

## 先進主要国における通信情報利用の実施過程とその制限・監督

令和6年7月26日

事務局

(内閣官房 サイバー安全保障体制整備準備室)

- 本資料は、先進主要国における通信情報の利用の実施過程（プロセス）及びその制限・監督の仕組みを把握するため、英、独、米、仏、豪の5か国における国家安全保障等の目的のための通信情報の利用を定める法制※について、外国がかかわる通信からの情報収集に関連するものを中心として、主に独立機関による監督に焦点を当てつつ御説明するもの。

※：個別具体的な調査対象を事前に特定せず通信情報を調査できる法的枠組

- 対象とする各国の法制は、それぞれ以下のとおり。



英国 調査権限法（IPA）に基づく海外関連通信※<sup>1</sup>の不特定型利用



ドイツ 連邦情報局法（BND法）に基づく戦略的対外通信偵察※<sup>2</sup>



米国 外国情報監視法（FISA）702条等※<sup>3</sup>に基づく非米国人情報を主な対象とする通信情報利用



フランス 国内治安法典（CSI）に基づく外国通信情報※<sup>1</sup>の国際通信監視



豪州 通信情報傍受及びアクセス法（TIA）に基づく外国通信情報※<sup>1</sup>の利用

※<sup>1</sup>：主に外国・国内間の通信      ※<sup>2</sup>：主に外国・外国間の通信      ※<sup>3</sup>：関連する大統領令（EO）を含む

注）本資料は、公表済みの各国法令の条文を参照し、現時点で判明している法制上の内容をまとめたもの。  
本資料に記載する内容は、各国政府の確認を得たものではなく、各国の法制及び実態の全てを網羅するものでもない。

# 概要

- 先進主要国の法律における通信情報の利用の実施過程については、おおむね共通するものとして、①開始前の準備・承認、②通信事業者への通知・指示等の措置、③受領したデータの処理・分析、④処理・分析した情報の提供・共有等、⑤データ・情報の保存・廃棄の各段階を認めることができるのではないかと。
- これらの各段階について、先進主要国では、独立機関が監督しており、事前の関与及び開始後の実施状況の監視を組み合わせることで統制を図っているものと考えられる。（例外として、豪州は、独立機関が事前審査に関与しない方式となっている。）

主な実施過程及びその内容 (おおむね共通するもの)		独立機関による監督				
		英 	独 	米 	仏 	豪 
準備・承認	○担当大臣による命令の発出 等	事前審査	事前審査	事前審査	意見提出	
通信事業者への措置	○通信事業者に対し、協力義務に基づく通知・指示 ○協力措置に関連する費用の分担 等					
処理・分析	○受領したデータを可能な限り自動化された方法で選別・フィルタリング ○必要性、比例性等を満たす範囲のみで分析を実施 等			申立を受けた場合の審査等		
提供・共有等	○処理・分析した情報の開示及び利用の範囲は、必要最小限に制限 ○刑事手続・訴訟における証拠としての利用の制限 等					
保存・廃棄	○データ・情報は、不要になった場合や保存期間の満了後、直ちに破棄 ○消去・廃棄について記録 等					

※独立機関の主な任務は、政府を監督することであり、通信事業者を直接に監督することではない。 3



○ 英国の独立機関は、事前の審査・承認に加え、実施開始後の継続的な監視のための役割及び権限も付与されている。

## 英国（2016年調査権限法）

組織	担当行政機関 (情報機関)	独立機関 (調査権限コミッショナー事務局 (IPCO) ※1)
準備・承認	<ul style="list-style-type: none"> <li>○運用目的は、あらかじめリストに記載。記載された目的は、<u>国務長官が確認・承認</u>。首相が年1回以上レビュー</li> <li>○担当行政機関の長官は、<u>必要性・比例性を考慮し、国務長官に許可の求め</u></li> <li>○<u>国務長官は、許可の求めを受けて必要性、比例性、公共の利益等を事前審査し、許可証※2発行</u></li> </ul>	<ul style="list-style-type: none"> <li>○事前審査・承認 許可証の目的、比例性、運用目的への合致性等を審査・承認。司法審査に用いられる裁判所と同様の原則を用いる。</li> </ul>
通信事業者への措置	<ul style="list-style-type: none"> <li>○国務長官は、<u>通信事業者等に対し技術協力を義務付ける通知等の発出が可能</u>。発出前に、当該通知がもたらし得る利益、実施の技術的可能性、費用、関係者への影響等を考慮</li> <li>○<u>関連費用の補償</u></li> </ul>	<ul style="list-style-type: none"> <li>○事前審査・承認</li> <li>○継続的な監督                             <ul style="list-style-type: none"> <li>・調査権限の行使について継続的にレビュー</li> <li>・調査、検査、監査の実施権限。装置、システム又はその他の施設若しくはサービスへのアクセスも可能</li> <li>・エラー（誤り）の状況を含む年次報告書を作成し、首相に提出するとともに公表</li> <li>・自らの職務遂行状況について年次報告書を作成、首相に報告</li> <li>・技術諮問委員会を設置。技術動向が調査権限の実行（コミッショナーによるレビューの対象となるもの）にもたらす影響並びにプライバシーへの干渉を最小化するための当該権限の技術の可用性及び発展について助言</li> </ul> </li> </ul>
処理・分析	<ul style="list-style-type: none"> <li>○<u>通信情報を可能な限り自動化された方法で選別</u></li> <li>○<u>分析の制限</u> 許可証記載の運用目的のための必要かつ比例的な範囲に限定、国内通信内容分析の原則禁止 等</li> </ul>	
提供・共有等	<ul style="list-style-type: none"> <li>○<u>利用の制限</u> 開示・利用範囲、開示・利用を許可する者の数等を許可証の目的に照らして<u>必要最小限に制限</u></li> <li>○<u>海外当局への提供の制限</u> 提供先の海外当局において、保存及び開示について英国の保護措置と類似の措置が講じられている旨を国務長官に申請</li> </ul>	
保存・廃棄	<ul style="list-style-type: none"> <li>○<u>不要になった場合は、原則直ちに破棄</u></li> </ul>	

※1 調査権限コミッショナー事務局 (IPCO) は、調査権限コミッショナー及び司法コミッショナーズを支える事務局であり、権限としては、調査権限コミッショナー又は司法コミッショナーがそれぞれに備えるものを行使することとなる。なお、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。（詳細は10ページに記載）

※2 許可証は、令和6年6月20日のテーマ別分科会（田川義博氏説明資料）では「令状」と訳されていたもの。原文（英語）では“Warrant”。大臣が発行。

注) 以上のほか、議会による監督も存在する。また、2016年には、脅威の変化や技術進歩を踏まえ、調査権限の内容・手法が目的にふさわしいもの (fit for purpose)となるよう、調査権限の強化とともに、プライバシーや言論の自由に関する保護措置や監督の仕組みを強化する改正が行われた経緯あり。



- ドイツのBND法は、独立した事前の審査及び継続的な事後監督の両方を備える。
- ドイツ連邦憲法裁判所判決（2020年）で示された通信の秘密との関係で必要とされる考慮要素（次ページの①から⑭まで）がおおよそ含まれていると考えられる。

## ドイツ（連邦情報局法（BND法））

組織	担当行政機関 (連邦情報局 (BND))	独立機関 (独立統制評議会 (UKRat))	
準備・承認	<ul style="list-style-type: none"> <li>○<u>目的・期間等の設定</u> 措置の目的、対象とする危険分野、地理的焦点、期間を限定</li> <li>○<u>長官(又は代理人)が命令</u>。独立機関審査後に実施。(①, ③, ④)</li> </ul>	<ul style="list-style-type: none"> <li>○<u>命令の実施前に、命令の適法性を審査・確認</u>。 <u>適法性が確認されない場合、命令は失効</u></li> </ul> <p>(①, ③, ④)</p>	
通信事業者への措置	<ul style="list-style-type: none"> <li>○<u>協力義務</u> 通信事業者等に対し、連邦首相府の命令により、BNDにおいて通信の監視及び記録が可能となるようにさせる義務を課す。罰金及び補償あり</li> </ul>	<ul style="list-style-type: none"> <li>○<u>BNDに対する監督の権限</u> <ul style="list-style-type: none"> <li>・文書及びデータの提出要求</li> <li>・事務所への出入り</li> <li>・情報技術システムへのアクセス</li> <li>・職員に対する質問</li> </ul> </li> <li>○<u>違法な状況がある場合、連邦首相府に対して異議申立が可能</u></li> <li>○<u>議会統制委員会※への報告</u> 6か月を超えない間隔で、議会統制委員会に活動状況の定期報告。5年ごとにその統制活動の有効性を評価する報告書を作成し、議会統制委員会に提出 等</li> </ul> <p>(⑬, ⑭)</p>	
処理・分析	<ul style="list-style-type: none"> <li>○<u>各種分析の制限</u> <ul style="list-style-type: none"> <li>・<u>自動フィルタリング技術を技術的に可能な限り利用</u>、自国民の個人データ取扱の原則禁止、コンテンツデータの取得のための適切かつ必要な検索用語の使用、分析により私生活の中核に属すると判明した個人データは直ちに消去、トラフィックデータの分析制限 等 (②, ⑤, ⑦~⑨)</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>○<u>検索用語の適法性の事後確認</u></li> </ul>
提供・共有等	<ul style="list-style-type: none"> <li>○<u>個人データ移転の制限</u> <ul style="list-style-type: none"> <li>・データ主体を保護する利益が移転による一般的利益を上回ると認められる場合等には個人データの移転不可</li> <li>・データの移転先の機関は、BNDから送信される目的のためにのみ個人データを処理可。外国機関等が所定の保証を遵守していない根拠がある場合、移転は実行されない</li> </ul> </li> <li>○提供時、記録・ログデータの保存義務 (⑪, ⑫)</li> </ul>		
保存・廃棄	<ul style="list-style-type: none"> <li>○保存期間満了後、原則、即時かつ不可逆的に削除</li> <li>○データ消去義務及び消去の事実の記録等 (⑥, ⑩)</li> </ul>		

※議会統制委員会 (PKGr) は、連邦情報局を監視する責任を負い、連邦情報局等の情報機関を監督する議会の組織。基本法45d条が根拠。議会統制委員会法により、連邦政府は、情報機関の活動全般及び特に重要な事項に関する包括的な情報を議会統制委員会に提供する義務を負う。同委員会は、その他の事項についても報告を求めることができる。



## 一般要件

「規範明確性(Normenklarheit)／確定性の原則(Bestimmtheitsgrundsatz)を満たす制定法が必要(Rn. 137 f.)」、「(基本権との関係で)比例原則を満たす必要がある(Rn. 141 f.)」

## 外国通信の戦略的監視に係るデータ収集・処理の基準

### 正当化理由

「特に深刻な」侵害の強度(Rn. 146 ff.)に対して…

- ✓ 外国情報収集のための特別な手段(Rn.159)
- ✓ 外国からの国際的次元の危険(国際社会での重大性と外交安保政策上の重要性を伴う)の早期検知という任務(Rn. 163)
- ✓ 運用権限(法執行権限)を持たない当局が実施(Rn. 165)。

2022年1月1日、新たに連邦情報局の技術的監視を包括的に統制する独立統制評議会(Unabhängiger Kontrollrat)設置。

### 制度設計に関する具体的な要件

- ① 取得するデータ量や監視対象とする地理的範囲の制限(Rn. 169)
- ② 国内通信に由来するデータの削除…フィルタリング技術の使用(Rn. 170 f.)
- ③ 監視目的及び得られた情報の利用目的の明確化(Rn. 175 ff.)
- ④ 目的・期間の特定と事前審査…目的には地理的範囲を含む。期間は更新可能。(Rn. 178 f.)
- ⑤ 特定の個人が対象となる場合の制限…ドイツ国民の通信傍受を目的とすることは原則禁止。(Rn. 186)
- ⑥ トラフィックデータ(非コンテンツ)の保持の制限(Rn. 191)
- ⑦ データ分析を管理する基本的枠組みの法定(Rn. 192)
- ⑧ 信頼関係における守秘義務の保護…ジャーナリズム、弁護士の取扱い(Rn. 193 ff.)
- ⑨ 私生活の中核の保護(Rn. 199 ff.)
- ⑩ データの削除義務(Rn. 208 ff.)

### その他の基準

⑪国内でのデータ共有の制限

⑫外国とのデータ共有の制限

⑬透明性、法的保護、監督に関する基準

⑭ 継続的で独立した事前・事後の監督・統制



- 米国では、専門の裁判所である独立機関が事前の審査・承認を行うことが定められており、必要があれば修正指示の上で命令を発出。実施開始後の監視については、申立・報告を受けることによって行う方式。

## 米国 (FISA Sec. 702, 大統領令14086)

組織

担当行政機関  
(司法長官、情報機関)

独立機関  
(外国情報監視裁判所 (FISC))

準備・承認

- 手続きの策定 司法長官及び情報機関長官は、あらかじめ最小化手続\*等の手続及びガイドラインを定める  
\*米国人が対象となることを最小化するための手続
- 事前審査の求め 両長官はFISCに宣誓・証明書提出
- 承認 独立機関の回答を得た後、両長官が共同でその実施につき承認

- 事前審査・継続承認  
最小化手続等について審査し、取得の開始・継続の命令を発出 (要すれば修正指示)

通信事業者への措置

- 通信サービス提供事業者への指示
  - ・従わない場合、独立機関に申立可
  - ・協力する事業者に対する補償

- 申立を受けた場合の審査  
申立内容が合法と判断した場合は、指示を遵守するよう事業者に命令

処理・分析

- 使用・開示の制限 取得した米国人関連情報は、最小化手続に従ってのみ使用・開示可。目的外での使用・開示は原則不可。意図せず収集した米国人に関する通信は、原則直ちに破棄
- 評価・報告 6か月に一度以上、各種手続等の準拠状況を評価、独立機関等に報告。違反についても報告義務

- 報告の提出受理  
定期的な評価・報告及び年次レビューの結果の提出を受ける

提供・共有等

- 刑事手続における使用の制限 米国人関連情報は刑事手続における証拠としての利用不可
- 外国提供時は目的・範囲、及ぼす影響等を考慮

保存・廃棄

—

\*以上のほか、上級裁判所として審査裁判所(FISCR)が存在し、上訴可能。また、議会による監視メカニズムも存在。7

## 4 フランス

- フランスでは、独立機関が事前審査を行って意見を述べ、この意見を踏まえて首相が許可を決定する。また、独立機関には、実施開始後の監督機能・調査権限も付与されている。

### フランス（国内治安法典（CSI））

組織	担当行政機関 (情報専門機関)	独立機関 (国家情報技術監視委員会 (CNCTR))
準備・承認	<ul style="list-style-type: none"> <li>○首相は、取得を許可する通信回線を指定</li> <li>○首相は、関係大臣の情報利用の要求を受けた場合、<u>独立機関の意見を踏まえつつ、許可</u></li> </ul>	<ul style="list-style-type: none"> <li>○関係大臣から要求を受けた場合、<u>原則24時間以内に首相に意見を提出</u></li> </ul>
通信事業者への措置	<ul style="list-style-type: none"> <li>○情報利用のための協力措置</li> <li>○対応するために生じた特定可能かつ具体的な追加費用は、<u>国が金銭的に補償</u></li> </ul>	<ul style="list-style-type: none"> <li>○<u>監督、情報・証拠の調査権限</u> 抜粋、記録簿、収集された情報、写し、抽出物、送信物、これらの情報が集中管理されている施設等及び情報技術的能力に関する研究等のために保存された情報に対し恒久的・完全かつ直接のアクセス。任務遂行に必要な全ての情報を首相に要請可。首相に対する情報専門機関等の監査報告書の提供要請</li> <li>○<u>勧告</u> 首相又は担当大臣及び関係機関に対し、所定条件下で、情報技術の使用を中止するとともに、収集情報の破棄を勧告可能。首相は遅滞なく委員会に対応を通知</li> <li>○<u>報告書の作成</u> 国防上の秘密・実施手順又は実施方法を守秘した上で、所定の項目の件数を含む委員会の公的報告書を作成</li> <li>○委員及び職員に対する守秘義務</li> <li>○委員会の業務は国防秘として取扱い</li> <li>○申立てがあった場合の検査(あらゆる者が申立可)等</li> </ul>
処理・分析	<ul style="list-style-type: none"> <li>○<u>仏国内の者の通信情報の原則破棄</u></li> <li>○<u>複写・抽出の記録は、独立機関が利用できるようにする義務</u></li> </ul>	
提供・共有等	<ul style="list-style-type: none"> <li>○<u>原則、許可において指定された情報専門機関が使用</u>。ただし、一定条件下では、複製・抽出情報を他情報専門機関又は政令で定められた非情報専門機関に伝達可</li> <li>○目的外送信等の場合、首相の事前許可が必要</li> <li>○伝達の記録を独立機関が利用可能とする措置等</li> </ul>	
保存・廃棄	<ul style="list-style-type: none"> <li>○保存可能期間は、最長で6年。通信は使用日から12か月又は収集日から最長4年後、また、接続データについては収集日から6年後に破棄。ただし、サイバー攻撃の要素を含み、かつ、技術的分析のために厳に必要な範囲内の暗号化された情報及び関連する復号化情報は、これを超えて保存可</li> <li>○「国家の基本的利益」のために保存する必要が解消次第、直ちに破棄。</li> </ul>	

※以上のほか、議会による監視メカニズムも存在。

○ 豪州では、実施開始後の監督・調査権限が独立機関に付与されている。（独立機関は、事前審査には関与しない。）

豪州（通信（傍受及びアクセス）法（TIA法）及びIGIS法）		
組織	担当行政機関 （情報機関）	独立機関 （情報安全保障監察官（IGIS））
準備・承認	<ul style="list-style-type: none"> <li>○外国インテリジェンス情報の取得のための外国との通信の利用について許可証を要請する書面通知を法務大臣に対し発出。国内通信を傍受するリスクの最小化手法を含む通信傍受の方法、他の手段では情報収集できない理由(代替困難性)等を明記</li> <li>○法務大臣は、国防大臣、外務大臣、IGIS及び情報機関長官と協議の上、<u>国内通信の破棄等を確保するための「義務的手続」を発行</u>。これは発行から1年後、以降3年毎に見直し</li> </ul>	(関与なし)
通信事業者への措置	<ul style="list-style-type: none"> <li>○許可証の執行が事業者等による措置を伴う場合、長官は、当該事業者等に許可証が発行されたことを速やかに通知</li> <li>○費用の負担・分担規定</li> </ul>	<ul style="list-style-type: none"> <li>○情報機関の法律遵守、特定の活動の妥当性や情報機関の活動の合法性又は適法性に関する当該情報機関の手続の有効性等の監督と見直しを支援</li> <li>○首相要請に基づく情報機関の監査</li> <li>○情報機関施設への調査・監査</li> <li>○情報機関保有情報・文書への完全かつ自由なアクセス、複製・抜粋</li> <li>○調査を実施し、義務違反又は不正行為の証拠がある場合、当該機関の長に証拠通知</li> <li>○調査完了時には調査報告書案を作成し、調査対象の機関の長に手交。調査対象の機関の長からコメントがあった場合は、これを最終報告書に含める。</li> <li>○年次報告書を作成し、法務大臣等に提出</li> </ul>
処理・分析	<ul style="list-style-type: none"> <li>○許可証で指定された目的と無関係な情報の原則破棄</li> <li>○義務的手続の履行（国内通信の破棄等）</li> </ul>	
提供・共有等	<ul style="list-style-type: none"> <li>○訴訟手続における証拠としての提出は原則不可</li> <li>○許可証の満了又は失効から3か月以内に傍受結果の有用性を法務大臣に報告</li> </ul>	
保存・廃棄	<ul style="list-style-type: none"> <li>○職務遂行若しくは権限行使に関して不要等と認める場合、記録又は複製物を廃棄</li> </ul>	

※以上のほか、議会による監視メカニズムも存在。

○ 英・独ともに、**高い独立性を有する組織を事務局が支える構造**となっている。

	英国の独立機関 (2016年調査権限法)	ドイツの独立機関 (独立統制評議会 (UKRat) (BND法))
組織形態	(調査権限コミッショナー (IPC)) ○体制 1人 ○要件 高位司法職にある者又はあった者	(準司法的統制機関) 事前の審査を主な任務とする。 ○体制 委員6人 ○要件 連邦最高裁等の裁判官としての勤務、長年の経験。 要セキュリティクリアランス
	(司法コミッショナーズ (JCS)) ○体制 内閣総理大臣が職務遂行に必要と認める人数を任命。 現在16人※ <sup>1</sup> (調査権限コミッショナー1人を含む。) ○要件 高位司法職にある者又はあった者	
	(技術諮問委員会 (TAP)) ※ <sup>2</sup> ○体制 調査権限コミッショナーが職務遂行に必要と認める人数を任命 現在6人※ <sup>1</sup> 。技術・政策の専門家、学識経験者等で構成	(行政統制機関) 開始後の監督及び準司法的統制機関を支援を 主な任務とする。 ○体制 定員61人※ <sup>1</sup> ○要件 長官：判事資格 職員：ドイツ国民、要セキュリティクリアランス
	(調査権限コミッショナー事務局 (IPCO)) ○体制 現在は、約150人※ <sup>1</sup> 監察官、審査官、法務官、事務官等から構成	
独立性	○政府から独立して職務執行。 ○内務大臣が財源を拠出するが、内務省の一部ではない。 ○任務遂行に必要な職員・施設・設備等の確保 ○各司法コミッショナーの任期は3年。再選可能 ○法定条件に当たらない限り罷免されない	○連邦の最高機関。BNDの技術情報を統制する独立機関として、 <u>法律のみに従う</u> ○独立した職務執行及び権限行使。指示に拘束されない ○任務遂行のため十分な職員・資源の確保 ○準司法的統制機関の委員の任期は12年。再選は不可
監督の対象	○公的機関による許可証に基づく通信データの取得等の事項に関する 法定機能の行使。取得又は保持された通信データ等の開示、保持 その他の利用に関する機能の行使を含む ○情報機関による不特定型個人データの取得、保持、使用及び開示、 国家安全保障関連通知の発出及び運用 等	○本法により付与された権限に基づくBNDによる技術的偵察及び関連 する送受信並びに協力の適法性

※<sup>1</sup> 人数等のうち法制によらないものについては、各組織のウェブサイト等を参照して作成（令和6年7月時点）

※<sup>2</sup> 技術動向が調査権限の実行（コミッショナーによるレビューの対象となるもの）にもたらす影響並びにプライバシーへの干渉を最小化するための当該権限の技術の可用性及び発展について助言