家安全保障概念

本稿では IPA2016 を始めとする法律や司法判断で、国家安全保障という用語が数多く登場しているが、ここで改めて国家安全保障とはどういう概念かについて考えてみたい。

「安全保障の概念には一定の曖昧さと変容がつきものである一方、一貫して正当化作用が潜んでいる。例えば、一般には政治家や官僚がこれは国の安全保障に関わることだと言明するとき、それはそれ以上の議論を許さない、実行するしかないとの響きをもつ。」

その理由として、「国家こそが個々の構成員のために内外にまたがり安全を保障するのだとイメージされる。それゆえ、国家安全保障は錦の御旗となりがちなのである[100]。」との指摘がある。

小林は、国家安全保障とは伝統的には、『「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」[101]』と述べている。この定義は軍事力に焦点を充てた定義であるように考えられる。

これに対して、冷戦時に米国で提唱された DIME モデルによって、安全保障が語られることがある。兼原信克は、安全保障の判断は、D（Diplomacy）、I

（上）（下）」法学教室 2019 年 3～4 月号、No.462~463、高橋和之「人権論の論証構造-「人権の正当化」論と「人権制限の正当化」論（1）~(3)」ジュリスト 2011.4.15-6.1、No.1421-1423、山本龍彦「三段階審査・制度準拠審査の可能性」法律時報 82 巻 10 号（2010 年 10 月号）、内野正幸[1995]「第 2 章 国益は人権の制約を正当化する」長谷部恭男編著『現代の憲法』、曽我部真裕[2013] 「人権の制約・限界」南野森編著『憲法学の世界』、松本和彦[2023]「第 3 章 三段階審査の手法」渡辺康行・宍戸常寿・松本和彦・工藤達朗『憲法 I［第 2 版]』、宍戸常寿[2014] 「4 憲法上の権利の制約、5 目的・手段審査」『憲法の解釈論と応用と展開』、小山剛[2016] 『「憲法上の権利」の作法 第 3 版』

[100] 出典:遠藤誠治・遠藤乾[2014]『シリーズ 日本の安全保障 I 安全保障とは何か』pp37~38

[101] 出典：小林、前掲注 14 p9

（Information）、M（Military）および E（Economy）を総合判断することであるとしている[102]。

DIME の 4 つの要素は国力（National Power）のインプットであるが、現在では国の強さと機会（strength and opportunities）をより良く表すには、DIME より拡大し、S（Scientific and Technological）、E（Environmental）および L（Legal and Law Enforcement）を加えた DIME SEL モデルも提唱されている[103]。

ちなみに 2022 年 12 月 16 日に閣議決定された「国家安全保障戦略」 では、「統合的な国力の要素」として、外交力、防衛力、経済力、技術力および情報力を挙げている[104]。

但しこの情報力は、戦略的コミュニケーションのことではなく、1.3.3 調査権限で述べた、インテリジェンスのことではないかと考えられる。

「安全保障とは、「何が（主体）」、「何を（価値）」、「何によって（手段）」守るかという問題をめぐる概念である[105]。」との概念設定によると、安全保障は国家（主体）が、国民の生命・財産、領域（領土、領海、領空）、主権（価値）を DIME SEL（手段）によって守ることになると考えられる。

但しこの安全保障の定義では、どのような脅威から守るのか、および安全保障が自由、平等などの他の価値に対してどの程度優先されるべきなのかについては定義していない。この点については、自由と安全の問題として本稿が述べてい

---

[102] 兼原はこの I は戦略的コミュニケーションであり、国民を説得し団結を訴えると同時に、国際社会に対して日本に理があることを説得することであると述べている。出典 : 兼原信克[2021]『安全保障戦略』pp68-74 。また兼原は「シビリアンコントロールとは、安全保障に関して、政府の最高レベルで「DIME」を総合判断できるということである。」と述べている。また戦略的コミュニケーションは、「長期的には、自分の価値を推進し、敵対者を抑止するための戦略ナラティブの構築と、それを可能とする情報環境の創出が優先事項である。

また偽情報の拡散、諜報活動と浸透工作、法律戦、サイバー戦、軍事力の行使あるいは威嚇による強要などの影響工作からの防衛にも、戦略的コミュニケーションの視点が有用である」との指摘がある。出典：青井千由紀[2022]『戦略的コミュニケーションと国際政治』pp189-198

[103] 出典：Konstantin Khomko [2019] “A Nation Needs More than a DIME” 筆者はオーストラリア空軍将校でパイロットである。

[104] 出典：「国家安全保障戦略について」[令和 4 年 12 月 16 日国家安全保障会議決定、閣議決定]pp11-12

[105] 出典：高橋杉雄『「安全保障」概念の明確化とその再構築』『防衛研究所紀要』第 1 巻 1 号（1998 年 6 月）p140

る問題である[106]。

9.2 自由と安全の関係

9.2.1 調査権限の人権制約

本稿は IPA2016 を中心として調査権限の内容、行使に当たっての保護措置、行使に関する事前承認を含めた監督の仕組み、および権利侵害を受けたとする人への救済の仕組みについて分析を行い、司法判断を参照しつつ、調査権限の行使に関する人権制約が、どこまで許容されるかについて探ってきた。

ここで改めて二項対立とも考えられている自由（人権）と安全の[107]関係について考えてみたい。

安全を優先する人権制約が認められないケースとしては、、調査権限規定そのものが人権保障に関して不十分である場合と、調査権限は必要かつ正当であるとしても、行使されるときに濫用・誤用される場合の 2 つが考えらえる。

司法判断では、安全保障の確保および重大犯罪との戦いを目的とする調査権限の必要性・正当性が認められる一方で、人権保障が不十分であるとの判断で無効・違法判決が下されている。

この不十分とされた理由としては、これまで分析してきたように、データ保存が一般的かつ無差別であることおよびその保存期間が一律に定められていること、国の機関の保存データへのアクセス目的が重大犯罪に限定されていないこと、裁判所または独立行政機関の事前承認を得ていないこと、濫用の可能性のあるバルク通信傍受についてはエンド・ツー・エンドの保護措置規定がない、などが挙げられている。

すなわち人権保障に関して、調査権限の範囲や行使目的に関する制限、行使に対する監督の仕組み、データを取得してから当該データの管理などに着目して、調査権限の規定の人権保障が不十分であるとされたものである。

一方で濫用に関しては、大統領令 14086 号 2 条（ⅱ）禁止される目的として、批判、異議、考えおよび政治的意見の自由な表現への抑圧、正当なプライバシーの利益への抑圧・制限などが列挙されている。この目的によるシギントを行うこ

---

[106] どの程度安全を保障するのかの問題については、遠藤・遠藤 前掲注 100　pp48~50 参照。

[107] 基本権憲章 2 条には生命の権利（Right to Life）、6 条には自由と安全の権利（Right to Liberty and Security）の規定がある。また人権条約 2 条にも生命の権利、5 条の自由と安全の権利の規定がある。

とは、濫用に該当すると考えられる。

また 8.7 でオバマ大統領は、収集したデータを歴史上濫用した例が多くあると述べている。従ってこの濫用を防止するための監督・監視の仕組みを作り、機能させることが、民主主義および人権を守るために極めて重要であると考えられる。

なお調査権限行使における濫用・誤用に対して救済を求める判決は、本稿では取り上げることができなかった。

9.2.2 司法判断の背景にある自由と安全

司法判断で調査権限の必要性・正当性が認められている背景としては、ヨーロッパは数多くの戦争において、また第 1 次および第 2 次大戦において多くの犠牲者を出し、戦後の冷戦時には核の恐怖のもと NATO とワルシャワ条約機構が対峙した歴史があって、安全保障に対する緊迫感があると考えられる。

一方で戦後まもなく締結された欧州人権条約前文には、正義と平和の基礎である人権と基本的自由について、一方には効果的な政治的民主主義、他方には人権についての共通の理解と遵守に対する深遠な信念を再確認すると述べられている。

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ば、民主主義国家の正当性が失われる。

しかし国家安全保障の目的の一つは、国民の生命・財産を守ることであるので、民主主義国家では国家対国民の対立という構図で、この自由と安全の問題を考えることは不適当である。

この難問について、辻貴則は「安全のなかの自由の法理」の概念に言及しつつ、次のように述べている[108]。

> この法理では安全は自由の条件であり、自由は安全の目的として重要である。当該法理は安全のための規制による自由の犠牲の許容という論理にとどまるものではなく、自由の重要性を前提としたうえで、市民生活における自由と安全の緊張関係を表現したもの。安全法制は自由と法益の保護に貢献するものでありながら、それが強化されすぎたり濫用されたりすると、逆に自由や法益を脅かしかねないので、より成熟した安全法制という難問にきちんと向き合わなければならない。

---

[108] 出典：辻貴則[2017]「第 8 章日本 各論わが国のテロ対策の現状と今後の展開」大沢秀介・新井誠・横大道聡編著『変容するテロリズムと法』

この法理によれば、人権は調査権限が保障すべき価値である、と認識することが重要である。この認識に基づいて、人権制約の許容度なり限界を探っていくことが、民主主義社会にとって極めて重要であると考えられる。

9.2.3 自由と安全の優先度

前 9.2.2 において安全は自由の（前提）条件であり、自由は安全の目的であると述べた。

自由の保障は民主主義社会の根本であり、仮に制約するとしても、制約は最小限かつ期間限定でなければならないと考えられる。すなわち自由を制約する場合には、その制約については他の手段がないこと、および脅威の存在とその急迫性を自由を制約する側が挙証する責任があるように考えられる。

上記の論は La Quadrature du Nez 判決において、「国家安全保障目的で電子通信事業者に対して、トラフィックおよび位置データの一般的かつ無差別な保存を求めることは、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、このような裁判所または独立行政機関による決定が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、およびその指示が真に必要である期間にのみ限定されている場合は許される。」と判示されていることと、整合的ではないかと考えられる。

また自由の制約は 9.1 で引用したように、「安全保障概念には、一貫して正当化作用が潜んでいる。」ので、8.7 でオバマ大統領が指摘している濫用のリスクもそれだけ大きくなる。

従って自由の制約については、上記のリスクを考慮して、調査権限についても 8.3 で述べた調査権限の適正執行に関して、濫用・誤用を含む人権保障の絶えざる検証が必要であると考えられる。

なお 8.3 調査権限の適正執行を確保する課題で述べた、監督・統制の仕組みのうち、行政、議会および司法のどの手法を用いるのかも検討が必要である。

9.2.4 自由（人権）を制約すると安全は高まるか

もう一つの問題として、調査権限が必要であり正当だとしても、人権制約を認めるだけでは、安全は高まらないことを認識すべきと考えられる。

というのも本来の行使目的である国家安全保障や重大犯罪との戦いに関して、調査権限を効果的・効率的に行使することによって、安全が高まるからである。

従って「安全のなかの自由の法理」における安全と自由の相互関係の理解に基づき、法制度整備および調査権限の行使を行うことが肝要であると考えられる。

調査権限の目的に対して整合的な法制度整備に関しては迅速性が、また人権

制約に関しては透明性が求められると考えられる。

9.3 プライバシーの価値[109]とは

（1）ダニエル・J・ソローヴの問題提起

ここまで自由と安全の問題を述べてきたが、ソローヴはこの自由のなかでプライバシーの価値について、個人的権利であることに留まらず、社会的価値を有するものとして再構築することで、プライバシーが「犯罪の検知・予防や国家安全保障のようなほかの価値とも衝突する」問題に対処することを提唱している。

ソローヴは、「プライバシーを個人的権利とみなす」ため、「対立する諸価値と重みを比較する際に、その社会的価値という点で考えられることが多い」ため、「プライバシーが軽んじられる。」、「またプライバシーと安全は共に必要不可欠な利益であり、両者の衡量方法は自由と民主主義の基盤そのものに影響する」と述べている。

（2）プライバシーの価値の基礎理論

プライバシーの価値の説明方法として、非帰結主義的説明と、プラグマティズム的説明があるが、ソローヴは後者を支持している。この説明方法とは、「対立する価値とプライバシーとの比較衡量」のことであるが、「可能の限り厳密かつ思慮に富むプロセスとすること」が挑戦すべき課題であると述べている。

比較衡量という手法は、「その場しのぎで安易だという強い批判にさらされてきた」ので、この批判に応えようとするものであると考えられる。

ソローヴは解明すべき課題とは、「個人に対するある種の危害を救済することがどうして社会にとって利益があるかを証明する」、「プライバシーは個人間の関係も防衛するが、個人間の関係は家族生活や社会参画、政治活動に必要不可欠な本質的なものである」と述べている。

このソローヴのプライバシーの社会的価値論を、どう現実の自由と安全の問題に生かしていくか、具体的な展開が期待される。

9.4 脅威の増大

IPA2016 でも調査権限として認められている通信傍受、通信データ取得、機器干渉が、安全保障や重大犯罪との戦いにおいて重要になっているのは、以下の事情もある。

---

[109] ここでの論議は、以下の文献に基づいている。ダニエル・J・ソローヴ[2013]「4 プライバシーの価値」『プライバシーの新理論』、ソローヴ[2017]『プライバシーなんていらない？情報社会における自由と安全』

① 国家安全保障上、インターネット空間を通しての脅威が増大してきたので、その脅威をインターネット空間で探知・把握する必要性が高まっている。

ロシアのウクライナ侵攻では、サイバー攻撃が先行してから、実空間への攻撃・侵入が行われた。これには将来的な攻撃準備として、重要インフラなどへのゼロデイ攻撃ウイルスの埋込みも含まれる。

さらには軍の指揮命令系統への攻撃もサイバー空間において行われていて、これが阻害されると、国家安全保障上重大な結果を招くことになる。

また偽情報の流通などいわゆる影響力工作としての利用も多くなっている。

② インターネット空間を通しての脅威が高まっているのは、経済社会活動がインターネットに多く依存して行われるようになっていて、その可用性が失われると極めて大きな悪影響が生ずるからである。

③ また大量の機密情報・個人情報が流通し、保存されているため、それらの情報の窃取を狙った攻撃や、故意または過失による情報漏洩が発生しやすくなっている。このためインターネットに保存されている情報管理が、より重要になっている。

④ 国家または国家の支援を受けた集団によるサイバー攻撃が激化して、欧米日において、機密情報・個人情報の流出、IT システムや重要インフラの可用性喪失が多発している。これはインターネットを利用した安全保障阻害行為や重大犯罪行為自体が増大していることを意味している。

⑤ 国家安全保障を脅かす敵対的行動を取る者や重大犯罪を企てる者も、このインターネットを利用していて、これを探知・把握することが国家安全保障や重大犯罪との戦いにとって有力なツールになる。

このような背景によって、サイバーセキュリティが国家安全保障により近接する状況が生まれている。

9.5「通信の秘密」における自由と安全

電話時代には電気通信事業者は自己が取扱う通信について、hands-off が求められ「通信の秘密」は厳守されていた。

これに対してインターネットは、表現メディアとしては発信者情報開示[110]などへの関与が求められ、また通信メディアとしてはサイバー攻撃への対処のための関与が認められるようになってきて、「通信の秘密」の保障を制限する事例

---

110 「プロバイダー責任制限法」により規定されているが、この改正案が、第 213 回国会に提出されている。法律名も「特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律」に変更提案されている。この法律の略称は「情プラ法」。

が多くなっている。

「通信の秘密」は憲法上自由権の一つであり、その保護法益はプライバシーと表現の自由であるとされている[111]。

また電気通信事業法においては、通信が知らないところで知得されないとの当事者の期待を保護するとの「通信の秘密」の本来の法益保護に加えて、重要インフラとしての通信システムの機能維持が保護法益であると考えられる。

この背景としては、9.3 で述べたように国家安全保障上、インターネットの正常な維持運営の確保がより重要性を増しているとの事情も加わっている。

インターネットの正常な維持運営を確保するために、関係 5 団体による「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」が公表されている[112]。

自由と安全の相互関係の視点からみると、「通信の秘密」の前提であるインターネットの安全を守るために、自由（「通信の秘密」）を制限するとの構図になっている。

但し「通信の秘密」を制限する場合であっても、これまで分析してきたように、恣意的運用ないし濫用防止の観点からは、制限に関する法的根拠、制限の範囲、保護措置、監督、救済の仕組みに関する明確かつ詳細なルールを透明性をもって設定することが極めて重要である。

安全は自由の（前提）条件であり、自由は安全の目的であるとの相互関係にあることから、明確かつ詳細なルールに基づいて、安全のために「通信の秘密」を制限することが、「通信の秘密」を守ることにもなると考えられる[113]。

---

[111] 鈴木秀美は保護法益は両方であるとしつつも、プライバシー保護に重点を置く学説が多いとしている。出典：鈴木秀美「通信の秘密」大石眞・石川健司編『憲法の争点』Jurist 増刊 2008 年 12 月 15 日号 p136

[112] このガイドラインでは、サイバー攻撃等への対処のために、一定の場合に「通信の秘密」の制限が認められている。しかし電気通信事業法には、「通信の秘密」の制限を認める場合の規定はない。ガイドラインの規定のみを根拠に「通信の秘密」の制限を認めることは、法律の留保の原則からは疑問が残る。

[113] この 9.4 の記述については、以下の文献を参照。田川義博「サイバーセキュリティからみた『通信の秘密』情報セキュリティ総合科学第 13 号、2021 年 11 月、情報セキュリティ大学院大学紀要

（別紙）

調査権限（ガバメント・アクセス）に関する動向と司法判断の時系列

年	英国、EU、米国の動向	司法判断
2000 年	欧州委員会のセーフハーバー決定	
2001 年	米国 9.11 同時多発テロ	
2006 年	EU データ保存指令	
2013 年	エドワード・スノーデンの NSA 秘密文書暴露	
2014 年	米国 PPD28 号発出 英国 DRIPA2014 成立	EU 司法裁判所の EU データ保存指令判決
2015 年	米国自由法 2015 成立	EU 司法裁判所のセーフハーバー（Schrems Ⅰ）判決
2016 年	米国司法救済法成立 欧州委員会のプライバシー・シールド実施決定 英国 IPA2016 成立	EU 司法裁判所の DRIPA2014 判決
2018 年	IPA2018 の Regulation による改正	英国国内裁判所の Liberty 判決
2020 年	英国の EU に対する十分性認定	EU 司法裁判所のプライバシー・シールド判決、Privacy International 判決、La Quadrature du Nez 判決
2021 年	欧州委員会の新 SCC 決定、英国に対する GDPR および刑事司法指令に基づく実施決定 英国の新 SCC 決定	欧州人権裁判所の Big Brother Watch 判決
2022 年	米国大統領令 14086 号発出	
2023 年	欧州委員会のデータ・プライバシー・フレームワーク実施決定 英国 IPA(Remedial)Order2023 成立 英国 IPA(Amendment)Bill 議会提出	