インターネット時代の「通信の秘密」各国比較

International Comparison of 'Secrecy of Communication' in the Internet Age

2014 年 5 月

情報セキュリティ大学院大学

「インターネットと通信の秘密」研究会

本報告書は、2013 年11 月から2014 年5 月にかけて開催された、「インターネットと通信の秘密」第2期研究会が到達した結論部分を、取りまとめたものである。

取りまとめは、情報セキュリティ大学院大学が、キヤノングローバル戦略研究所の協力を得て行い、研究会には以下の各社（社名のアイウエオ順）が参加した。

NTT コミュニケーションズ（株）、（株）KDDI総研、ソネットエンタテインメント（株）、ニフティ（株）、ビッグローブ（株）、ヤフー（株）。

本件のお問い合わせ先：情報セキュリティ大学院大学、林紘一郎研究室。

〒221-0835 横浜市神奈川区鶴屋町2-14-1

電話＆Fax: 045-410-0222、E メール：hayashi@iisec.ac.jp

Executive Summary

・先進諸国においては「通信の秘密」は基本的人権の一つとして保護され、その侵害に対しては、刑事罰が科せられる。「通信の秘密」の根拠は、プライバシー保護の一環だとする考え方が一般的である。しかしプライバシー保護のあり方については、国ごとに歴史的・文化的な差があるため、保護の仕方や範囲などに微妙な差が生じている。そこで、米国・英国・オーストラリアという英米法系の国と、ドイツ・フランスという大陸法系の国、さらに隣国である韓国を加えて、それぞれの国ごとの実情を調査するとともに横断比較を行って、わが国への教訓を探ることとした。

・「通信の秘密」は絶対的保障を受けるわけではなく、「公共の福祉」の観点から、より高位の法益があれば制限される場合があることは、共通した理解である。わが国も理論的には同じ理解に立っていると思われるが、実際の運用は極めて厳格で、明確な「違法性阻却事由」がない限り「通信の秘密」が守られるとしている点は、先進諸国の間では「保護の程度が高い」類型になろう。「公共の福祉」の観点から、通信傍受などが違法性を阻却されるケースは、大きく分けて (a) 事業者のネットワーク制御に伴うものと、(b) 公権力の関与に伴うもの、に 2 分される。後者はさらに、(b-1) 犯罪捜査に伴うもの、(b-2) 国家安全保障にかかわるもの、に分けられる。

・このうち (a) について本調査では、ISP が関与する以下の 5 つの個別事項に関して、各国での実施状況・法的規定・利用者の同意の 3 点について、調査を行った。①迷惑メールのフィルタリング（ブロッキング）、②帯域制御、③サイバー攻撃などに対する情報セキュリティ対策、④違法コンテンツサイトへのアクセスブロッキング、⑤行動ターゲティング広告。

・その結果、これらの事項は調査対象のいずれの国においても何らかの形で実施されているが、「各国ともほぼ同じようなレベルで実施されているもの」と「実施されているが、ISP が関与する程度が異なるもの」がある。また関与を認める法的根拠や実際の運用についても、必ずしも各国で足並みが揃っているわけではない。

・このように一般的な傾向が明確でない中で、各国の ISP の関与について強いて大きな分類をすれば、EU 型においては「ネットワーク中立性」が重視され、事業者の裁量が制限されているのに対して、アメリカ型ではネットワーク事業者の自由度が高いという対照があるように思われる。なお、ここでネットワーク事業者というのは電気通信事業者に限らず、コンピュータ・サービス提供者を含めた概念であり、後者において営業の自由度が高いのは「インターネット非規制政策」を取ってきた同国の特徴と考えられる。電気通信事業者に限って言えば、アメリカ型でも「ネットワーク中立性」の議論がある。

・(b)に関する部分については、以下のような諸点が注目される。①関与の目的は、犯罪捜査とテロ対策を含む国家安全保障の二つ、②関与の方式としては、現に行われている通信過程に関与する通信傍受と、通信終了後に通信事業者等によって蓄積された情報（保

存資料）へのアクセスの二つ、③関与の対象は、通信内容と、通信内容以外の通信に関わるトラッフィクデータ・通信データ・メタデータ・通信属性と呼ばれる情報および通信自体ではなく加入契約に基づいて得られる加入者情報の三つ、④関与の手続きとしては、裁判所の令状を必要とする司法傍受と行政機関・捜査機関の手続きで良い行政傍受に分かれている。

・(b-1) の犯罪捜査に伴うものに関しては、サイバー犯罪対策で国際条約ができたように、国際的な制度の調整（ハーモナイゼーション）が最も進んでいるが、法制度は現実の各国の風土の中に存在するものだから、傍受に関する社会的受容度によって、実際の運用面ではかなりの差ある。とりわけ「令状主義」を貫徹し司法傍受しか認めないか、一定の条件の下では行政傍受を認めるかは大きな差であり、前者しか認めないわが国は「最も厳格な令状主義」を維持していると考えられる。

・(b-2) の国家安全保障にかかわるものに関しては、各国のナショナル・セキュリティに関する感度（センシビリティ）が反映している。国家安全保障に係るインテリジェンス活動のための公権力の関与は、通信傍受と保存資料へのアクセスの二つがある。また手続き的には司法傍受と行政傍受と呼ばれる二つがある。犯罪捜査の場合とは違って、各国とも裁判所の関与なしで（行政・捜査機関だけの手続きで）傍受や保存資料へのアクセスを認めているが、基本的人権を必要以上に侵害することのないよう、手続き的な担保の規定もおいている。

・とは言うものの、権限が濫用される危険と背中合わせであることに、より配慮しなければならない。いみじくもスノーデン事件で明らかになったように、歯止めのない傍受・アクセスが行われる危険があるからである。各国とも手続き的な工夫に努力しており（特にドイツにおいて顕著かと思われる)、インテリジェンス活動を一切止めよという声は少ないが、人権の保障にはなお努力が求められている。

・各国比較による日本の制度への教訓として、以下のような諸点を引き続き検討すべきかと思われる。①「通信の秘密」を第一義的な問題として論ずることの妥当性（他の視点での検討の方が適している場合があるのではないか)、② 事業者の正当行為（わが国の流儀では「違法性阻却事由」）を予め法定化することの妥当性と、その際に電気通信事業者や ISP の財産権を根拠とすることの妥当性、③ 公権力の関与に関しても、これを法定化することの妥当性。

・また本調査では手が回らなかったが、位置情報など、今後「通信の秘密」との関連で重要度が増すと思われる事項も多い。別途の機会を得て、これらも引き続き検討していきたい。

目次

第 1 部　各国横断比較

2012 年 11 月から 2013 年 5 月にかけて開催された「インターネット時代の『通信の秘密』第 1 期研究会」では、「通信の秘密」の法解釈について歴史的に考察した結果、インターネットが通信の主流になった今日、「通信の秘密」の制度と運用には過剰と空白が生じているとの問題意識をもつに至った。この問題意識をもとに、インターネット時代にふさわしい「通信の秘密」に関する法制度面での検討課題の抽出と、検討の方向性について考察した。

第 2 期研究会では、主要先進国別に調査メンバーを選定し、チームとして各国の「通信の秘密」に関する法制度の横断的調査を行ない、その調査結果を踏まえて日本の「通信の秘密」の法制度の特徴点を抽出するとともに、法制度見直しに関するインプリケーションを得ることを目的としている。

本研究会では、米国、英国、ドイツ、フランス、オーストラリア、韓国の 6 カ国を調査対象国として、(1)「通信の秘密」は憲法・法律レベルでどのように規定されているか、(2)ISP（インターネット・サービスプロバイダ、以下 ISP）等事業者による「通信の秘密」の関与がどのように認められているか、(3)公権力の「通信の秘密」の関与がどのように認められているか、および公権力が関与する場合に、通信事業者なりプロバイダがどのような協力義務を負っているか、の 3 つのテーマについて取り上げた。

日本では「通信の秘密」は憲法 21 条 2 項後段に明文の規定があり、電気通信事業法など法律レベルでも「通信の秘密」の遵守義務と罰則が規定され、また他の法律で遵守義務を制約ないし免責する規定が整備されている。一方調査対象国では、憲法レベルで「通信の秘密」に関して明文の規定を欠いている国があり、法律レベルでも共通性とともに相違性もあることが確認できた。

ただ、憲法レベルで明文の規定がないことが、必ずしも「通信の秘密」の保護の程度が低いことを意味するわけではない。それぞれの国の憲法の仕組み・構成や歴史的な経過が異なるためである。同様に、各国で「通信の秘密」の法制度に共通性と相違性があるのは、通説では「通信の秘密」の保護法益であるとされる「プライバシーの権利」の法概念が、各国によって異なっており、このことが「通信の秘密」の規定に影響を与えているからであると考えられるので、この点に関して若干の考察を行った。

報告書第 1 部においては、各国の「通信の秘密」の法制度に関する共通性と相違性について概観するとともに、日本の法制度へどのようなインプリケーションがあるかについて考察を行った。また各国の「通信の秘密」の規定に影響を与える「プライバシーの権利」に関する試論を付記した。第 2 部においては国別に調査結果が収録されている。

なお、第 1 部の記述については、各論の記述を多く引用しているが、出典はスペースが限られていることから省略し、また具体的な条文などについては、各論を参照願いたい。

第 1 章「通信の秘密」に関する法的規定の横断比較

1　憲法レベルにおける「通信の秘密」に関する法的規定

明文の規定があるのが、ドイツ（基本法 10 条）と韓国（憲法 18 条）である。

これに対して、フランスでは現行憲法にまとまった人権条項はなく、人権保障は憲法院で積み重ねてきた判例と共に、現行憲法前文で言及されている 1789 年のフランス人権宣言等が憲法ブロックと呼ばれ、憲法的な規範とされている。

但し、憲法 66 条には人身の自由の規定があり、憲法院でプライバシー権の保障も含まれているとの判決があるので、「通信の秘密」もここに含まれていると考えることもできるし、ヨーロッパ人権条約 8 条 1 項には、「通信の秘密」に該当する記述がある。

また米国では、「通信の秘密」に関する明文の規定はないが、「通信の秘密」の問題は、憲法上は第 4 修正（修正 4 条）の規定との関連で「通信のプライバシー問題」として論じられてきている。そして、第 4 修正のプライバシー権の保護範囲の主要な判断基準として、「プライバシーの合理的な期待」が多くの判例で採用されている。

英国については、成文憲法がないので、憲法レベルで「通信の秘密」の規定はない。

オーストラリアには成文憲法はあるが、人権規定はない。

注：日本の「通信の秘密」の英語訳は secrecy of communication であるが、調査対象国ではこの用語を使っている国はなく、secrecy of correspondence、confidentiality of communications (information)というような用語が一般的に使われている。なお、日本国憲法で secrecy of communication を「通信の秘密」としているが、もともと communication は会話を含む概念であり、通信と訳したのは誤訳との指摘もある。

2　法律レベルにおける「通信の秘密」に関する法的規定

2.1 「通信の秘密」の遵守に関する法的規定

ドイツでは、電気通信法 88 条で「通信の秘密」の遵守、89 条で「盗聴の禁止」、90 条で「不正利用の禁止」を規定している。加えてプロバイダが必ずしも電気通信事業者であるとは限らないため、テレメディア法において行うサービスの責任を定めている。

韓国では、通信秘密保護法と電気通信事業法および情報通信網利用促進および情報保護に関する法律に、やや幅広い範囲で遵守規定（その例外も規定）がある。

フランスでは、郵便・電子通信法典と国内安全法典に遵守規定（その例外も規定）がある。

米国では、前述したように直接的な「通信の秘密」の規定がないが、連邦通信法における 705 条（通信の無権限な公表禁止）と 222 条 c 項（顧客に関する専属的な網情報[CPNI]の秘密性）、それと電子通信プライバシー法（以下、ECPA）に規定がある。

オーストラリアでは、1997 年電気通信法 276 条等に、通信サービスプロバイダなど主体別に通信内容、通信サービス等の秘密性を保護することを求める規定がある。

なお、上記の「通信の秘密」遵守規定の名宛人については、「何人も」が多いが、ドイツの電気通信法 88 条 2 項で「すべてのサービス提供者」に向けた規定があり、また、米国では連邦通信法 222 条は電気通信事業者が対象となっているなどの例もある。

2.2 「通信の秘密」に対する侵害行為に関する罰則

ドイツでは、刑法 202 条において罰則が規定されており、通信事業者に対しては刑法 206 条 1 項から 3 項において、罰則が加重されている。また電気通信法 148 条でも罰則が規定されており、同法 89 条 2 項では、「すべてのサービス提供者は、電気通信の秘密を維持しなければならない。その義務は、業務終了後も継続する」との規定もある。

フランスでは、刑法典 226-1 条 1 項、226-3 条、226-15 条 1 項に罰則規定があり、事業者に対しては、432-9 条で刑罰加重の規定がある。　韓国では上記の 3 法においてそれぞれ罰則規定がある。また電気通信事業法 83 条 2 項では、電気通信業務に携わっている者または携わった者が、「在職中、通信に関して知った他人の秘密」の漏えいを禁じており、違反行為に対しては同法 94 条 4 号で罰則が規定されている。（日本の電気通信事業法でも他人の秘密の漏えいを禁じているが、これに対する罰則はないとされている。）

米国では、連邦通信法 705 条違反の罰則規定は、一般人が対象であり、事業者も同じ扱いになっている。また連邦通信法 222 条は、電気通信事業者向けの規定であり、同種の義務違反に主体ごとに異なる刑罰を科すというような法構成にはなっていない。

英国では、捜査権限規制法 2000（RIPA、以下 RIPA）において違法傍受についての罰則が定められているが、通信データへの違法アクセスには罰則が定められていない。

オーストラリアでは、刑法典 474.4 条が、傍受装置の製造、広告、販売、所持を違法行為として、罰則を定めている。また、情報漏洩行為については、1997 年電気通信法 276 条以下に事業者ごとに規定され、罰則が定められている。さらに違法通信傍受に関しては、1979 年電気通信（傍受およびアクセス）法 7 条で、その漏えいは 63 条でそれぞれ禁止され、罰則が定められている。

2.3 「通信の秘密」の対象になる「通信」の範囲

「通信の秘密」の対象範囲は、まず「通信内容」があり、またトラッフィクデータ、通信データ、メタデータ、通信属性など、さまざまに呼ばれる「通信内容以外の情報」とに分かれている。

例えばドイツでは、電気通信法 3 条 30 号でトラフィックデータが規定され、96 条 1 項と 113 条 a で具体的にどのような事項がトラッフィクデータに該当するかが規定されている。フランスでは、郵便・電子通信法典 L34 条の 1 において、トラッフィクデータ、通信内容および加入者に関するデータに区別されている。このドイツやフランスの例は、EU のプライバシー・電子通信指令（2002/58/EC）において、confidentiality of communications と traffic data が区分されていることに対応した規定であると考えられる。

また米国では通信内容とそれ以外の情報を区分しているのに対して、オーストラリアの1997年電気通信法では、明確な区分はなされていないようである。

なお、この通信内容と通信内容以外の区分については、公権力の「通信の秘密」への関与において、さまざまに規定されているので、3において改めて取上げる。

第2章　ISP等の事業者の「通信の秘密」への関与に関する法的規定の横断比較

本調査では、ISP等が関与する以下の5つの個別事項に関して、各国での ① 実施状況、② 法的規定、③ 利用者の同意の3点について調査を行った。調査メンバーによる調査に加えて、イギリス、ドイツ、フランス、オーストラリアの調査に関しては、ヤフー社の多大なご協力を得た。同社に感謝申し上げる。

1 迷惑メールのフィルタリング（ブロッキング）

①実施状況については、各国とも実施している。②、③については、以下の通りで若干の違いがあるが、各国とも法的根拠に基づいて実施されている。なお各国とも迷惑メール全般に関する法律があり、ほぼオプトインが採用されている。

	迷惑メールに関する法的規定と利用者の同意
米国	通信傍受法（18USC2511条(2)(a)(i)は、事業者の権利、財産を保護するために社員に通信傍受を認める規定。 ペンレジスター法（18USC3121条(b)は、事業者の権利、財産の保護に加えて、サービスの濫用や違法使用から加入者を保護するために、ペンレジスター（通話を追跡するが、録音はできない装置）の設置を認める規定。 注：ECPA（電子通信プライバシー法）は、三つの部分からなっており、上記の法はいずれもECPAに含まれている法規定である。
英国	通信に関するプライバシー保護に関する基本的な法的枠組みは、データ保護法1998、プライバシー・電子通信指令規則2003（SI2003・2426）（PEC規則）である。 メッセージのメタデータの利用による場合の直接規制法はない。 メッセージ内容の利用による場合は不法の恐れがある。 利用者の同意は不要だが、ブロックされていることは利用者に通

	知されるべき。(Lawful Business Practice Regulation2000 およびデータ保護ルールに規定がある。)
ドイツ	データ保護指令 7 条(b)。国内法では認める具体的規定はない。現在の通説、当局の見解では、受信者の暗黙ないし明確な同意があればよく、送信者の同意は不要とされている。
フランス	データ保護指令 7 条(b) 電子プライバシー法 4 条 CNIL（フランスデータ保護庁）は、利用者にスパムメールフィルターの利用を奨励。またデータ保護法により、この仕組みおよびフィルターを利用しない可能性について、利用者に情報提供すべきとされている。
オーストラリア	Spam Act2003、Spam Regulation2004 サービス提供規約で、スパムメールの排除を予め明示していることが多い。
韓国	情報通信網利用促進法 50 条の 4　第 1 項 利用約款による包括的同意で良い。(同条第 2 項)

注：なお、この迷惑メールのフィルタリング（ブロッキング）は、ISP 以外の e メール
サービス提供事業者も実施している。

2 帯域制御

①の実施状況については、各国とも実施している。ネットワークの管理業務との捉え方が通例のようである。②、③については、以下の通りで若干の違いがある。また、この帯域制御に関しては、「通信の秘密」の問題というよりも、ネットワーク中立性の問題として捉えられている国がある。

	帯域制御に関する法的規定と利用者の同意
米国	通信傍受法(18USC2511 条(2)(a)(i) ペンレジスター法(18USC3121 条(b) 帯域制御はネットワーク中立性の問題として議論されている。
英国	法的な禁止規定はない。電気通信法 2003 の一般条項 9.2(e)によって、公衆電気通信サービス（PECS）を提供しているとされる場合には、利用者へは明確で、理解しやすくかつ容易にアクセスできる方式で情報提供が義務づけられている。
ドイツ	法的に明確な規定はない。EU 委員会はネットワーク中立性を支持しているが、現時点では明確な法的規定はない。国内でも電気通信法 41 条 a でネットワーク中立性保障要件を定める権限が政

	府にはあるが、現時点では立法化されていない。 電気通信法 43 条 a で、明確に、包括的にかつ容易にアクセスできる方式で利用者契約の中で規定することとされている。
フランス	正当な目的で行われる帯域制御は、刑法典 226-15 条の通信の秘密侵害罪の成立要件である悪意が欠けるという前提があると考えられる。帯域制御はネットワーク中立性の問題として議論されているが、ネットワーク中立性は郵便・電子通信法典により法律上の原則とされ、監督機関（ARCEP）がその遵守を監督する。（同法典 L36-6 条）また ARCEP の見解によれば、ネットワークの混雑対策や安全対策のための帯域制御は、対策目的との適合性、有効性、必要最小限性、透明性、差別の禁止の条件のもとで認められる。
オーストラリア	法的規定はない。利用者の個別同意は不要であるが、利用約款のなかで規定されているのが一般的である。
韓国	情報通信網利用促進法 15 条第 3 項、未来創造科学部のガイドラインによって認められている。 利用者の同意は、利用約款による包括同意で良い。但し、ISP がトラッフィク管理に必要な措置を取る場合には、当該利用者に告知が必要。

3 サイバー攻撃などに対する情報セキュリティ対策

①実施状況については、各国とも実施している。②、③については以下の通り若干の違いがある。またこの対策については、帯域制御と同じくネットワーク中立性の問題として捉えられている国がある。

	情報セキュリティ対策に関する法的規定と利用者の同意
米国	通信傍受法(18USC2511 条(2)(a)(i) ペンレジスター法(18USC3121 条(b)
英国	電気通信法 2003 一般契約条項「通信プロバイダにおいてセキュリティまたはインテグリティのインシデント、脅威、脆弱性に対する手法のタイプ」として、利用者への情報提供が求められる。ISP がそのような環境で一方的な行動を取る権利は利用約款で与えられているので、利用者の同意は一般的に求められていない。
ドイツ	電気通信法 109 条 1 節では、ISP は「通信の秘密」の保護対象であるデータ・コンテンツを保護するために十分な技術的

	安全性を保障する義務がある。 同法 100 条では、上記の保護を行うためにトラフィックデータや登録データを収集、処理することを認めている。 データ・コンテンツ保護のためのステップが適切であれば、利用者の同意は不要。
フランス	トラフィックブロッキングは、帯域制御の一つ。電子プライバシー法 4 条で、ISP にサービスのセキュリティ確保のための対策を取るように求めている。
オーストラリア	法的な規定はない。利用者の同意は不要。
韓国	情報通信網利用促進法 46 条の 2 利用者の同意は、利用約款による包括同意で良い。

4 違法コンテンツサイトへのアクセスブロッキング

①の実施状況については、各国で対応が分かれている。②、③については以下の通り若干の違いがある。

	アクセスブロッキングに関する実施状況、法的規定と利用者の同意
米国	ブロッキングを義務づける法的規定はない。 18USC2251 条以下に児童ポルノに関する犯罪の規定がある。 ISP が児童ポルノを発見した場合には、サイバーチップラインへの通報が義務づけられている。また自主的な対応として、利用約款で児童ポルノを含む画像の伝送や頒布のためにサービスを利用した場合には、サービス提供を拒否、制限、サービス停止・終了する権限があることを明示している例がある。 同意を要求する法的規定はないが、必ずしも同意不要とはいえず、実務上も利用約款に規定があるので、包括同意で運用しているといえる。
英国	児童ポルノに関して実施されている。 自主規制として、Internet Watch Foundation が実施。 利用者は、技術的なエラーまたは禁止ページであることを示す splash page を受取ることで通知されるのが一般的。
ドイツ	プロバイダは具体的な知識がある場合に限り、違法コンテンツをブロックすることが求められる。これは limited liability regime と呼ばれ、電子商取引法 14 条 1 節に規定されている。 ＊同様の規定は、テレメディア法にも規定がある。

	＊同様の原則が、例えば検索エンジンプロバイダーのような他のインターネットサービスプロバイダーに判例法で適用されている。
フランス	裁判所が無許可オンラインブロッキングサイトへのアクセス停止を命じた場合には、ISP は DNS ブロッキングの実施義務がある。（2011 年 12 月 30 日デクレ 1 条）ただし、こうした明文の規定がなくとも、著作権侵害を含む違法有害サイトについて個別判決によってブロッキングを命ずることは可能。児童ポルノのブロッキングに関しては、2011 年 3 月 14 日法（国内安全大綱法[通称 LOPPSI2]）によって義務付けられた。しかし、この義務付けについての批判も強く、施行令が制定されず、実施されていない。
オーストラリア	行われているようであるが、どのような場合に行われるかについては明確ではない。法的規定についても明確ではない。違法コンテンツへのアクセスがブロッキングされたことを、利用者に知らせるには、ISP によって様々な方法が取られている。
韓国	情報通信網利用促進法 44 条の 7（不法情報の流通禁止） 主な ISP は不法・有害サイトへのアクセスブロッキングを有料で提供している。また利用者が放送通信委員会およびサーバー警察庁に登録されている不法・有害サイトへアクセスした場合に、警告サイトに誘導し、不法・有害サイトであることを通知している。

注：ドイツでは連邦制のもとで連邦と州に規制権限が分かれており、放送及びテレメディア事業者に対する有害情報規制は、青少年メディア保護州際協定によって規定されている。

5 行動ターゲティング広告

①の実施状況については、各国で実施されている。②、③については、以下の通り若干の違いがあるが、主としてプライバシー保護の観点から法的な規制が行われている。

	行動ターゲティング広告に関する法的規定と利用者の同意
米国	同意を要求する法的規定はないが、法的には不法行為法上のプライバシー権および ECPA により規制。また自主規制も行われており、FTC 法 5 条がその実効性の担保規定とされる。実務的には、利用者の選択を尊重している。また「追跡拒否(Do Not Track)原則」が FTC 報告書で提唱されており、主要

	ブラウザーはこれに対応している。
英国	データ保護法によって顧客のパーソナルデータ利用を制限。 プライバシーポリシーで利用者にパーソナルデータの収集方法や利用用途について説明されている。
ドイツ	個人識別情報利用のプロファイリングは、オプトインが求められる。仮名データ（pseudonymous data）利用のプロファイリングは、オプトアウトで認められている。
フランス	プライバシー・電子通信指令(2002/58/EC)とユニバーサルサービス・電子通信ネットワーク・サービスに関する利用者の権利指令（2009/136/EC）によってクッキー利用広告を規制。 プライバシー・電子通信指令 5 条 3 項によって、情報蓄積や利用者の端末機器の蓄積情報に対するアクセスを規制。 CNIL の勧告などによって、利用者に詳しい情報提供を規定。 商業的・マーケティング目的でトラフィックデータを利用する場合には、利用者の事前同意を得ることが必要。 IP アドレスに関しては、各論資料を参照。
オーストラリア	プライバシー法とプライバシー原則（APPs）によってパーソナル情報利用とダイレクトマーケティングを規制。 また、自主規制も行われている。 利用者に対しては、プライバシーノーティス、利用約款、アイコンによって通知されている。
韓国	法的な禁止規定はなく、ガイドラインもない。行動履歴情報は、非識別個人情報と考えられており、識別個人情報と組合せることなく匿名で処理する限り、情報通信網利用促進法 2 条および個人情報保護法 2 条に定める個人情報にあたらない（匿名で処理していない場合は同法で問題となり得る）。またアクセスログやクッキー情報を収集する行為は、盗聴とはみられない。そのため法的問題は生じないと考えられている。 行動履歴情報の行動ターゲティング広告への利用については、利用者の同意は不要と考えられる。

注：行動ターゲティング広告を行う技術的手法としては、DPI（Deep Packet Inspection）方式もあるが、この方式は通信内容（ペイロード情報）を取得する方式であり、現時点では「通信の秘密」を侵害し、違法の恐れがあることから、各国とも実施されていない。

6 通信事業者等の「通信の秘密」への関与に関する法的規定

この他一般的に、「通信の秘密」の保護を制約する法的規定として、公権力の関与とともに通信事業者等が関与を認められている規定がある。

ドイツでは電気通信法 100 条 1 項で、ISP がトラッフィクデータを収集、利用が許される場合の目的が細かく規定されており、その中で機器の故障・障害に対処するため、加入者データ、トラフィックデータの取得・利用が認められている。

この故障概念には、解釈上 DDoS、マルウエア、ボット利用などインターネットサービスの妨害行為が含まれるとされている。また DDoS 攻撃などへの探知が可能かが問題になるが、電気通信法 92 条の反対解釈として可能と解釈されている。

但しデータ保護法があるので、通信内容を他通信事業者と共有はできない。DDoS 攻撃に対しては発信元を探知するが、トラッフィクデータについては、発信者と受信者のリレーの形になるので、第三者提供問題は生じないので、認められると解釈されている。むろん、利用者の同意がある場合には可能である。

また米国では、連邦通信法でサービス提供に必然的に付随する活動やプロバイダの権利もしくは財産の保護に必然的に付随する活動の場合に明確にプロバイダに対する「通信の秘密」の例外を認める規定があり、ECPA にも規定がある。これらの規定によって、プロバイダは「通信の秘密」に関する情報を比較的広く利用できるとの指摘もある。

第 3 章　公権力の「通信の秘密」への関与に関する法的規定の横断比較

1 公権力の「通信の秘密」への関与に関する類型

「通信の秘密」の保障を制約する公権力の関与に関して、

①関与の目的としては、犯罪捜査とテロ対策を含む国家安全保障の二つに分かれている。

②関与の方式としては、現に行われている通信過程に関与する通信傍受と、通信終了後に通信事業者等によって蓄積された情報（保存資料）へのアクセスの二つに分かれている。

③関与の対象としては、通信内容と、通信内容以外の通信に関わるトラッフィクデータ、通信データ、メタデータ、通信属性と呼ばれる情報および通信自体ではなく加入契約に基づいて得られる加入者情報に分かれている。

④関与の手続きとしては、裁判所の令状を必要とする司法傍受と行政機関・捜査機関の手続きで良い行政傍受に分かれている。なお、この司法傍受と行政傍受の用語は、フランスでは使われているが、他の国では必ずしも明示的に使われていないようであるが、実態的には両方の手続きによって、公権力の関与がなされている。

またこの 4 つの観点に関しては各国によって異なっているので、国別に公権力の関与の法的規定を概観するが、公権力の関与に関して事業者に協力義務が課されている場合があるので、併せてこの協力義務についても概観する。

なお、公権力濫用防止の制度的な仕組については、別項にて述べる。

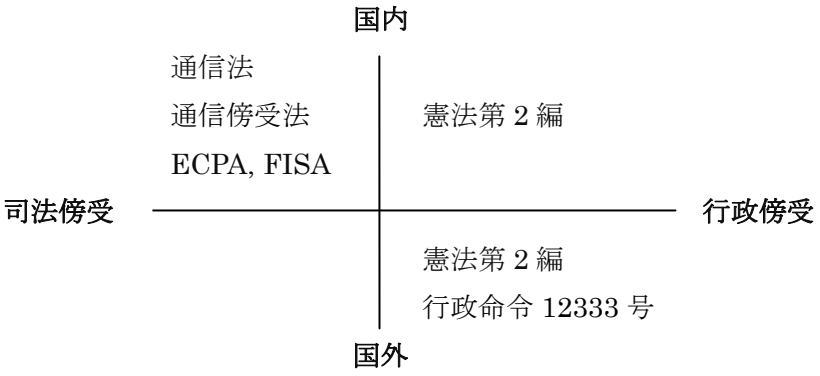
1.1 米国

通信傍受に関する規定としては、連邦通信法 705 条などがあるが、電子的な通信も保護対象にした包括的な法として、電子通信・プライバシー法（ECPA）がある。ECPA は、通信傍受法、蓄積された通信に関する法（SCA）とペンレジスター法の三本から構成されている。この他外国諜報監視法（FISA、以下 FISA）、愛国者法（Patriot 法）があり、行政命令 12333 号でも通信傍受や保存資料へのアクセスを規定している。スノーデン事件で米国の幅広い通信傍受や通信内容以外のメタデータと呼ばれる情報収集活動が知られるようになっている。特に 2011 年 9 月 11 日の同時多発テロ事件発生以来、公権力が関与する通信内容や通信内容以外の通信に関わる情報収集が強化されているのが特徴的事項であり、その合憲性をめぐっても議論が行われている。

このように通信内容の取得と通信内容以外の通信に関わる情報の取得の両方があるが、それぞれの法では、以下のように分類される。

・ECPA（通信傍受法）では、リアルタイムの通信内容の取得
・ECPA（SCA）では、保存資料の取得（通信内容・顧客記録）
・ECPA（ペンレジスター法）では、リアルタイムの通信内容以外の情報の取得

米国の法的規定の特色としては、国内外および米国人/外国人で関与の範囲が異なることおよび関与の手続きが異なることである。これを例示すると、以下の図のようになる。



注：原則は司法傍受が犯罪捜査目的、行政傍受は国家安全保障目的だが、FISA は国家安全保障目的であるにもかかわらず令状が必要。ただし、FISA 令状は犯罪捜査のための令状よりは容易に取得できる

また公権力の関与に関するプロバイダ等の協力義務については、以下のような法的規

定がある。

・ECPA：（18USC2704 条）プロバイダに対する捜査対象たる電子的通信内容のバックアップ保存義務、(18USC3124 条)プロバイダ等に対するペンレジスター・トラップ&『トレース装置の設置及び利用支援の義務付け

・FISA：(50USC1802(a)(4)) 司法長官は通信事業者にあらゆる情報、施設、技術的支援を提供するように指示することができる。

また、この他に法執行法（CALEA）にも協力義務規定がある。

なお、NSA による通信記録収集問題については各論参照。

1.2 英国

公権力の関与に関する代表的な法律は、前述した RIPA である。同法の第 1 部第 1 章では通信傍受の原則禁止規定を置いたうえで、認められる場合の手続きを規定している。

1.3 ドイツ

1968 年の緊急事態法制整備の一環として、基本法 10 条が改正され、また「信書、郵便及び電信電話の秘密の制限のための法律」（以下 G10 法）が施行され、「安全保障のための通信傍受」が認められた。その後一定の犯罪に関する通信傍受もできるようになり、また「個人関連データの不利益利用」も認められた。これらの規定においては、裁判所の関与は不要とされている。また G10 法に基づかない犯罪捜査は刑事訴訟法によって司法手続きのもとで傍受が行われている。

プロバイダの協力義務としては、電気通信法 111 条でプロバイダに顧客の個人データの収集を義務づけ、112 条と 113 条で官庁への提供を義務づけている。また 113 条 1 項 2 文では、通信事業者に対して警察等捜査機関の要求に応じて顧客の個人情報、パスワード、IP アドレスの提供を義務づけている。

さらに通信内容とトラッフィクデータ・個人情報の区分がされており、通信内容の取得は通信傍受を除いてはみとめられていない。

データ保護指令（2006/24/EC）に対応する電気通信法 113 条 a によって、トラッフィクデータの保有義務が電話、電子メール、インターネット接続等の区分ごとに定められている。しかしながら、同条は一部違憲判決が下されている。

また 2014 年 4 月に EU 司法裁判所はデータ保護指令をプライバシー尊重や個人情報保護の原則に違反しており、無効とする判決を行った。

1.4 フランス

通信傍受には、犯罪捜査のための司法傍受と治安等を目的とする行政傍受がある。

司法傍受に関しては、「電子コミュニケーションによる通信の秘密に関する 1991 年 7 月 1 日法律」に基づく通常の司法傍受と、2001 年に新たに設けられた組織犯罪に関する司法

傍受がある。前者に関しては、電気通信による傍受、録音および書き起こしができる。（刑事訴訟法典 100 条以下）

事業者の協力に関しては、予審判事又はその委任を受けた警察官は、傍受装置の設置のために事業者の従業員を徴用できる。また、暗号化通信の場合には、暗号を提供する自然人又は法人は、傍受の命令権者の求めにより協力義務を負う。

行政傍受については、国内安全法典 L241-1 条以下に規定されている。

また保存資料へのアクセスに関しては、犯罪捜査のためのアクセス、通信傍受の準備のため、首相は事業者に対して必要情報の提供を求めることができる。さらに郵便・電子通信法典 L34 条の 1 の 1 によって、テロの予防のための情報提供に関して、事業者が保存及び処理したデータの提供を求めることができる。これらの手続きに関してはすべて裁判所の関与を経ないで行うことができる。

電気通信事業者が取扱う個人に関するデータの種別としては、トラッフィクデータ、通信内容及び加入者に関するデータに区分されている。（同法典 L34 条の 1）

トラッフィクデータの取扱原則は、消去または匿名化である（同法典 L34 条の 1 Ⅱ）. が、広範な例外があって、犯罪捜査等の必要性がある場合には、消去・匿名化を最長 1 年間延期することが実質義務化されている。また保存義務の対象となる具体的な内容もデクレ（政令）で定められている。（同法典 R10 条の 13 Ⅰ）

この他の協力義務としては、「コンテンツの制作に寄与したものを識別するためのデータ」という概念があり、接続プロバイダやホスティングプロバイダ等はこれらのデータを取得・保存し、必要に応じて公権力に提供する義務もある。（デジタル信頼法 6 条Ⅱ）

また発信者情報についても保存義務があり、プロバイダの種類によって保存すべき内容が異なっている。（2011 年 2 月 25 日デクレ）データの提出先は司法機関であり、その要求に応じて提供される。（デジタル信頼法 6 条Ⅱ3 項）

1.5 オーストラリア

国家安全保障に属する内容に関して、通信傍受も保存資料へのアクセスは、防衛長官の要請に基づく、法務長官の令状によって行われている（行政傍受）。他方、警察等による通信傍受と保存資料へのアクセスについては、令状によって行われている（司法傍受）。

また、1979 年電気通信（傍受及びアクセス）法 30 条で、死亡又は深刻な侵害の恐れがある場合に、相手方の位置情報取得が、警官又は救済できそうな通信の一方当事者の緊急要請によって令状なしに認められている。

1.6 韓国

通信内容と通信内容以外の情報は通信事実確認資料と呼ばれ区分され、犯罪捜査や国家安全保障の目的のために、通信制限措置（郵便の検閲又は電気通信の傍受）や通信事実確認資料の提出要請が通信秘密保護法で規定されているほか、電気通信事業者の協力義務が

規定されている。

2 公権力（行政・捜査機関）の濫用を防止・監視する制度的仕組み

3 権分立の観点から、裁判所の令状発出レベルでのチェックがまず挙げられる。また、裁判所の有する違憲立法審査機能によってその濫用の防止を図る制度的枠組みがある。

これに加えて立法府や行政府のなかで、その濫用を防止・監視の仕組みを設けている国もある。まずドイツでは、G10 法 15 条で、10 条審査会の設置規定がある。この審査会は、連邦議会に置かれる委員会で、G10 法に基づく通信傍受活動を統制することを目的としている。同審査会は情報収集、加工および利用等「通信の秘密」を制限する措置の全体の統制に当たるとされ、広範な権限が与えられている。

またフランスでは、行政機関の保存資料へのアクセスの統制のために、独立行政機関である国家治安傍受統制委員会が設置されている。テロ予防のために内務省に置かれた専門官が、事業者に対して保存及び処理したデータの提供を請求する決定を行うが、同委員会は専門官の選任を行うとともに、その適法性を監視し、違反の場合には内務大臣に勧告することで、濫用の防止を図る仕組みを有している。

さらに英国の RIPA では、同法で認められた傍受や通信データの取得などが、適切に行われているかを審査する仕組みとして、首相が通信傍受委員や情報機関委員を任命する制度や行政審判所の設置が規定されている。（同法第 4 部）

第 4 章　各国調査結果の日本の法制度へのインプリケーション

1 「通信の秘密」の概念に関する日本との比較

まず第 1 に、「通信の秘密」の法的な適用範囲が異なっているように考えられる。米国では「通信の秘密」は、その保護法益とされるプライバシーの一局面、すなわち「通信のプライバシー」として捉えられている。また、米国とヨーロッパでは、帯域制御なり情報セキュリティ対策の問題は、主としてネットワーク中立性の問題として議論されている。さらに、違法情報のブロッキングに関しては、インターネットにおいて表現の自由およびその制限をどうするかの問題としても議論されている。従って、「通信の秘密」が第一義的な法的問題となる場面は、日本よりも限られているようである。

第 2 に、通信事業者なりプロバイダの「通信の秘密」への関与に関しては、「ドイツの規定は、実定法に詳細な規定を置き、通信事業者にとっては、何をしなければならないか、逆に何をしてはいけないかが詳細に規定されているため、法的な判断をする場面が日本よ

りもはるかに少ない」と述べられているように、ドイツでも米国でも通信事業者なりプロバイダが、どのような場合に「通信の秘密」の保護に対して制約となる行為をなし得るかが法律レベルで規定されている。

このため、通信事業者なりプロバイダの「通信の秘密」への関与に関する法的規定が多いことが特徴的であり、この法的規定には、公権力の「通信の秘密」への関与に対する協力義務規定も含まれている。

第3に、公権力の「通信の秘密」への関与に関しては、関与の目的、方式、対象および手続の面で、幅広くかつ詳細な法的規定がなされている。これらの法的規定に基づいて公権力の関与によって、「通信の秘密」の保護を制約する場合が、日本よりはるかに多いことも特徴として挙げられる。

2 「通信の秘密」の法体系

第1に、例えば迷惑メール対策として、フィルタリング・ブロッキングを行うことは、利用者の保護に加えて、通信ネットワークに加重されるトラッフィクの負荷を軽減することで、通信ネットワーク・サービスの円滑な運営を図ることが理由となっている。また情報セキュリティ対策として、様々な措置を講ずることは、利用者の通信利用を確保するとともに、通信事業者なりプロバイダのネットワーク資産を守ることもその理由になる。

このように「通信の秘密」の保護を制約する行為をなし得る理由として、米国ではサービスに付随する事業者の権利もしくは財産を保護することが法律レベルで規定されており、通信事業者なりプロバイダの権利を明確に認める法的な規定があることもその特徴と言える。

第2に、現在の「通信の秘密」に関する法体系では、通信内容とそれ以外の区別を行うことがEU指令で定めらており、国内法化されている。米国でも、トラッフィクデータとの用語は用いられていないが、法律によって両者は使い分けられている。また、米国でもEU諸国でも通信過程のリアルタイムでの傍受と保存資料の取得の区分に基づいて法的規定が使い分けられている

米国のECPAではこの二つの区分のうちで、通信内容の公権力への提供や、リアルタイムの通信傍受に関してはより厳格な手続きを要求しているとされる。しかしながらこのような法的構成は、蓄積される情報が少ない時代に通信傍受がよりプライバシー侵害のリスクが大きかったことを反映しているものと考えられる。現在ではスノーデン事件で明らかになったように、通信内容以外のメタデータの取得・蓄積・分析が大量に行われると、プライバシーへの脅威はより大きくなるとも考えられる。

この観点からは、通信内容とそれ以外の区別と通信傍受と保存資料の取得・分析の二つは、インターネットにおける個人情報や機密情報の膨大な蓄積が可能になった現在およびこの可能性がより大きくなる将来においては、「通信の秘密」をはじめとする人権を保護する立場からは、その有効性がゆらいでくる可能性もあり、この点を視野に入れて今後の法

的規定の検討が必要になるようにも考えられる。

第 3 に、現在の「通信の秘密」の法体系は、通信事業者なりプロバイダの主体に着目して、事業者の権利義務や公権力の関与が法的に規定されている。しかしながら、インターネットに関するサービス提供者の類型が多彩化することで、第 1 期研究会報告書でも述べたように、誰が「通信の秘密」の適用事業者であるかあいまい化しており、多層レイヤー化が一層進展すると予想される今後はさらにその傾向は進むものと考えられる。

したがって、「ドイツは、電気通信事業者の問題としてではなく、情報化時代のネットワーク上の何を規制対象とするかを考えた唯一の国ではないだろうか」と述べられているように、将来的には主体に着目した規制体系だけではなく、サービスといういわば客体によりウエイトを移した規制体系を加味していくことが、さまざまな保護法益を守るために有効であるようにも考えられる。

第 4 に、各国の公権力の「通信の秘密」への関与の法的規定を見ると、9.11 以降の憲法上の大問題である「自由と安全」のトレードオフとも言われる難問に対して、法的にどのような理論的、実践的な処方箋を打出していくかが問われているように考えられる。

第 5 章「プライバシーの権利」に関する補足

「通信の秘密」の保護法益は「プライバシー保護」であるとする見方が有力である。わが国の憲法学界でも、それが主流だとされている（長谷部 [2011] など)。しかし、事業者的に見ると、法人の通話量が個人のそれを圧倒している現状に照らし、プライバシー保護の観点だけで説明することに、若干の逡巡がある。プライバシー保護を主とし、言論の自由を従とする程度の理解が、妥当かと思われる(法人にはプライバシーはないが「言論の自由」はあるだろうから)。

憲法論を離れて刑事手続法的に見ると、わが国の場合「通信の秘密」の保護根拠を、 ①「生命、自由及び幸福追求」の権利を保障する憲法 13 条、② 少なくとも電気通信の傍受に関しては同 21 条 2 項、③ 適正手続きを定めた同 31 条、④ 令状主義の保障を定める同 35 条のいずれに依るべきかという議論があり得る。しかし、これらは相互に排他的なものではなく補完的なものであり、いずれも実体的には「プライバシーの権利」を保障するものだと考えられている（井上 [1997])。

とすると、少なくとも先進諸国の間では、「通信の秘密」の保護については共通の認識がありそうだが、実はプライバシーの概念そのものが国によって微妙に違っており、「通信の秘密」に関する統一的な原則を見出すのは、予想以上に難しい。そこで、拙速な一般化が危険を伴うものであることを知りつつも、敢えて類型化を試みれば、プライバシーの理解には EU 型、アメリカ型、イギリス型の 3 つのパターンがあると思われる。

EU 型の特徴は、プライバシーを基本的人権の中心的価値の一つだと考え、それを保護することに細かい配慮をしていることである。人格権であるから「不可譲（inalienable）の権利」であり、約款などで安易な情報開示（譲渡）を認めることに抵抗があり、EU 加盟国以外であっても EU と同等の「十分なレベルの保護」（adequate level of protection）がなされていない国に、個人データが流出するのを認めることができないとしている（Ruiz [1997] など）。これは、ナチズムによるユダヤ人虐待という歴史的に大きな「負の遺産」を背負った国々の、共通の認識かもしれない。

一方アメリカ型の特徴は、プライバシーを人格権の 1 つとすることに変わりはないが、資本主義のチャンピオンを自認する国だけに、自立した個人が承認した上でプライバシーをあたかも財産権（property）の一種のように売買することにも、抵抗感がないことである。人権派の代表格と見られるレッシグが、P3P（Platform for Privacy Preference）などの「コード」によって、プライバシー情報を取引条件にすることを推奨していることは、日本人には理解しがたい面がある（Lessig [2000]）。しかし、property 化して alienable にする方が個人の自立を尊重していることになり、それは資本主義の精神そのものだというのが、アメリカ的理解であろう（林 [2012] ）。プライバシー保護の一般法がなく、業界や利用形態毎の個別法に依っていること、利用者が承諾すれば多様な個人データの利用がなされていること、などがその結果として生じている。

イギリスは従来、英米法系に属する国として（さらには英米法の発祥の地として）アメリカと同じような特徴を持つものと理解されてきた。しかし、ことプライバシーに関する限り、両国には思いもかけぬ差がある（名誉毀損についても両国の差は甚大）。というのも、イギリスでは従来プライバシー侵害という訴訟原因（cause of action）を認めず、「信頼関係の毀損」（breach of confidence）として裁いてきたからである。つまり対世効をもった「客体」としてのプライバシー保護という視点ではなく、情報の授受当事者である confider と confidant の間の信頼「関係」の維持という点に、価値を認めてきたのである（Gurry [1984]）。

これは信託をはじめとする信任関係の法が、歴史的に大きな比重を占めてきたイギリスの特徴であり、英連邦諸国に共有されていると思われる。ただし、どの程度の普遍性があるかは、それぞれの国ごとに検証しなければならない（オーストラリアとカナダでは違いがありそうである）。しかも、発祥の地であるイギリスにおいては、EU に加盟し人権条約を批准したあたりから変化もが生じ、EU 型に近づく傾向を示している（林 [2013]）。

このようにプライバシーに関しては、先進国の間だけでも 3 つのパターンがあり、大陸系と英米法系という単純化はできない。とすると、プライバシーを源泉とする「通信の秘密」の保護に関しても、パターンの差が生じていてもおかしくないことになろう。一般化は危険であるが、理解のために敢えて単純化すれば、人格権重視の EU 型、市場における契約重視のアメリカ型、情報の授受当事者間の関係重視のイギリス型という大まかな分類は、おおむね妥当するものと思われる。

なお、「インターネット時代の通信の秘密」をテーマにした本研究会の議論では、インタ

ーネットそのものに対する扱い、とりわけ経済的・社会的両面における規制政策のあり方が影響を与える点を無視できない。この点では、インターネットの商用化以降、一貫して「非規制政策」を取り続けている米国（しかも、今もなおインターネット関連産業で世界をリードしている）と、その他の国の間には、目に見えない対応の差があると考えられるが、本研究会では深入りすることができなかった。この点については、林［2002］を参照されたい。

[第 5 章の引用文献]

井上正仁［1997]『犯罪捜査のための通信・会話の傍受』有斐閣

長谷部恭男[2011]『続・Interactive 憲法』有斐閣

林紘一郎［2002]「インターネットの非規制政策」林紘一郎・池田信夫（編著）『ブロードバンド時代の制度設計』東洋経済新報社

林紘一郎［2012]「Privacy と Property の微妙なバランス：Post 論文を切り口にして Warren and Brandeis 論文を読み直す」『情報通信学会誌』Vol.30, No.3

林紘一郎［2013]「個人データ保護の法益と方法の再検討：実体論から関係論へ」『情報通信学会誌』Vol.31, No.2

Gurry, Francis [1984] “Breach of Confidence”, Clarendon Press

Lessig, Lawrence [2000] “CODE and Other Laws of Cyberspace”, Basic Books

Ruiz, Blanca R. [1997] “Privacy in Telecommunications”, Kluwer Law International

第 2 部　国別調査結果

第 1 章　米国

城所岩生（米国弁護士）[1] 松前恵環（駒澤大学）[2]

1 「通信の秘密」に関する法的規定

1.1 米国における「通信の秘密」の保護の概要

米国において、日本における「通信の秘密」の問題は、「通信の秘密」という概念の下で論じられているものではなく、プライバシーの権利、中でも「通信のプライバシー（communication privacy）」[3]の問題として議論されることが多い。S.D. ウォーレン（Samuel D. Warren）と L. D. ブランダイス（Louis D. Brandeis）の手になる 1890 年の論稿[4]が発表されてから 1 世紀余りが経過した現在、米国においては、かかる通信のプライバシーを含むプライバシーの権利の保護は、主に合衆国憲法、不法行為法、そして、制定法等によって図られている。

通信のプライバシーがとりわけ古くから問題とされてきたのは、合衆国憲法第 4 修正[5]との関係においてであり、法執行機関による犯罪捜査等のための通信傍受が、第 4 修正上の「不合理な捜索・押収（unreasonable search and seizure）」に該当するかどうかという点が争点となってきた。当初、こうした通信傍受が第 4 修正上の「捜索・押収」に該当するためには、「憲法上保護された領域」への「物理的な侵入」を要するとする、いわゆる「不法侵害法理（trespass doctrine）」が採用されており[6]、禁酒法違反の捜査の過程で当局が数ヶ月に亘り無令状で行っていた電話盗聴の合憲性が問題となったオルムステッド判決では、家への不法な侵入を伴わない電話盗聴は合憲であるという判断がなされた[7]。しかし、こうした財産権と結び付いたプライバシーの法的保護の基準は、とりわけ 20 世紀中葉以降の盗聴技術の進展を受けて、その終焉を迎えることとなる。連邦最高裁判所は 1967 年のカッツ判決において、捜査当局が、電子盗聴器及び録音機を、被告人が電話をしている公衆電話の外側に取り付けて会話を盗聴したことが、第 4 修正上の捜索・押収に該当するかが争われた事案について、「第 4 修正は、人を保護しているのであって、場所を保護しているのではない」[8]と述べて「不法侵害法理」を放擲した。現在では、第 4 修正上のプライバシー権の

---

[1] 本章 2.1～2.3、3、及び 4 を執筆
[2] 本章 1、及び、2.4, 2.5 を執筆
[3] *See* e.g., PRICILLA M. REGAN, LEGISLATING PRIVACY 7 (1995).
[4] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[5] U.S. CONST. amend. IV.
[6] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §2.1 (a), (b) (4th ed. 2004).
[7] Olmstead v. United States, 277 U.S. 438 (1928).
[8] Katz v. United States, 389 U.S. 347, 351 (1967).

保護範囲を決する主要な基準として、「プライバシーの合理的な期待」の基準が多くの裁判例で採用されるようになっている[9]。

こうした法執行機関による通信傍受の他に、例えば雇用者が被用者の通信を監視するといった場合には、不法行為法上のプライバシー権が問題となる。不法行為法上のプライバシー権の侵害の判断に際しては、今日も、W. L.プロッサー（William L. Prosser）が提示した四類型、すなわち、「侵入」（intrusion）、「私事の公開」（public disclosure of private facts）、「公衆の誤認」（false light in the public eye）、「盗用」（appropriation）が基本的に用いられている[10]。近時はとりわけ雇用者による被用者の e メールの監視が問題となっており、例えば、被用者の e メールの傍受は行わないと明言していたにもかかわらず、被用者の e メールの傍受を行い、不適切な意見があったとして被用者を解雇した雇用者を、被用者が提訴するといった事案が見られる[11]。

通信のプライバシーの保護に関わる連邦レベルでの制定法としては、「電子通信プライバシー法」（ECPA: Electronic Communications Privacy Act of 1986）[12]や「通信法」（Communications Act of 1934）[13]等が挙げられる。これらは、米国における通信のプライバシーの保護のための具体的な規定として特に重要な位置を占めるものであるため、次項でやや詳しく検討を加える。

1.2 主な制定法の規定

(1) 通信傍受に関する規定

まず、通信傍受を一般に禁ずる刑事法の規定について検討する。先に述べたように、通信傍受に関しては、とりわけ法執行機関との関係で裁判例の蓄積があるが、これと並行して、通信傍受の一般的禁止を定めるとともに、通信傍受が許容される要件や手続を明確化する法律の制定も進められた[14]。20 世紀前葉には、先述オルムステッド判決において通信傍受に関する立法措置の必要性が示唆されたことを受けて制定された、「通信法」の第 605（現 705）条が、米国において通信傍受を規律する唯一の規定であった。もっとも、同法の規定は通信回線以外の場所に盗聴装置を仕掛ける場合には適用されず、その実効性には限界があったため、不法侵害法理を放擲したカッツ判決等を受けて、「総合的犯罪防止及び街路の安全に関する法律」（Omnibus Crime Control and Safe Streets Act of 1968）が制定さ

---

[9] *Id.* at 361.
[10] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).
[11] Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). もっとも本件について法廷意見は、「侵入」類型のプライバシー侵害について、自由意志でなされた e メールのコミュニケーションについては、プライバシーの合理的な期待が存しないと判断している。
[12] Pub. L. No. 99-508, 100 Stat. 1848 (1986).
[13] Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934).
[14] 米国における通信傍受に関する制定法の歴史については、*See* e.g., DANIEL J. SOLOVE AND PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (3rd ed.) 294-296 (2009). また、邦語文献としては、右崎正博「犯罪捜査のための通信の傍受・盗聴に関する法制の概要」『盗聴法の総合的研究：「通信傍受法」と市民的自由』（日本評論社、2001 年）293-301 頁等を参照。

れ、同法の第三篇に通信傍受に関する規定が置かれるに至る。これは、通信と会話のプライバシーを保護し、その傍受が認められる場合と条件に関する統一的な基準を定めるものであった。しかし、その対象は音声の伝達に限定されていたため、1970 年代から 1980 年代にかけて、移動体通信、ファクシミリや電子メール等の音声の伝達以外の新しいデータ通信技術の登場に伴い、これらの新たな通信への対応の必要性が高まる。そこで制定されたのが、電子的な通信をも保護対象に含めた ECPA である。同法は、それぞれ①「通信傍受法」（Wiretap Act）[15]、②「蓄積された通信に関する法」（SCA: Stored Communications Act）[16]、③「ペンレジスター法」（Pen Register Act）[17]と呼ばれる三つの部分から構成されている。

まず、いわゆる①「通信傍受法」には、通信の伝送中におけるリアルタイムでの、通信内容の傍受に関する規定が置かれている。すなわち同法では、「何人も、有線通信、口頭の会話又は電子的通信を、意図的に傍受し、傍受を試み、又は他の者を説得して傍受させ、若しくは傍受を試みさせてはならない」[18]と規定され、「傍受」（intercept）とは、「電子的、機械的その他の装置の利用を通じて、有線通信、電子的通信又は口頭の会話の内容を音声その他の形態で捕捉すること」[19]とされている。かかる規定に反した場合、民事上の損害賠償責任[20]のほか、刑事罰として、罰金若しくは 5 年以下の拘禁刑、又はその併科[21]が規定されている。

同規定に関しては、幾つかの例外が定められており、有線通信又は電子的通信サービスのプロバイダによる一定の通信の傍受、開示、又は利用の場合[22]、裁判所命令等に基づき、法により授権された者に対し、情報、設備、又は技術的支援を提供する場合[23]、通信の一方当事者の事前の同意がある場合[24]等は、通信の傍受が違法とならないとされる。プロバイダによる一定の通信の傍受等が認められるための要件としては、そのサービスの提供に必然的に付随する活動、又は、プロバイダの権利若しくは財産の保護に必然的に付随する活動、に従事する場合であることが求められている[25]。

---

[15] 18 U.S.C. § 2510-2522.
[16] 18 U.S.C. § 2701-2711.
[17] 18 U.S.C. § 3121-3127.
[18] 18 U.S.C. § 2511(1). 以下の ECPA の訳については、平野美惠子・土屋恵司・中川かおり「米国愛国者法（反テロ法(下)）」『外国の立法』215 号 1 頁（2003 年）を参考にしつつ、一部改訳した。
[19] 18 U.S.C. § 2511(4). 「内容（content）」とは、「有線通信、口頭の会話又は電子的通信に関して使用される場合は、通信の主旨、意図又は意味に関する情報を含む」（18 U.S.C. § 2510(8)）とされている。
[20] 18 U.S.C. § 2520.
[21] 18 U.S.C. § 2511(4)(a).
[22] 18 U.S.C. § 2511(2)(a)(i).
[23] 18 U.S.C. § 2511(2)(a)(ii).
[24] 18 U.S.C. § 2511(2)(c)(d).
[25] *Supra* note 22. 前者の例としては、長距離電話のオペレータが、回線が確立されているかを確認するのに必要な時間、傍受を行うことや、モーテルの電話交換手が業務を遂行する間、会話を傍受すること等が認められている。後者に関しては、「必然的に付随する」といえるかどうかは、プロバイダが、より制限的な態様で傍受を行えなかったこと、かつ、他の合理的な手段を利用できなかったこと、を示すことや、傍受と傍受の理由との間に、「実質的なつながり（substantial nexus）」があること等が必要とされている。*See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance,* 2009 U.ILL. L. REV. 1417, 1481-1487

これに対し、リアルタイムの傍受ではなく、蓄積された通信の内容や、顧客に関する記録へのアクセスに関する定めを置いているのが、いわゆる②SCA である。同法は、電子的に蓄積された通信への違法なアクセスを処罰するとともに[26]、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダが、サービスにおいて電子的に蓄積されている通信の内容を意図的に漏示（divulge）することを禁じている[27]。かかる規定についても一定の例外が設けられており、例えば、法の規定に基づいて開示される場合、通信の当事者の同意がある場合、サービスの提供又はサービスにおけるプロバイダの権利若しくは財産の保護に必然的に付随する場合等には、開示が許容される[28]。

これら蓄積された通信の内容に関する規定に加え、SCA では、蓄積された通信の内容以外の、「サービスの受信契約者又は顧客に関する記録その他の情報」についても、幾つかの規定が置かれている。まず、電子的通信サービス又は遠隔コンピュータ処理サービスのプロバイダは、かかる顧客記録を政府機関に対して意図的に漏示することを禁じられている[29]。もっとも、政府機関が法の規定に則り開示を要求する場合、通信の発信者又は受信者の適法な同意に基づく場合、サービスの提供又はサービスにおけるプロバイダの権利若しくは財産の保護に必然的に付随する場合、人の死又は重大な身体的傷害の急迫の危険に関わる緊急事態のために、情報の開示が正当化されるとプロバイダが合理的に信ずる場合、政府機関以外に対して開示する場合、等の一定の場合には、開示が認められている[30]。

他方で、いわゆる③「ペンレジスター法」は、通信の内容以外の、通信の処理に関する情報（transactional information）のリアルタイムでの取得についての規定であり[31]、こうした情報を記録・解析する装置である「ペンレジスター装置」[32]、又は、「トラップ&トレース装置」（trap and trace device）[33]を、法の規定に基づく裁判所命令を事前に得ずして、設

(2009).

[26] 18 U.S.C. § 2701.

[27] 18 U.S.C. § 2702(a)(1)(2). 「電子的蓄積（electronic storage）」とは、「(A) 電子的送信に伴う有線通信又は電子的通信の、暫定的、中間的な蓄積」「(B) 通信のバックアップの保護の目的で、電子的通信サービスにより行われる通信の蓄積」（18 U.S.C. § 2510(17)）であるとされる。なお、紙幅の都合上、本稿では詳細な検討を加えることは控えるが、プロバイダについては、「電子的通信サービス（ECS: electronic communication service）」のプロバイダと「遠隔コンピュータ処理サービス（RCS: remote computing service）」のプロバイダとの区別が設けられている。

[28] 18 U.S.C. § 2702(b).

[29] 18 U.S.C. § 2702(a)(3).

[30] 18 U.S.C. § 2702(c).

[31] Cybertelecom, *ECPA: Title III: Pen Register Act: Non Content: Trap & Trace*, http://www.cybertelecom.org/security/ecpatrapandtrace.htm (last visited May12, 2014). なお、通信内容以外の通信に関する種々の情報をどのように呼称するのかは論者によって区々であり、例えば S. フライウォルド（Susan Freiwald）は、「通信属性」（communication attribute）として説明している。*See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 46-47 (2004). O. S. カー（Orin S.Kerr）は、「メタデータ（metadata）」、あるいは「包装情報（envelope information）」という用語を用いている。*See* e.g., Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 384 (2014).

[32] 18 U.S.C. § 3127(3). 「有線通信又は電子的通信の送信元となる機器又は設備により送信される局番、経路、宛先又は信号の情報（ただし、この情報には通信の内容は含まれない。）を記録し、又は解読する装置又はプロセス」と規定される。

[33] 18 U.S.C. § 3127(4). 「有線通信又は電子的通信の源を合理的に特定するような発信者番号又は他の局

置し、又は利用することが禁止されている[34]。これらの装置によって取得される情報としては、伝統的にはダイアルされた電話番号などが想定されていたが、「米国愛国者法」（USA Patriot Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism）[35]による改正で、電子的な通信に関する、e メールのヘッダ情報や IP アドレスなども包含されるようになったと言われている[36]。もっとも、その他の情報として何が含まれるのかは必ずしも明確ではないという指摘もある[37]。

なお、詳しくは本章の 3（公権力の「通信の秘密」への関与に関する法的規定）に譲るが、ECPA では、以上のような通信傍受の禁止に関する一般的な規定に加え、政府機関が、通信内容（リアルタイム/非リアルタイム）、通信内容以外の顧客に関する記録、及び、通信内容以外の通信の処理に関する情報を取得する場合の手続についても、それぞれ規定されており、取得される情報の性質や開示要求を受けるプロバイダの種類等によって、異なる手続及び令状要件等が定められている[38]。通信の内容に関しては、その取得についてとりわけ厳格な手続及び要件が要求されていることが特徴的である。

(2) 電気通信事業者のプライバシー保護に関する規定

通信のプライバシーの保護のための制定法としていま一つ言及しておくべきは、「通信法」である。同法は「1996 年電気通信法」（Telecommunications Act of 1996）[39]によってアップデートされ、顧客情報の保護に関する電気通信事業者の義務が規定されている。すなわち同法の下で合衆国法典第 47 編第 222 条(c)(1)は、は、「電気通信サービスを提供することによって、顧客に関する専属的ネットワーク情報（CPNI: Customer Proprietary Network Information）を受領又は取得する電気通信事業者は、法律の要求がある場合又は顧客の承認（approval of the customer）を得た場合を除き、(A)当該情報が得られた電気通信サービス又は(B)その電気通信サービスに必要な又は関連して利用されるサービス（ディレクトリの公開を含む）を提供する場合にのみ、当該情報を利用し、開示し又はその情報へのアクセスを許可することができる」[40]と定めている。ここで「顧客に関する専属的ネットワーク情報」とは、「電気通信サービスの数量、技術構成、種類、宛先、位置及び利用総額に関する情報で、通信事業者と顧客との関係を理由としてのみ顧客が通信事業者に利用させるもの」、及び、「通信事業者の顧客が区域内電話サービス又は長距離電話サービスに関して受領した請求書に記載された情報」とされている[41]。

番、経路、宛先若しくは信号の情報を特定する、入来する電子的その他の信号を捕らえる装置又はプロセス（ただし、この情報には通信の内容は含まれない）」と規定される。

[34] 18 U.S.C. § 3121(a).
[35] Pub. L. No. 107-56, 115 Stat. 272.
[36] Freiwald, *supra* note 31, at 51, n279.
[37] *Id.* at 49.
[38] 18 U.S.C. § 2518; § 2703(a)(b); § 3122-3123.
[39] Pub. L. No. 104-104, 110 Stat. 56 (1996).
[40] 47 U.S.C. § 222 (c)(1).
[41] 47 U.S.C. § 222 (h)(1).

電気通信事業者が CPNI の利用に際して取得しなければならない「顧客の承認」に関しては、「承認」の意味及び方法等について必ずしも具体的な基準が示されていないという点が問題とされており、連邦通信委員会（FCC: Federal Communications Commission）は、電気通信事業者の上記義務の実施に関する規則を制定し、その内容の具体化を図ってきた[42]。近時 FCC は、2007 年の「報告・命令・規則制定案告示」において、社外に CPNI を提供する際には、事前に顧客の積極的な同意を得なければならないとして、承認の方法についてオプトイン規制を採用している[43]。

なお、電気通信事業者の上記義務に関しては、例外規定が設けられており、例えば、電気通信サービスの開始、提供、宣伝、集金のために行う場合、事業者の権利若しくは財産の保護、又は、サービスの利用者若しくは他の事業者の、当該サービスの詐欺的、濫用的若しくは違法な利用若しくは購入からの保護、のために行う場合、顧客の承認のもと、勧誘、照会、又は管理サービスの提供のために行う場合等には、顧客に関する専属的ネットワーク情報の、利用、開示、又は当該情報へのアクセスが許可される[44]。

1.3 近時の議論動向

通信のプライバシーに関するこれらの制定法に関しては、近時の情報技術の進展に伴い、現状と法の規定との乖離が指摘されるようになっている。とりわけ論議を醸しているのが ECPA の規定であり、1986 年の制定当時から同法が採用している幾つかの「二分法（dichotomy）」が、新たな通信形態が次々と登場する現状にはそぐわないのではないかという問題が提起されている[45]。

こうした「二分法」のうち、まず指摘しておくべきは、通信の内容（content information）と、通信の内容以外の通信に関する情報（non-content information）との区分であろう。先述の通り、ECPA においては、通信内容とそれ以外の通信に関する情報とを区分した上でそれぞれについて別の規制が設けられるとともに、政府機関への提供の場面ではこの区分によって異なる手続や令状要件が定められており、通信の内容がより手厚い保護を受けるという構造が見られた。しかし、情報技術の進展著しい現代においては、通信の内容以

---

[42] こうした FCC による規則制定の経緯や展開については、*See* In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 F.C.C.R. 14860, paras. 10-25 (2002). 詳しくは、松前恵環「位置情報技術とプライバシーを巡る法的課題―GPS 技術の利用に関する米国の議論を中心に―」堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、2010 年）235-286 頁を参照。

[43] In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carrier's Use of Customer Proprietary Network Information and Other Customer Information, Report and Order and Further Notice of Proposed Rulemaking, 22 F.C.C.R. 6927 (2007). この 2007 年の命令に対しては、全米ケーブルテレビ協会（NCTA: National Cable and Telecommunications Association）が第 1 修正の下で保障される言論の自由を侵害するとして規則の無効を申し立てていたが、コロンビア特別区巡回控訴裁判所は FCC の規制を支持した。*See* Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996 (D.C. Cir. 2009).

[44] 47 U.S.C. § 222 (d).

[45] *See* e.g., Kerr, *supra* note 31, at 390.

外の情報を蓄積し分析することによって、個人のプライバシーに重大な影響が及ぶことが指摘されており、インターネット時代においてはかかる区分はもはや意味をなさなくなってきていることが指摘されている[46]。

また、ECPA が採用するいま一つの「二分法」としては、リアルタイムでの通信の取得と、蓄積された通信の取得との区分が挙げられる。すなわち、ECPA では、前出の通信傍受法と呼ばれる部分において、リアルタイムでの通信内容の取得を規制し、他方で、SCA と呼ばれる部分において、蓄積された通信内容の取得に関する規定を置き、とりわけ政府機関との関係において、リアルタイムでの通信内容の取得についてより厳格な手続等を要求している。これは、蓄積される情報が少なく、リアルタイムでの通信傍受こそがプライバシーへの大きな脅威として捉えられていた法制定当時は意味のある区分であったが、インターネットや低価格のストレージサービスが普及し、あらゆるものがプロバイダのサーバ等に蓄積される現在においては、リアルタイムでのアクセスと蓄積された通信へのアクセスとで、個人のプライバシーへの脅威は何ら変わらないという指摘がなされており[47]、かかる区分を維持することの意義に疑義が呈されている。

こうした議論を受け、近時米国では、ECPA の改正を主張する声が高まっており、例えば「デジタルデュープロセス連合」による法改正の提案や、「2011 年電子通信プライバシー法改正法」の提案などがなされている[48]。

2 ISP の「通信の秘密」への関与に関する法的規定

2.1 迷惑メールのフィルタリング

(1) 法規制

以下の法律により実施可能。

① 通信傍受法（合衆国法典集第 18 編 2511 条(2)(a)(i)[49]

事業者の権利、財産を保護するために社員に通信傍受などを認める規定。

② ペンレジスター法[50]（合衆国法典集第 18 編 3121 条(b)）

事業者の権利、財産を保護するため、あるいはサービスの濫用もしくは違法使用から加入者を保護するためにペンレジスターの設置を認める規定。ペンレジスターは通話を追跡する（録音はできない）装置。

(2) 実施状況

実施している。以下は事業者の利用規約の関連規定。

(a) ヤフー

---

[46] *Id.* at 398-401.
[47] *Id.* at 390-395.
[48] Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 153-161 (2011-2012).
[49] 18 U.S.C. §2511(2)(a)(i).
[50] 18 U.S.C. §3121(b).

Universal Anti-Spam Policy に禁止行為を列挙し、これに違反した場合はサービスを一方的に停止するとしている[51]。

(b) ベライゾン

利用規約[52] 違反行為の例として

①加入者が欲しない通信、データあるいは情報を伝送したり、スパム行為を行うこと(§2(b))

②電子メールその他のインターネットトラフィックを大量に発生させること(§2(i))

をあげ、こうした規約違反に対して、サービスを拒否したり、制限したりただちにサービスを停止したりすることができると定めている(§1)。

(c) AT&T

利用規約に Spam/E-mail/Usenet Abuse の項目があり、迷惑メールを禁止し、違反した場合はサービスを停止するとしている[53]。

2.2 帯域規制

(1) 法規制

上記 2.1 (1)のとおり。

なお、帯域制御の問題は、米国ではネットワークの中立性の問題として議論されている。2010 年、FCC はインターネットサービスプロバイダー（ISP）に、すべてのインターネットのトラフィックを平等に扱うことを義務づける（裏返すと、追加料金を払うコンテンツサービス事業者のトラフィックを優先させることを禁じる）規則を制定、2007 年の大統領選挙キャンペーン時以来、ネットワークの中立性を提唱していたオバマ大統領も規則を支持した。

2014 年 1 月、首都ワシントンの連邦控裁は中立性規則が FCC の規制権限を逸脱しているため、無効であるとした[54]。無効判決を受けた FCC は新たな規則案を策定し、5 月のパブリックコメントを募集したが、ネットの中立性に逆行する案だったため、反対運動が巻き起こり、FCC にも抗議電話が殺到した。反対論者は ISP を通信事業者のようなコモンキャリアに分類することを要求している。コモンキャリアはすべてのトラフィックを平等に扱わなければならない。これに同調する議員も何人かいて、規則の行方は不透明である。

(2) 実施状況

実施している。上記 2.1 (2) (b) ②参照。

2.3 DDoS などのサイバーセキュリティ関連の攻撃に対するトラフィック遮断

---

[51] https://info.yahoo.com/legal/us/yahoo/guidelines/spam/

[52] Verizon Acceptable Use Policy https://my.verizon.com/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=AcceptableUse

[53] AT&T Acceptable Use Policy, http://www.corp.att.com/aup/

[54] Verizon v. FCC, 740 F.3d 623, 628 (D.C. Cir. 2014).

(1) 法規制

上記 2.1 (1)のとおり。

(2) 実施状況

実施している。以下は事業者の利用規約の規定。

(a) ベライゾン

上記 2.1 (2) (b)のとおり

(b) AT&T

利用規約に Security Violations の項目があり、サイバーセキュリティ関連の攻撃に対する攻撃を禁止し、違反した場合はサービスを停止するとしている[55] 。

2.4 違法コンテンツサイトへのアクセスブロッキング

そもそも違法コンテンツサイトには、例えば児童ポルノに関わるものから、フィッシング詐欺サイトのようなもの、更には著作権侵害に関わるサイトなど様々な種類のものが含まれ得るが、ここではとりわけ、プロバイダによるアクセスブロッキングの是非を巡って近時議論が高まっている、児童ポルノサイトに焦点を当てる。

児童ポルノについて米国では、16 歳以下の児童を含むわいせつ物の製造又は商業的頒布を禁じた、1977 年の「性的搾取からの児童保護に関する法律」（Protection of Children Against Sexual Exploitation Act of 1977）を皮切りに幾つかの法律が制定され、1988 年には、「児童の保護及びわいせつ強制執行法」（Child Protection and Obscenity Enforcement Act of 1988）によって、コンピュータを用いた児童ポルノの頒布が禁じられた[56]。現在では合衆国法典第第 18 編第 2251 条以下に、児童ポルノに関する犯罪が規定されている。通信のプライバシーが問題となるのは、主にこうした児童ポルノサイトへのアクセスをプロバイダ等が遮断するといった場面においてであり、近時は欧州連合（EU: European Union）を中心に、プロバイダにアクセスブロッキングの実施が義務付けられる例も見られるようになっているが、現時点において米国では、こうした義務付けは行われていない。

もっとも、プロバイダが児童ポルノを発見した場合には、失踪児童の捜索や児童の性的搾取の防止などに取り組む「全米失踪・被搾取児童センター」(NCMEC: National Center for Missing & Exploited Children）[57]が運営する、「サイバーチップライン」（Cyber TipLine）[58]へ通報することが義務づけられている[59]。プロバイダが報告すべき内容には、児童ポルノ

---

[55] *See supra* note 5.

[56] 米国における児童ポルノ関連法の歴史については、*see* e.g., Michael J. Henzey, *Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action*, 11 APPALACHIAN J. L. 1, 11-38 (2011).

[57] http://www.missingkids.com/home (last visited May11, 2014)

[58] http://www.missingkids.com/CyberTipline (last visited May11, 2014)

[59] 18 U.S.C. § 2258A. 「サイバーチップライン」は、一般の利用者及びプロバイダからの通報を受け、連邦捜査局や司法省、州及び地方の法執行機関等と協力して児童の性的搾取に関する事案の捜査や児童の保護に取り組んでいる。「サイバーチップライン」のホットラインは年中無休で電話及びインターネットで受

に関する法に違反していると思われる個人の身元に関する情報―メールアドレス、IP アドレスなどを含む―、児童ポルノがアップロードされ、送信され、又は受信された時間や方法、法に違反していると思われる個人の居所やウェブサイトの場所、及び、児童ポルノと思われる当該イメージ等が含まれる[60]。1998 年から 2013 年 12 月までにサイバーチップラインに寄せられた、児童ポルノと疑われる事例やその他の児童の搾取に関する犯罪に関わる報告は 220 万件にものぼり[61]、2012 年に受けた報告のうちの 93 パーセントは、児童ポルノの所持、製造、及び頒布に関するものであったというデータが示されている[62]。

また、プロバイダによる自主的な対応としては、幾つかのプロバイダの利用規約等において、児童ポルノに関する違法行為が行われた場合、サービスの停止等の措置を採る可能性があることが示されている[63]。例えば、ベライゾン社の利用規約においては、利用規約違反行為の例として、ベライゾン社の「サービスを、児童ポルノを含む画像の伝送や頒布のために用いる」ことが挙げられており、かかる利用規約違反行為を行った場合には、ベライゾン社はサービスの提供を拒否又は制限すること、あるいは、即座にサービスを停止又は終了する権限を有することが明示されている[64]。

2.5 行動ターゲティング広告

米国において、行動ターゲティング広告は、それにより消費者のウェブ上での行動が明らかになり、ひいては個人のプロファイリングまでもが可能になるということから、とりわけプライバシーの権利への脅威として議論の対象とされてきた。企業が行動ターゲティング広告を実施した場合、先に見た法規との関連では、不法行為法上のプライバシー権、及び ECPA の規定等が問題となり得る。かかる論点が取り上げられた初期の著名な事案として、クッキーベースの行動ターゲティング広告を行っていたダブルクリック社が消費者からプライバシー侵害を理由に提訴された事案がある[65]。本件において原告は、ダブルクリック社の行為が ECPA の規定に違反すると主張したが、法廷意見は、ダブルクリック社のクッキーを利用しているウェブサイト側の同意を認定し、原告の請求を退けている。

こうした法規制に加え、行動ターゲティング広告に関する自主規制も行われている。そもそも米国のプライバシー保護法制には、民間部門に関しては包括的な規制法を持たず、

け付けられており、日本のインターネット・ホットラインセンター等と同様の活動を行っているものとされる（独立行政法人日本貿易振興機構「米国における青少年保護のためのインターネット規制と運用」（2012 年）10 頁（http://www.jetro.go.jp/jfile/report/07000913/us_youth_internet.pdf (last visited May11, 2014)））。

60 18 U.S.C. § 2258A(b).

61 *Supra* note 58.

62 NCMEC, *2012 Annual Report: Every Child Deserves A Safe Childhood*, 7 (2012), http://www.missingkids.com/en_US/publications/NC171.pdf (last visited May11, 2014)

63 *See* e.g., Verizon Acceptable Use Policy § 1, § 2(k) , https://my.verizon.com/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=AcceptableUse (last visited May11, 2014). *See* also AT&T Acceptable Use Policy, Prohibited Activities: Child Pornography, http://www.corp.att.com/aup/ (last visited May11, 2014).

64 *Id.*

65 In re DoubleClick, 154 F. Supp. 2d. 497 (2001).

分野ごとの個別立法で対応するセクトラル方式を採用し、それらの個別の法規制に、民間事業者による自主規制の仕組みを組み合わせることで、問題に対応してきたという特徴がある。かかる自主規制においては、プライバシー保護の原則として、1973 年に公表された、米国保健教育福祉省（HEW: Department of Health, Educational, and Welfare）の「記録、コンピュータ及び市民の権利（Records, Computers, and the Rights of Citizens）」[66]に起源を有する「公正な情報慣行原則（Fair Information Practice Principles: FIPPs）」が確立されており、現在では①通知/認識、②選択/同意、③アクセス/参加、④データの完全性/セキュリティ、⑤施行/救済の、五つの原則が基本とされている[67]。また、自主規制の実効性の担保として、連邦取引委員会（FTC: Federal Trade Commission）による、FTC 法第 5 条（「不公正又は欺瞞的な（unfair or deceptive）取引行為・慣行は違法である」）[68]の執行が用意されていることも特徴的である。「不公正(unfair)」な行為とは、消費者に対し、消費者自身では避けられない重大な損害、そして消費者や競争にとっての利益より重要な損害を生じさせ、若しくは生じさせるおそれのある行為、そして、「欺瞞的(deceptive)」な行為とは、合理的な消費者を誤解させる可能性のある表示、省略、そして慣行をいうとされており[69]、民間事業者によるこれらの行為があった場合、FTC は調査・訴追する権限を有している。

こうした背景のもと、行動ターゲティング広告についても、FTC を中心としたプライバシー保護のための自主規制が 2000 年前後から行われてきた。近時は、2009 年に公表された「オンライン行動ターゲティング広告のための自主規制原則」[70]において、行動ターゲティング広告に関する自主規制原則として、透明性及び消費者のコントロールの確保、消費者のデータに関する合理的なセキュリティの確保とデータ保持の制限、プライバシーポリシーの変更に際しての積極的な同意の取得、センシティブデータの利用に際しての積極的な同意の取得又はかかるデータの利用禁止、が提示され、以降、これに沿った民間事業者による自主規制が実施されている。更に、2010 年に公表された FTC の報告書、「急速な変化の時代における消費者プライバシーの保護（事前報告書）」[71]では、消費者がウェブ上で

---

[66] U.S. Department of Health, Educational, and Welfare, *Records, Computers, and the Rights of Citizens* (1973).

[67] U.S. Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Oct. 8, 2011).

[68] 15U.S.C. § 45(a)(1).

[69] 15U.S.C. § 45(n).

[70] U.S. Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles for Online behavioral Advertising* (2009), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf (last visited May11, 2014).

[71] U.S. Federal Trade Commission, *Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers* (2010), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (last visited May11, 2014). なお、2012 年には、本報告書に対するパブリックコメントを踏まえて修正を加えた報告書（U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change:*

の行動追跡を拒否できるための仕組みとして、「追跡拒否（Do Not Track）原則」が提唱されている。これは、行動ターゲティング広告を望まない消費者が、ウェブブラウザ上で自身の意思を表明できる仕組みであり、現在では、Internet Explorer や Firefox 等、主要なブラウザがこの仕組みに対応している。

3 公権力の「通信の秘密」への関与に関する法的規定

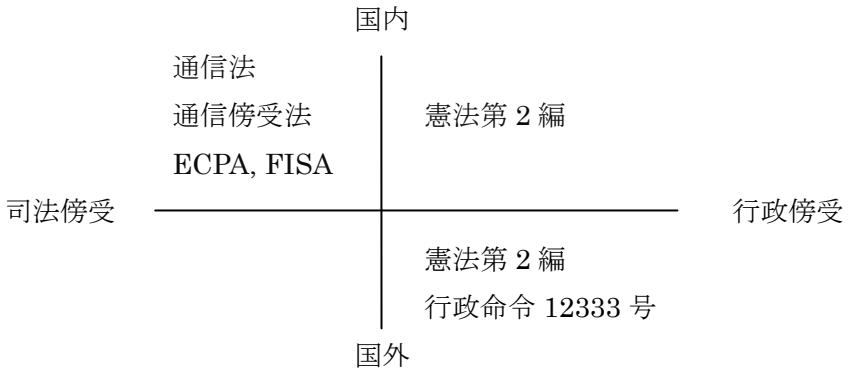
3.1 司法傍受 v. 行政傍受

米政府は伝統的に国家の安全にかかわる事件については、合衆国憲法第 2 編にもとづく大統領の固有の権限として、不合理な捜索、押収を禁じた憲法修正 4 条の制約なしに捜索や通信傍受ができるという解釈をとっていた。このため通信傍受については裁判所の令状が不要な行政傍受が、令状が必要な犯罪捜査のための司法傍受とは別に認められていた。
1972 年、再選をめざしたニクソン大統領は、選挙戦中に民主党全国委員会本部の通信を国家安全の名目で令状なしに傍受した。再選後の 1974 年に辞任に追い込まれたウォーターゲート事件である。1978 年、議会は行政府による捜査権限の濫用を阻止すべく外国諜報監視法（FISA：Foreign Intelligence Surveillance Act of 1978 [72]）を制定した。国家安全目的の FISA 令状を許可することによって、行政府の捜査権限濫用を阻止するとともに外国諜報については、国内捜査より簡単に令状が取得できるようにした(下記 3.3(2)参照)。

3.2 国内の犯罪捜査 v. 外国諜報収集

FISA は国内のアメリカ人に対する外国諜報収集のための通信傍受に緩和された令状要件を課したが、国外のアメリカ人に対する諜報収集のための通信傍受に対しては、行政命令 12333 号 [73] で令状がいらない行政傍受が認められている（下記 3.3(3)参照）。

上記 3.1 および 3.2 の区分を図示すると以下のようになる。



注 1. ECPA：電子通信プライバシー法
注 2. 原則は司法傍受が犯罪捜査目的、行政傍受は国家安全保障目的だが、FISA は国家安全保障目的であるにもかかわらず令状が必要。ただし、FISA 令状は犯罪捜査のための令状

Recommendations for Business and Policymakers (2012).）が公表されている。
[72] 50 U.S.C §§ 1801 et seq.
[73] Exec. Order No. 12333, 3 C.F.R. 200 (1981).

よりは容易に取得できる（下記 3.3(2)参照）。

3.3 公権力が、事業者に対して「通信の秘密」に該当する情報の提供を求める場合の法的根拠と手続き

(1) ECPA

ECPA の概要は前記 1.2 (1) のとおりだが、通信事業者に対する協力義務については以下のように定めている。

① 政府の要請にもとづいて電子通信の内容のバックアップコピーを保存することを通信事業者に義務づけた[74]。

② 法執行当局がペンレジスターやトラップアンドトレース装置を設置する際に必要な支援をすることを通信事業者に義務づけた[75]

(2) FISA 第 1 編 [76]

通常の令状には犯罪を信ずるに足る「相当の理由」が必要だが、FISA は令状の「目的」が外国政府またはその代理人であるとであると信ずるに足る相当の理由があれば、令状の発行を許可した。政府の要請を審査して FISA 令状を発行するために、合衆国最高裁長官の指名する 7 名（その後、11 名に増員、任期は 7 年）の連邦地裁判事で構成する外国情報監視裁判所（FISC：Foreign Intelligence Surveillance Court）を設立した。

令状の対象が合衆国市民、永住権保持者、合衆国企業の場合は、より詳しい説明 (pleadings) が必要だが、FISC が広汎な監視活動を認めた結果、実際は合衆国市民の通信も監視の対象にされた。FISA 令状の申請が却下された場合、外国情報監視控訴裁判所（Foreign Intelligence Surveillance Court of Review）に上訴できる。同裁判所は合衆国最高裁長官の指名する 3 名の控裁判事（任期 7 年）で構成する。

FISC、外国情報監視控訴裁判所とも当事者は合衆国政府のみ、決定も原則非公開で、毎年 4 月に前年の取扱い件数、令状発行数を議会に報告しなければならないが、それ以上の詳細な報告は国家安全の観点から要求されていない。2014 年 4 月に公表された最新のデータ[77]によれば、2013 年には 1655 件の申請があり、うち 34 件は修正したが、却下はなく、2009 年以来、却下ゼロの年が続いている。FISC 審査が「めくら判」視される所以でもある。

通信事業者に対する協力義務については、「司法長官は通信事業者にあらゆる情報、施設、技術的支援を提供するよう指示することができる」としている[78]。

(3) 行政命令第 12333 号

---

[74] 18 U.S.C. § 2704.
[75] 18 U.S.C. § 3124 (a) (b).
[76] 50 U.S.C. §§ 1801-11.
[77] http://www.justice.gov/nsd/foia/foia_library/2013fisa-ltr.pdf.
[78] 50 U.S.C. § 1802 (a)(4).

国外での監視活動・諜報活動を規制するため、1981 年にレーガン大統領が発出。国家安全保障局（NSA：National Security Agency）を SIGINT (Signal Intelligence) とよばれる通信傍受による情報収集担当にした [79]。この命令によって、国内の通信傍受は FISA、国外のアメリカ人に対する通信傍受は行政命令、国外の外国人に対する通信傍受は制約無しという棲み分けができた。通信事業者に対する協力義務について定めた規定は特にない。

(4) 法執行支援法（CALEA：Communications Assistance for Law Enforcement Act [80]）

通信傍受法は、通信事業者に傍受を可能にするために必要な支援を行うことを義務づけたが、その後のデジタル通信技術の発展により事業者の支援があっても傍受できないケースも出てきた。1994 年、議会は捜査当局の要請に応えて法執行支援法を制定し、捜査当局が法的に許可された傍受を可能にするように、通信事業者に以下のような設計変更を義務づけた。

通信事業者は発着信機能を加入者に提供する機器、設備、サービスが、以下の機能を満たすことを保証しなければならない [81]。

① 通信をすみやかに特定し、政府が傍受できるようにすること
② 通信識別情報をすみやかに特定し、政府がアクセスできるようにすること
③ ①、②の情報を政府に引き渡すこと
④ 傍受を許可されていない通信のプライバシーとセキュリティを守り、もしくは妨げないように上記の行為を実施すること

(5) 米国愛国者法 215 条 [82]

米議会は 911 同時多発テロ事件の翌 10 月に米国愛国者法（Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism Act of 2001、以下、「愛国者法」）を制定した。国境防備、捜査権限の強化、テロ資金の規制が 3 本柱のテロ対策法で、既存の法律が麻薬取引や組織犯罪に対して捜査官に与えていた、より広い権限をテロ対策にも適用できるようにした。「捜査権限の強化」では通信技術の発達、人と金の迅速・容易な移動に対応して通信傍受法を最新化した側面もあるが、捜査当局の要望にほぼ満額回答した。

愛国者法 215 条は、外国諜報や國際テロの捜査を目的とした、営業記録へのアクセスについて定めた FISA の条項を以下のとおり大幅に改正した。

① FISA501 条は、FBI が FISA 令状によって取得できる営業記録を一般交通機関、公衆宿泊施設、有体物倉庫、レンタルカー施設の営業記録に限定していた。第 215 条はこの制約を取り除いた。これにより通信事業者の通信記録が収集できるようになった。

---

[79] 人手による情報収集 HUMINT （Human Intelligence）は CIA が担当。
[80] 18 U.S.C. §§ 2522, 3121 and 47 U.S.C. §§ 229, 1001-1010.
[81] 47 U.S.C. § 1002(a).
[82] 50 U.S.C. § 1861.

② FISA 令状によって取得できる営業記録は、「外国勢力またはその代理人」に関係していなければならないという制約も撤廃した。取得できる項目も「記録」から「有体物すべて」に拡大した。これにより情報が蓄積されたコンピュータ情報も取得できるようになった。
③ 合衆国市民が表現の自由を保障した憲法修正 1 条の活動のみにもとづいて行動している場合の捜査は禁止した。
通信事業者の設備提供や技術支援に関しては現状を維持する（新たな義務を課さない）とした [83]。

FISC は NSA が 215 条にもとづいて通信事業者から電話番号（発信、着信）、通話時間（時刻、長さ）などのメタデータを収集することを認めてきた。司法省は 90 日毎に許可の更新を申請してきたが、FISC は 2006 年以来、継続して更新を認めてきた。FISC から令状を取得するには、政府はメタデータが國際テロリズム、スパイ対抗策、外国インテリジェンスに「関係する」（relevant）ものであることを示す必要があるが、政府はこの「関係する」を広く解釈していると批判されている。

(6) 愛国者法 505 条 [84]

愛国者法は国家安全書状（National Security Letter）についての改正も行った。国家安全書状は行政召喚状の一種で、政府が情報を入手するために使用する点は、令状や裁判所命令と同じだが、令状や裁判所命令のように裁判所の許可を必要とせず、行政府の判断で発出できる。

電子通信プライバシー法、金融プライバシー権法、公正信用報告法の 3 法は、FBI に国家安全書状によって電話加入者情報や預金者情報を入手することを認めた。愛国者法 505 条は、書状のあて先、調査対象、送付権限保有者などを拡大した。要求する情報がテロやスパイ行為の調査に関係すると政府が信ずる場合に発出できる。書状に対する守秘義務があり、政府から要求があったことを開示することが、損害を招くおそれがある場合は要求があったという事実も開示できない。

(7) FISA 改正法 702 条 [85]

後記 3.4 のとおり、ジョージ・ブッシュ大統領（ジュニア）は 2001 年 9 月 11 日に発生した同時多発テロ事件直後から、通信大手による令状なしの盗聴、通信記録収集を認めていた。後に新聞報道で暴露された事実である。これを受けて、議会は 2008 年に FISA を改正し、政府の傍受権限を基本的に拡大した。改正法 702 条は、国家情報長官と司法長官は共同して、国外にいると信じられる人物を対象にした諜報の取得を許可できるとした。1 年まで許可できるため、大量取得令状ともよばれている。

---

[83] 18 U.S.C. 3124 note.
[84] 18 U.S.C. § 2709.
[85] 50 U.S.C. § 1881a.

3.4 公権力が、事業者に対して「通信の秘密」に該当する通信記録等の保存を義務づけるまたは保存を要請する場合の法的根拠と手続き

FCC は現在、通信事業者に長距離通信の記録を 18 ヶ月間、保存するよう義務づけている。しかし、個々の通話についての料金を課されない定額通話の加入者にも適用されるのか否かは不明確である。後記 3.5 で紹介するオバマ政権の NSA 改革案によれば、通信事業者は裁判所の許可を条件に NSA にメタデータを提供しなければならない。このため、通信事業者は現在より長期間保存することや現在ビジネス目的で実施している方法と異なる方法で保存することには反対している。

3.5 前記 3.4 の問題に関しての議論、判例、注目すべき論点

① 最大の問題は、2013 年 6 月、NSA の元外部契約社員だったエドワード・スノーデン氏の内部告発で明るみに出た NSA による通信記録収集問題である。

② NSA による大量の通信記録収集問題が明るみに出たのは、実は今回が初めてではない。2001 年 9 月 11 日に発生した同時多発テロ事件直後から、ジョージ・ブッシュ大統領（ジュニア）は、テロリスト監視計画（TSP：Terrorist Surveillance Program）により、令状なしの盗聴、通信記録収集を認めていた。数年後の新聞報道ではじめて明るみに出た計画である。

③ 2005 年 12 月 16 日付ニューヨークタイムズ紙は、ブッシュ大統領の令状なしの通信傍受疑惑について報じた。それまで米国内に発着する國際通話や電子メールについては、令状を取得していたが、テロ容疑者と直接あるいは間接的に関係がある国際通信について、令状なしの通信傍受を 2002 年の大統領命令で NSA に許可していたと報じた。また、2006 年 5 月 11 日付 USA Today 紙は、NSA が通信事業者から、数百万の電話番号の通信記録を収集していたと報じた。提出を求められた大手 4 社のうちクウェストを除く 3 社が提出した。

④ いずれも憲法修正第 4 条違反のおそれのある行為に対して、ブッシュ大統領は憲法第 2 編に定める大統領権限と、テロ直後に大統領にテロリストに対する武力行使を認めた上下両院決議を根拠にあげた。ゴンザレス司法長官は 2005 年 12 月のニューヨークタイムズ紙の報道以来、一貫して TSP の合法性を主張し続けたが、2007 年 1 月、上院司法委員会委員長にあてた書簡で令状なしの通信傍受を取りやめると表明した。

⑤ NSA の要請にもとづいて通信記録を提出していた通信事業者に対しても集団訴訟が提起されていたが、FISA 改正法第 702 条（前記 3. 3(7) 参照）は通信事業者を免責した。こうして幕引きしたかと思われた TSP は、実は PRISM という新たな NSA のプログラムに置き換えられて復活していた。

⑥ 令状なしの通信記録収集がくり返される背景には、1979 年の最高裁判決がある[86]。その後の政府による通信傍受を正当化するのに大きな影響を及ぼした判決である。判決は被告

[86] Smith v. Maryland, 412 U.S. 735 (1979).

人が発信した電話番号に対するプライバシーを期待していたとしても、社会的には合理的なものとはいえないとした。理由として、(a) 被告人が発信した電話番号は、通話と同時に通信事業者という第三者に通知されるものである　(b) 通信事業者がその情報を事業記録として保存することは一般に知られている　ことをあげて、通信事業者による電話番号記録装置の設置は「捜索」にあたらないので、令状は不要であるとした。

⑦ この判例の考え方にもとづけば、NSA の通信監視が電話番号等のメタデータ収集にとどまるかぎり、プライバシー侵害、修正 4 条違反の問題は生じないことになる。その後、1986 年に制定された電子通信プライバシー法は、電子通信役務提供者による特定の場合の例外を除いて、FISA にもとづく令状なしの電話番号記録装置、捕獲・追跡装置の設置・使用を、原則として禁じた[87]。しかし、911 同時多発テロ事件後に制定された愛国者法 215 条（前記 3.3(5)参照）、FISA 改正法 702 条（前記 3.3(7)参照）が政府の傍受権限を拡大した。

⑧ 2013 年 6 月、英米の 2 紙がスノーデン氏の内部告発にもとづいて、NSA による大量の通信記録収集について報じた。6 月 5 日付の英ガーディアン紙は、NSA が FISA 令状にもとづいて、米通信大手ベライゾンからすべての通話のメタデータ（発着信番号、日時、通話時間、その他の識別情報など）を収集していたと報じた。翌 6 月 6 日付のワシントンポスト紙は、NSA が PRISM とよぶ情報収集プログラムによって、米ネット大手のサーバから直接電子メール（通信内容も含む）、ネット検索の履歴などに関する情報を収集していたと報じた。NSA は令状なしにネット企業の通信網に侵入して情報収集した行為を、FISA 改正法 702 条（前記 3.3(7)参照）を根拠に正当化した。

⑨ 翌 7 月、愛国者法 215 条による通信記録やメタデータの収集を原則禁止する提案が下院で採決され、賛成 205 票、反対 217 票の僅差で否決された。

⑩ 8 月 9 日、司法省は「愛国者法 215 条にもとづく電話メタデータの大量収集に関する白書」（以下、「白書」）を発表[88]。FISA 令状を取得するには、政府はメタデータが國際テロリズム、スパイ対抗策、外国インテリジェンスに「関係する」（relevant）ものであることを示す必要があるが、政府はこの「関係する」を広く解釈していると批判されていたが（前記 3.3(5)参照）、白書は議会が 215 条制定時に広い解釈を想定していたはずだと弁明した。

⑪ 白書は NSA が国際通話だけでなく国内通話も含めすべての通話のメタデータを 2006 年 5 月から収集していた事実を認めたが、PRISM によって収集できる情報には通信コンテンツは含まれないので、通信の傍受や録音はできないとした。しかし、白書発表 11 日後の 8 月 20 日付ウォールストリートジャーナル紙は、NSA と FBI が 2002 年の冬期オリンピック大会で、通信会社クウェストの協力を得て、5 ヶ月間にわたり、ソルトレイクシティに発着する電子メール通信をコンテンツも含めて監視していたと報じた。

⑫ ProPublica（NPO）のウェブサイトは、過去 8 年間の政府の監視に対する主要な訴訟を

---

[87] 18 U.S.C. § 3121.

[88] Administration White Paper on NSA Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act http://publicintelligence.net/doj-bulk-telephony-collection/

38 件リストアップ　している[89]。2 件が連邦最高裁まで行ったが、最高裁は 1 件を原告適格がないとの理由で第 2 控裁判決を覆し[90]、もう 1 件は上訴を受理しなかった。

⑬ 1979 年の前記⑥の最高裁判決の後、1986 年に ECPA が制定され、通信の内容とそれ以外の通信に関する情報を区分して異なる規制を設けた（前記 1.3 参照）。スノーデン事件後、オバマ大統領が「通信内容」ではなく、「通信記録」を監視しているだけだと弁明したのもこの二分法に関係している。この二分法が修正 4 条に違反していないかについては、その後争われていなかったが、NSA の監視問題に対して 2 件の訴訟が提起され、メタデータ収集に対する修正 4 条違反問題が争点となった。2013 年末、2 つの連邦地裁が前記⑥の最高裁判決の適用をめぐって以下のような対照的な判決を下した。

(a) ワシントン DC 連邦地裁判決[91]

前記⑥の最高裁判決はその後の技術革新によって本件にはあてはまらないとし、メタデータ収集は不合理な捜索、押収を禁じた憲法修正第 4 条違反の疑いがあるとして、NSA の収集した通話履歴の破棄と今後の収集停止を命じた。ただし、国家安全保障上の重要案件であるとして執行は猶予した。

(b) ニューヨーク南連邦地裁判決[92]

前記⑥の最高裁判決をメタデータにも適用し、NSA のメタデータ収集は合理的かつ合法で、テロリストの攻撃を阻止するための重要な手段であるとした。 メタデータの収集は広範囲に及ぶが、テロ対策のための捜査の視野もかってないほど広い。犯罪捜査は事後でよいが、国家安全のための捜査は攻撃阻止のために事前でなければならない。時間的にも長期間にわたり、地理的にも広範囲となる点を指摘した。

⑭ 2014 年 1 月、オバマ大統領は NSA 改革案を発表。「情報収集は国防上必要。制度の悪用はなかったが、その恐れがあるため改革する」として、3 月 28 日までに具体策を策定するよう司法長官に指示したことを明らかにした。

⑮ 3 月末にオバマ大統領は以下の具体的改革案を発表した。

(a) NSA による大量の通信記録収集はやめる。代わりに通信事業者が一定期間、保存する。

(b) 政府は緊急時を除き、外国諜報監視裁判所（FISC）判事が国防上の理由から個別に許可した場合にのみ通信記録を取得できる。

(c) 政府が収集できる記録は 2 ホップ（ホップは当初の電話番号の発信先または着信先をたどる回数）までとし、その使い方も FISC が承認した最小化手続きに従う。期間も限定する。

(d) 議会が法改正するまでは現在のプログラムを継続する。

⑯ 議会にはすでにいくつかの法案が提案されていたが、2014 年 5 月、下院は以下のような合衆国自由法案を承認した。

(a) 愛国者法 215 条にもとづく通信記録の大量収集を停止し、記録は通信事業者に蓄積させ

---

89 http://projects.propublica.org/graphics/surveillance-suits.
90 Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).
91 Klayman v. Obama, Civ. No.13-0851 (D.D.C. December 16, 2013).
92 ACLU v. Clapper, No. 13 Civ. 3994 (S.D.N.Y Dec. 27, 2013).

る。
(b) 通信事業者は通常の通信記録保存期間を超えてデータを保存しない。
(c) 政府は通信事業者から通信記録を取得する際に、FISC の許可をとらなければならない。

4 日本法へのインプリケーション

前記 3.1 で紹介した司法傍受 v. 行政傍受、国内の犯罪捜査 v. 外国諜報収集の 2 つの区分は日本法にはない。また、通信内容とメタデータを区別して、メタデータである電話番号にはプライバシーは期待されないため、通信事業者による電話番号記録装置の設置は「捜索」にあたらず、令状は不要であるとした米最高裁判決のような判例もない。しかし、スノーデン事件で暴露された NSA のメタデータ収集問題に対して、この判決が適用されるかどうかは 2 つの地裁で判断が分かれた（前記 3.5 ⑬参照）。議会もプライバシー保護の観点からメタデータの収集には何らかの規制を加えるものと思われる。

テロ戦争の脅威も増す中、国家安全目的の行政傍受の必要性は大きい。米国だけでなく欧州諸国でも広く認められていることからも導入を真剣に検討すべきである。しかし、通信の秘密が憲法で保証され、司法傍受もかなり限定されている日本の現状から、一気に行政傍受を導入するのは困難が伴う。そこで、浮上してくるのが日本版 FISA である。捜査当局の権限濫用を防止するために令状要件は課すが、発出要件は緩和して国家安全目的の通信傍受をしやすくする FISA は、現実的な解決策と思われる。米国にならった国家安全保障会議（日本版 NSC）の発足に続いて、日本版 FISA の導入を提言したい。

第 2 章　英国

高橋郁夫（弁護士）

1 「通信の秘密」に関する法的規定

1.1 「通信の秘密」と憲法との関係

本調査においては、「通信の秘密」と憲法における規定が調査対象とされている。しかしながら、英国においては、この調査事項は、あまり意味がない。英国において、「憲法」というのは、基本的に、国家の仕組みの枠組みを意味するものとされる。従って、例えば、英国の憲法（The Constitution）の教科書を調べてみても、人権規定に関する記述は、一般的に存在しないので、この部分については、論じられていないということになる。

従って、どのような規定がなされているか、保護法益はどうか、ということじたいあまり議論をしても意味がないことになる。

1.2 「通信の秘密」の英国法のもとでの位置づけ

「通信の秘密」の英国法のもとでの位置づけを考えるのに際しては、コモンロー・制定法的な意義という観点から考える必要がでてくる。そして、それらの観点から論じられている概念に適用しうるように我が国での「通信の秘密」の内容を解釈するということが最初の作業とならなければならないことになる。

本調査においては、(1)事業者の行為規範(2)公権力の関与の二つの問題があること、また、保護の対象として、隔地者における意思伝達の問題であって、その意思伝達の内容およびそれに関連する事実関係が問題になることが示唆されている。

英国法の体系のもとでは、意思伝達の当事者間において、どのような保護があたらえられるのかというのは、コンフィデンス保護の法理において保護されることになる。

これ以外の問題について、特に、隔地者間において、どの程度の保護がなされるかどうかという点について、2000 年捜査権限規制法 （Regulation of Investigatory Powers Act 2000 ）（RIPA という）[93]の規制が参考になる。

また、電気通信のプロハイダが、どのような規定を遵守すべきかどうかという観点については、2003 年通信法（Telecommunications Act2003）とも深い関係を有するものである。

1.3 保護の対象およびその区分についての制定法の定め

(1) 枠組み

[93] http://security.homeoffice.gov.uk/ripa/about-ripa/
横山潔「イギリス「調査権限規制法」の成立 ―情報機関等による通信傍受・通信データの取得等の規制―」(外国の立法 214) (http://www.ndl.go.jp/jp/data/publication/legis/214/21402.pdf)に制定時の条文の翻訳がある。
漆原貴久「英国 2000 年捜査権限規制法（アメリカ犯罪学の基礎研究(97)）」(比較法雑誌 比較法雑誌 41(4), 161-174, 2008)日本比較法研究所

英国における上記の問題を検討する際には、通信の内容とそれ以外の区別が重要になる。そもそも、「通信（Communication）」というのは、用語からして、通信の内容の部分を意味するのであって、通信に関係する事実関係を含まないことになる。これらの区別が、明確になっているのは、法執行機関のアクセスに関しての法的な規制を論じた上記 RIPA であり、本稿においては、RIPA の記述を最初に検討することとする。

RIPA は、犯罪（テロリズムを含む）の予防のための監視および情報収集のための方策を定めている。RIPA の法目的は、犯罪（テロリズムを含む）の予防のための監視および情報収集のための方策の定めであるが、通信に関する傍受等の定めは、通信傍受、通信データの取得に関する一般法の定めとしての性格をも有することになる。具体的には、RIPA は、「通信の傍受」「通信に関連するデータの取得および開示」「監視の実行」「秘密人的諜報資源（covert human intelligence sources）の利用」「暗号もしくはパスワードによって保護された電子データへのアクセス」「コミッショナーの氏名およびこれらの問題の監督機関の設立」を定めている。この中で、通信に直接関係するものは、「通信の傍受」「通信に関連するデータの取得および開示」の定めであり、また、「暗号もしくはパスワードによって保護された電子データへのアクセス」も、暗号通信に対する法執行機関のアクセスという観点からは興味深いものである。

従って、法執行機関等が取得するものが通信なのか、それに関するデータなのかどうかというのが、最初に問題となることになる。法執行機関が通信の内容を取得する場合に関する規制は、RIPA の 1 章によって規制されている。一方、2 章（Chapter２）は、通信の内容以外のデータについての法執行機関の取得方法を定めている。

(2) 通信データの概念

この 2 章は、通信の内容以外のデータについては、「通信データ（communications data）」というタイトルのもとで、具体的な概念について論じている。通信データというのは、通信に関する内容以外のデータをいうが、これは、「トラフィックデータ」、「サービス利用情報」、「加入者データ」の 3 種類からなりたっている(RIPA 法 21 条(4)項)。（以下、通信内容以外について通信データということがある。）

具体的な定義としては、トラフィックデータは、「郵便もしくは遠隔通信システムの目的のために、発信人により、もしくは、それ以外により、通信に、含まれ、もしくは、付帯するデータであって、それにより送信し、されうるもの」と定義されている（同法 21 条(4)(a)）。具体的な内容については、省略する。

「サービス利用情報」は、「通信の内容を含まずに、(a)郵便サービスもしくは遠隔通信サービスの従事者または (b)遠隔通信サービスに関連し、または、従事者によって用いられる利用についてのすべての情報」と定義されている(同法の 21 条(4)(b))。具体的な内容については、省略する。

「加入者情報」は、「トラフィックデータおよびサービス利用情報以外で、郵便サービスも

しくは遠隔通信サービスを提供するものにより、保持もしくは取得された、サービスを提供される人に関連するすべての情報」と定義されている(同法 21 条(4)(c))。具体的な内容については、省略する。

これらに対して、「通信の内容」については明確な定義は定められていないが、上記 21 条(4)で定められた「通信データ」以外の情報をいうと理解することができる。

(3) 通信データへのアクセス

通信データの取得については、法執行機関が裁判所の関与なしで、これを求めることができることになっている。RIPA 第 22 条は、所管大臣又は行政府の長の権限について定めるとともに、通信データへの合法的アクセスを定める。この具体的な合法的アクセスについては、「Code of practice for the acquisition and disclosure of communications data」[94]が準備されている。同条(2)項によるとき、(a) 国防の利益（interests of national security）(b)犯罪の抑止，捜査，秩序の維持の目的（preventing or detecting crime or of preventing disorder） などの目的のために、「関連する公的機関」（同 25 条(1)）は、通信データを通信運営者に対して、取得または開示することを求めることができると定めている。

英国においては、通信データの取得・開示請求が、いわば、法執行機関等の判断のみでなされるために、どのようにこの濫用を防止するのかという制度がきわめて重要になってくる。具体的には、記録の取得、紛争処理と監督の問題ということになる。データの取得について、不服がある場合には、調査権限審判所に対して不服を申し立てることができるようになっている。この詳細は、同 65 条以下に記載がある。また、通信傍受コミッショナー(Interception of Communications Commissioner)が独立の監督をなす責任を負っている。

通信傍受コミッショナーは、法執行機関における通信データ取得の実務について、査察をなして報告をなしている。

(4) 通信内容へのアクセス

上記の通信データに該当する情報以外を強制的に取得しようという場合(すなわち、通信内容を取得したいという場合である)は、別である。これらについての英国のもともとの定めは、"Interception of Communications in the United Kingdom" (CM 4368) published on 22 June 199 であった。

これは、法的には、「傍受」および「記録の取得」の二つの場合がある。

ここで、RIPA では 1 条は、「違法な傍受(Unlawful Interception)」を禁止している。

同条(1)は、「何人も、連合王国の場所において、次の各号の 1 により、ある者が通信の伝送の過程で、故意に、かつ合法的な許可を得ないで通信を傍受することは、犯罪である。

---

94 https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

(a) 公衆郵便業務
(b) 公衆遠隔通信システム」としており、また、同条(2)においては、私的遠隔通信システムでの傍受が犯罪に該当することが定められている。ここで、傍受とは、同 2 条(2)において、「通信が伝送されている間(while being transmitted)に、通信の送信者又は想定受信者以外の者に通信の内容の一部又は全部を利用させるために、
(a) 当該システム又はその管理を変更し、又は妨害すること
(b) 当該目的のために、当該システムによって行われた伝送をモニターすること
(c) 当該目的のために、当該システム中に含まれる装置へ、又は装置から無線電信によって行われる伝送を監視すること行われる伝送を監視すること
おこなわれる伝送をモニターすること」
をいうものとされている。

そして、同 2 条(7)は、この「遠隔通信システムによって通信が伝送されている間とは、通信が伝送されている、又は伝送されていたシステムが、(想定受信者が通信を収集/アクセスすることができる方法で)通信を記録するために用いる時間を含むものとみなす」としている。この条文は、Web ベースのメッセージやポケベルメッセージで読まれる前のものについては、傍受が成立する[95]ということを物語っている。

法執行機関（具体的な申請者は、同 6 条(2)に記載されている）は、この傍受にあたる場合、傍受令状を取得しなければならない。この傍受令状は、いわば、法執行機関等の上級の職員による申請に基づいて(同法 6 条(1))、裁判所が発布する。傍受令状は、国務大臣の署名に基づいて発付されるか、上級職員の署名に基づいて発付される（7 条(1)）。

その一方で、通信内容が記録された記録についていえば、法執行機関は、捜索令状によらずに、Police and Criminal Evidence Act 1984 等における提出命令(production order)もしくは、捜索令状によって取得することができる。提出命令は、権限あるものによる嫌疑の記載とともになされれば足りる。

1.4 刑事罰の適用について

上記規定に従わない場合のアクセスに対しては、刑事罰が適用されることになる。

通信データへの違法なアクセスについては、RIPA において、刑事罰の準備がなされていない。

その一方で、違法な傍受に関しては、RIPA2000 は、その 1 条 7 項において、刑事罰をさだめる。具体的には「(7) 第 1 項又は第 2 項に基づく罪により有罪となった者は、次の各号の定めるところに従う。
(a) 正式起訴に基づく有罪宣告により、２年以下の拘禁若しくは罰金に処し、又は両者を併科する。

[95] ただし、特定の場合には、記録通信として、提出命令が発布される場合があり(Police and Criminal Evidence Act 1984 の別表 1 の場合など)、その場合は、傍受に対する例外となる。

(b) 略式起訴に基づく有罪宣告により、法定上限以下の罰金に処する。
と定めている[96]。

2 ISP の「通信の秘密」への関与に関する法的規定

2.1 電気通信プロバイダに対する行為規制による通信のコンフィデンスの保護

上記は、英国における我が国における「通信の秘密」保護に相当する問題に対する基本的な枠組みを見るために、捜査当局が、どのような規制のもとに、通信内容や通信データにアクセスしうるのかという問題から、我が国における「通信の秘密」の保護のおよぶ範囲について検討した。しかしながら、電気通信プロバイダが、利用者との間で締結する電気通信サービス利用契約において、通信に関するプライバシに関する事項がどのように保護されるのかという観点から、論じられる問題もある。これらの点についての英国における基本的な規制の枠組みは、データ保護法 1998 とプライバシおよび電気通信（EC 指令）規則 2003（SI 2003/2426）（PEC 規則）である。そして、それに、2003 年通信法や上記の RIPA 等が基本的な枠組みを構築していることになる。

データ保護法 1998 については、我が国においても基本的な紹介がなされており、そこに譲ることにする。データ保護法と通信の秘密の関係において、もっとも興味深い問題としては、IP アドレスが、同法第 1 条に定められた個人データに該当するかを検討する必要がある。

「個人データ」とは、自然人に関連するデータであって、
(a) そのデータから、又は
(b) そのデータ及び当該データを管理する者が保有している、又は保有する可能性のあるその他の情報と相まって
当該自然人であると特定されるデータをいい、当該個人に関する意見の表明及び当該個人に関してデータ保有者その他の者が行う意思の表示をも含む。
と定義されているところである。EU における 29 条作業委員会においては「個人データの概念に関する意見書（2007 年 4 月）」を発行し、その中で「当ワーキングパーティは IP アドレスについて特定可能な個人に関連するデータであると考える」 としている。英国においては、一般的に具体的な状況によるものと解されている。情報コミッショナーは、個人データの判断に関する実務規範を明らかにしている。その規定などをもとにするときに、特に、関連する機器の性質が関連すると解されていると考えられる。もし、iPhone に関するデータであれば、その機器が、特定の個人に関連づけられているのであり個人データと解される可能性が高いのに対して、図書館におけるコンピュータの IP アドレスであれば、個人データとは考えられにくくなる。

電気通信に対する政府の規制の枠組みを定めた 2003 年通信法は、「枠組み指令(2002／21

[96]横山 潔「イギリス「調査権限規制法」の成立―情報機関等による通信傍受・通信データの取得等の規制―」（http://www.ndl.go.jp/jp/data/publication/legis/214/21402.pdf）

／EC)」、「認証指令(2002／20／EC)」、「アクセス指令(2002／19／EC)」、「ユニバーサル・サービス指令(2002／22／EC)」の４つの指令に対応し、また、通信・放送分野を横断的に監督する通信庁（OFCOM;Office of Communications）の規制権限を定めるものである。同法においては、OFCOM は、公共の電子通信プロバイダ（Public Electronic Communications Service）と顧客との取引契約約款の有効性に関する指針を明らかにすることができ、そこで、顧客の通信の伝達に際して、プロバイダがなしうる事項が規制される仕組みが構築されることになる。

また、プライバシおよび電気通信（EC 指令）規則 2003（SI 2003/2426）（PEC 規則）は、EU の e プライバシ指令(2002/58/E.C)に対応して、種々の問題に対する対応の枠組みをさだめたものである[97]。ダイレクトマーケッティングに対して、どのような利用をなしうるか、クッキーの利用、トラフィックデータの消去義務、請求書情報、位置情報それぞれについての定めがなされている。

2.2 個別問題に対する対応

本調査においては、迷惑メールのフィルタリング、帯域制御、DDos 攻撃等情報セキュリティに関する攻撃に対するトラフィック遮断、違法コンテンツに対するアクセスブロッキング、行動ターゲッティング広告などが調査項目として提案されている。

これらに対しては、本調査に協力してくれたヤフーUK から、寄せられている回答をもとにするとき、個々の問題についての英国の対応は、以下のとおりである。

(1) 迷惑メールのフィルタリング

これについては、それぞれのプロバイダが、迷惑メールのブロッキングをなしており、それらは、いろいろな技術に基づくものである。メタ・データ（例、IP アドレス）に基づく場合においては、データ保護法との関係が生じる場合以外を除いては法的な問題は生じない。通信の内容による場合においては、傍受となるので、RIPA 法との関係から、サービスの利用規定に関してなされるか、システムの無権限使用を調査するためであれば、許容されることになる（適法業務規則 2000 、Lawful Business Practice Regulations 2000）。顧客の同意がかならずしもいるわけではないが、上記法制度からは、事前におけるノーティスが必要とされる。

(2) 帯域制御

英国において帯域制御は法的に禁止されているわけではなく、実際に導入されている。法的には、公共電気通信サービス（PECS）を提供するものとされる場合には、契約条項として、導入する旨の情報を提供しなければならない。これは、2003 年電気通信法の一般契

[97] 情報コミッショナのホームページに説明がある
(http://ico.org.uk/for_organisations/privacy_and_electronic_communications)。

約条項（General Conditions of Entitlement (‘GCE’)）の 9.2(e)によるものである。この規定は、「明確で、理解しやすく、アクセスしやすい形態」でなされなければならない。

(3) DDos 攻撃等に対応するトラフィックブロック等

DDOs 攻撃に対するトラフィックブロック等の手法については、具体的に明確にされているものとはいえないが、そのような手法を採用する場合には、上記の一般契約条項の「通信プロバイダにおいてセキュリティもしくはインテグリティのインシデント、脅威、脆弱性に対する手法のタイプ」として、顧客に対して、情報が提供されなければならないことになる。

(4) 違法コンテンツに対するアクセスブロック

児童虐待のコンテンツに対するアクセスは、IWF(Internet Watch Foundation)の提供する自主規制スキームによってブロックされている。また、Google やマイクロソフトなどのサーチエンジンは、自主的な取り組みとして、特定の検索語をブロックするようにした。裁判所は、特定のプロバイダに対して、著作権侵害のコンテンツを含むサイトへのアクセスをブロックする義務を課してきている(e.g. Golden Eye & ors v Telefonica [2012] EWHC 723 (Ch))。

(5) 行動ターゲッティング広告

行動ターゲッティング広告という用語自体多義的な文脈で利用されることになる。これらの許容制は、個人データ保護法のもとで許容性が論じられることになる。

ディープパケットインスペクションは、傍受に該当すると考えられており、(1)でふれた根拠に基づいて許容されないかぎり、違法であると考えられる。そのため、この違法性の問題が、一般化の妨げになっているものと考えられる。

この場合、サービスプロバイダの利用に関する条件やプライバシポリシにおいて、個人データが収集される(ヘッダ情報インスペクション)方法や、利用され方(マーケット分析)が、詳細にされることになる。

(6) TOR(オニオン・ルータ)の取扱

英国においては、匿名通信技術に関して、法的な契約は存在しない。

本調査においては、これらの事項に対する法的な解釈論をともなった詳細な分析は、困難なところであり、今後の課題となるということができる。

2.3 保護の時間的範囲

ここで、便宜上、保護の時間的範囲としたが、我が国における電気通信事業法４条が、

通信の範囲が、「電気通信事業者の取扱中に係る通信」となっていることと比較して、発信者の意思の生成から、受信者の意思の受領のうち、どのような範囲まで、上記制定法によって保護されているのかという問題である。

この点については、傍受については、「遠隔通信システムによって通信が伝送されている間」という概念が適用されることは、上述した。それ以外については、記録の取得の問題となるので、電気通信に関するプロバイダにおいて保持されるかぎりにおいて保護されることになる。

3 公権力の「通信の秘密」への関与に関する法的規定

3.1 問題提起について

本調査においては、「通信の秘密」に対して、「公権力」が、犯罪捜査のためにアクセスする場合とテロや国家安全保障の場合とで、どのような相違があるのか、という点が提起されている。

まず、英国においては、制定法上、テロリズムについての定義が与えられている。英国は、北アイルランド紛争およびテロリズム防止法 1974 の時から、テロリズム防止法の経験を有している。これらの法律は、警察に創作、逮捕、拘留の特別の権限を認めていた。そして、これらの権限は、国際テロにまで拡張されてきた。その一方で、冤罪事件も引き起したことなどにより批判もあり、また、北アイルランドでの和平交渉の進展により、テロリズム法 2000 へと法が改正され、その後、2001 年反テロリズム、犯罪及び安全保障法（Anti-Terrorism, Crime and Security Act 2001 ）、2005 年テロリズム防止法、2006 年テロリズム法、2008 年テロリズム法などによる改正がなされている[98]。テロリズムの定義については、(1)行動もしくは脅威が、人、財産、生命等、電気システムに対する暴力・損壊等であること (2)政治的、宗教的、イデオロギー的な原因を意図するものであること(3)政府等に対する影響を与えようとするものであることが求められている。

3.2 通信に関するアクセスについて

もっとも、このようなテロ対応の方策が進んでいるとしても、通信に対するアクセスの規制法規は、上記 RIPA であり、これによる規定については、特段に異なるものではないことになる。

国家安全保障を理由とするアクセスについていえば、一般的に、このような任務を司る SIS の長官も、RIPA の規制に従うべきことが定められていることは上述した。なお、英国においては、米国におけるような諜報機関が、米国外において、米国法規に縛られることなく自由に活動しうるのが原則であるというような理論は、採用されていないように思わ

[98]岡久　慶「英国 2006 年テロリズム法―「邪悪な思想」との闘い」（http://www.ndl.go.jp/jp/data/publication/legis/228/022806.pdf）

れるが、この点については、今後の研究課題であるということがいえる。

3.3 通信データの保持に関する規定

本調査事項については、「通信の秘密」に該当する通信記録等の保存を義務づけ、または保存を要請することは、どのような場合に認められ、どのような手続が必要とされているかという点が質問されている。

この点については、英国においては、データ保持(EC 指令)規制法 2009 は、通信データの保持を規定している。同規制法は、公共の通信プロバイダは、インターネットの特定の通信データを保存しなければならない（付表　3 部(Schedule Part 3)）と定めている。詳細については、省略する。

第 3 章　ドイツ

笠原毅彦（桐蔭横浜大学）

1「通信の秘密」に関する法的規定

1.1 基本法と G10 法（信書、郵便及び電信電話の秘密の制限のための法律）

ドイツにおける電気通信に関する規制の法律は、度重なる改正により変遷を重ねている。

その変遷と議論からは、日本法に示唆する内容も多く含まれることから、まず簡単にその経緯に触れる。

1968 年の緊急事態法制の一環としてなされた基本法 10 条の改正と、「基本法 10 条関連法（G10 ― 以下「G10 法」と略す。）」に遡る。この改正により、基本法 10 条 2 項に第 2 文が追加され、「(信書の秘密ならびに郵便および電気通信の秘密の）制限は、法律に基づいてのみ行うことができる。その制限が、自由で民主的な基本秩序の擁護、または連邦およびラントの存立もしくは安全の擁護のためのものであるときは、法律により、その制限が当事者に通知されないこと、および裁判上の方法に代えて、議会の選任した機関および補助機関によって事後審査を行うことを定めることができる」とされた。

この改正と G10 法により、「安全保障のための通信傍受」が認められた。その内容として、「国またはその民主的秩序を脅かす特に重大な犯罪行為を計画し、実行し、完了したという嫌疑についての手がかりが成立する場合」（2 条 G10）の個別的解明と、「国に対する武力攻撃の危険を早期に認識し防御するため」(3 条 G10)の戦略的監視の 2 つが認められた。

G10 法は、1994 年に改正され、「安全保障のための通信傍受」だけでなく、一定の犯罪に関しては、「犯罪捜査のための通信傍受」もその対象となった[99]。また、「個人関連データの不利益利用」を認めることになった。個人関連データは、特定の犯罪行為の阻止、解明、または訴追のため、連邦及び州の憲法擁護庁、軍防諜部、税関刑事局、連邦輸出局、検察、警察に対する引き渡しが認められるようになった（7 条)。

司法は関与せず、裁判所の命令も不要とされる。また、組織も連邦情報局（Bundesnachrichtendienst BNDG）で、日本でいう内閣府（Bundeskanzleramt）に置

[99] その後, 1999 年 7 月 14 日連邦憲法裁判所第 1 法廷違憲判決を受けて, 2001 年 6 月 26 日大幅改正(BGBl I, S.1254)，2002 年 1 月 9 日にテロ対策法による改正（BGBl I, S.361）がなされている。特に 2001 年の改正は，同名の新法を定めた。G10 法 2 条 3 文は，通信事業者（と郵便事業者）の義務を定め，連邦情報局の求めに応じて，通信の「詳細な状況（näheren Umstände)」に関する情報を提出し、通信の監視と記録を可能にする措置を取らなければならないとしている。通信傍受を前提とした法律であり，特にトラフィックデータに関する規定は置いていないが，「詳細な状況」に含まれる。申立権者は，連邦と州の憲法擁護局（Verfassungsschutzbehörde)，軍防諜局（Militärische Abschirmdienst)，連邦情報局の 4 者のみに限定されている。主な規定は以下の通り。

個別的制限の対象となる犯罪の拡大（第 3 条)，通信技術の進歩への対応（第 5 条)，戦略的制限の対象としての通貨偽造（第 5 条)， 戦略的制限で得たデータの刑事訴追官庁等への伝達（第 7 条)，伝達された全データへの標識付与の義務付け（第 4 条、第 6 条)，通信の秘密の制限を受けた者への告知（第 12 条)，基本法 10 条審査会の設置，制限措置の統制の強化（第 15 条)，外国における身体及び生命を脅かす誘拐の解明措置（第 8 条)

詳細に関しては，渡邉斉志，「ドイツ「信書、郵便及び電信電話の秘密の制限のための法律」の改訂」参照。http://www.ndl.go.jp/jp/data/publication/legis/217/21703.pdf

かれ、警察機能を付加することはできない（G10 法 1 条 1 項)。

1.2 1997 年マルチメディア法から 2007 年テレメディア法まで

(1) 刑法上の違法文書[100]

新しいメディアが出現するとまず欲望産業がこれを取り込み、それがまたメディアの普及に弾みを付けるのは、洋の東西を問わないように思われる。ドイツでもインターネットの普及に伴うポルノ問題が、他の問題に先駆けて立法の原動力となった。日本と異なり、他の欧州諸国同様ドイツでも、通常のポルノに関しては、1974 年の刑法改正以来、成人に対する頒布等は禁止されていないため、青少年に対する頒布の禁止が問題となる。このため日本法との比較のためには、青少年保護法関連の規制も検討の対象とする必要がある。後述する。

また、州ごとに有害なメディアサービスの監視のためのに「青少年保護ネット（Jugensd-schutz.net)」が設立された。同様に、インターネット・プロバイダ企業も「社団法人マルチメディアサービスプロバイダ自主規制委員会（Freiwillige Selbstkontrolle Mutimedia-Dinestanbieter: FSM)」を設立し、独自の自主規制規格を作成した。

(2) 刑法上の通信の秘密

刑法 202 条は封印された手紙及び文書の開披罪を規定し、1 年以下の懲役または罰金、若しくは併科を定める。同様に刑法 202 条 a は、権限のない者が見ることができないよう措置を講じた他人宛てのデータを、パスワードを回避する等の手段で不正に取得した場合、3 年以下の懲役または罰金、若しくは併科を定める。

刑法 202 条 b は、技術的手段を用いて、非公開のデータ通信またはデータ処理装置の電磁気から、他人宛のデータを不正に取得した者は、2 年以下の懲役または罰金、若しくは併科を定める。刑法 206 条 1 項から 3 項は、信書または通信の秘密を守らなければならない者がその秘密を犯す罪を規定し、5 年以下の懲役または罰金、若しくは併科を定める。同様に、同条 4 項は守秘義務がない公務員が通信の秘密を犯した場合に 2 年以下の懲役または罰金、若しくは併科を定める。元々通信･郵便関係は国営で、守秘義務のある公務員とない公務員で 5 年の 2 年の差があったのが、民営化され公務員の地位がなくなっても 5 年のまま残されている。

(3) 1997 年マルチメディア法

ドイツでは、1997 年に世界に先駆けて、インターネットを中心とするネットワークに対

100 刑法が禁じる「文書」には，以下がある。
「闘う民主制」に反する宣伝（刑法 86)，憲法違反の団体の標章の使用（刑法 86a 条)，殺人、人間性に反する犯罪、傷害、強盗・脅迫，公の平穏を害する犯罪を促すもの（刑法 126 条 1 項)，民衆煽動的文書の頒布（130 条)，暴力表現（131 条)，青少年へのポルノ文書の頒布（刑法 184 条)，暴力行為又は獣姦淫行為の描写物の頒布（刑法 184a 条)，児童ポルノの頒布・入手・所有（刑法 184b 条)，青少年ポルノの頒布、入手、所有（刑法 184c 条)，青少年へのメディアを通じたポルノ提供（刑法 184d 条)

応する法制度を制定した。1997 年 7 月 22 日情報通信サービスの枠組みを定める法律 （以下「マルチメディア法」)、1997 年 8 月 1 日メディアサービスに関する州際協定である。基本法の制約から、電気通信、経済、著作権に関しては連邦が、新聞、雑誌に関しては州に立法権があるため、二つの法律が制定されたが、プロバイダの責任に関しては、ほぼ同じ条文がそれぞれに置かれている。

マルチメディア法第一章「テレサービスの利用に関する法律（以下、「テレサービス法)」は、第 2 条第 1 項で、「以下の規定は、通信手段を伝送手段の基盤に持ち、文字、図案または音響のような相互に関連付けられるデータの私的利用を目的とするすべての電子的な情報サービス及び電子的な通信サービス (テレサービス) について適用がある」と規定した[101]。

第 3 条にはプロバイダの定義を置いた。

「この法律において、サービスプロバイダとは、自然人もしくは法人または人的団体であって、利用に向けられた自己もしくは他人のテレサービスを実施し、または利用へ向けられた接続を媒介するものを意味する。」

州が管轄する従来からの放送、新聞、出版等のマスメディアからテレサービスを区別し、電気通信事業者に対してでなく、電気通信を利用する情報の伝達サービスを行う者のサービスを規制するもので、そのためにテレサービスという概念を作る意欲的なものであった。しかし、当初からその区別が懸念されていたように、その後のネットワークの進展と普及に伴い、両者の区別は曖昧なものとなり、2002 年以降の法改正へと繋がっていく。

(4) 2002 年「青少年保護法」「青少年メディア保護州際協定」[102]

青少年保護法は、14 歳未満を「児童」、14 歳以上 18 未満を「青少年」と定義している（1 条 1 項)。州法で規制される「放送」を除いて、「パッケージメディア (Trägermedien)[103]」と「テレメディア (Telemedien)」に分け、前者は物的な媒体に記録され携帯・頒布に適したものに記録された文書・画像・音声を指す（第 1 条 2 項)。後者は、テレメディア法で定義された他の全てのメディアを指す（1 条 2 項、3 項）[104]。「連

---

101 具体的には以下の通り，
・個別通信の領域における提供（たとえば電子バンキング、電子データ交換)、
主として一般大衆の意見形成に重きを置いた編集物以外の、情報または通信の提供 (データ・サービス)、
・インターネットまたは広域ネットワークの利用の提供、電気通信による諸々の利用の提供、双方向的で直接的に接続可能な機能を持った電子的で即答的なデータバンクにおける物品供給またはサービス供給の提供（「無償であるか有償であるかどうかを問わず、適用がある」（第 3 項))

102 「Jugendschutzgesetz-2002」，Jugendschutzgesetz-Jugendmedienschutz-Staatsvertrag」
詳しくは，内閣府政策統括官（共生社会政策担当）「アメリカ・ドイツに於ける青少年のインターネット環境整備状況等調査報告書」
http://www8.cao.go.jp/youth/youthharm/chousa/h22/net-us_de/index.html

103 鈴木秀美「メディア融合時代の青少年保護 －ドイツの動向―」，慶應義塾大学メディア・コミュニケーション研究所紀要，メディア・コミュニケーション 61 号 21 頁以下では，「携帯メディア」と訳されている。

104 Bundesministerium für Familie, Senioren, Frauen und Jugend, "Jugendschutzgesetz und Jugendmedienschutz- Staatsvertrag der Länder" 11 頁参照。
http://www.bmfsfj.de/RedaktionBMFSFJ/Broschuerenstelle/Pdf-Anlagen/Jugendschutzgesetz-Jugen

邦と州の間で、原則として、連邦はオフラインコンテンツ、州はオンラインコンテンツについて有害表現規制を行うという合意が成立[105]」した形になっている。

青少年に有害なパッケージメディア（11 条～15 条）及びテレメディア（16 条）は、連邦青少年有害メディア審査会（連邦審査会 Bundesprüfstelle für jugendgefährdende Medien、 BPjM[106]）が「有害メディアリスト[107]（18 条)」に記載し、全面的に頒布禁止され、または[108]、あるいは同時に、官報で公表する[109]。

テレメディアについては、リスト記載決定の前に、連邦審査会は州の青少年メディア保護委員会（後述）の見解を求める（21 条 6 項)。また、リストに記載されたテレメディアの規制に関しては、州法に委ねられる（16 条)。

この法律に違反する者は刑罰（最長 1 年の禁固刑又は罰金）又は秩序違反の罰（最高 5 万ユーロの罰金）を科される（第 27 条、第 28 条)。

2 ISP の「通信の秘密」への関与に関する法的規定

2002 年の青少年保護法の改正で採用された「テレメディア」概念は、2007 年に電気通信法、テレメディア法の改正でも採用された。

一般的に電気通信を規制する法律として、電気通信法（Telekommunikationsgesetz、**TKG**[110]）とテレメディア法 （Telemediengesetz、**TMG**[111]）が制定されている。また、電気通信、経済、著作権に関しては連邦が、放送、新聞、雑誌に関しては州に立法権があるため、テレメディア州際協定*[112]*が締結されている。

電気通信法 3 条、24 条は、電気通信サービスを「通常において、電気通信もしくは、放送に用いられる通信サービスを含むネットワークにおける信号の伝達に対して報酬を得て提供されるサービス」と定義している。一方、テレメディア法は、この電気通信サービス

---

dmedienschutz-Staatsvertrag,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf

105 コンピュータのように，メディアの再生・頒布双方が可能な場合，記録されたメディアを再生し，青少年に観賞させる場合はパッケージメディア、そのメディアを電子頒布する場合はテレメディアと定義される。鈴木秀美前掲（注 6）23 頁参照

106 http://www.bundespruefstelle.de/bpjm/root.html

107 不道徳なもの，粗暴性を助長するもの，暴力・犯罪・人種間の憎悪を煽動するもの，及び殺人・殺戮等の暴力行為や，私刑を唯一の正当な方法と描写するもの（17 条，18 条 1 項)。ただし，政治的・社会的・宗教的内容に関わるものは，その内容ゆえに記載してはならず，芸術・学術的研究に寄与するもの及び公共の利益に資するもので，その手法・表現が不適切でないものは記載してはならない（18 条 3 項）

108 「極めて有害な」パッケージメディアは、リストに記載されなくとも青少年への提供等を禁止する（第 15 条 2 項）：1. 刑法第 86 条（憲法違反の組織を宣伝するもの)、第 130 条（特定の集団への憎悪を煽動するもの、ナチス犯罪を賞賛又はその存在自体を否定するもの)、第 130a 条（罪を犯すと脅迫して公の平穏を害するもの)、第 131 条（非人間的な暴力を賛美するもの）又は第 184 条に違反するもの（ポルノグラフィー)，2. 戦争を賛美するもの，3. 暴力自体を目的とした、特に真に迫った、残酷で凶暴性のある描写，4. 不自然で性を強調した姿勢をとる青少年の描写，5. その他青少年の発達に著しく有害であることが明白なもの

109 BPjM Aktuell - Amtliches Mitteilungsblatt der BPjM

110 Telekommunikationsgesetz v. 22. Juni 2004 (Neufassung BGBl. I S. 1190)

111 Telemediengesetz（TMG）v. 26. Februar 2007，1. März 2007 施行

112 「放送およびテレメディアにおける人間の尊厳の保護および青少年保護に関する州際協定」
Telemediendienste Staatsvertrag

の定義に該当しないすべての電子情報･通信サービスに適用される(テレメディア法 1 条)。「テレメディア」の概念は、放送とパッケージメディア以外の全てを含む広い概念になっている。一般の電子掲示板などは、テレメディア法の対象となるし、その一方で、ISP は、電気通信法の適用対象となる。もっとも、両法と「州際協定」は重複した規制になっている。

通信事業者が電気通信を取得、利用、共有する際についての規制については、電気通信法の 7 編「電気通信の秘密、データ保護、公共の安全」に規定されている。

まず、同法 88 条で通信の秘密、89 条で盗聴の禁止、90 条で不正利用の禁止を定める。

同法 88 条 1 項は、「通信の内容および詳細な状況（ihre näheren Umstände）（特に、人が電気通信を行っている、または、いたか否か）は、通信の秘密となる。通信の秘密には、更に、繋がらなかった接続（の試み）も含まれる。」と述べている。また、同 2 項は「すべてのサービス提供者（Dienstanbieter）は、電気通信の秘密を維持しなければならない。その義務は、業務終了後も継続する」と定めている。

その上で、同法 96 条は、サービス提供者は、この章に述べられている目的のためにトラフィクデータ（Verkehrsdaten）を利用することができると規定している。ここで許容される目的としては、請求目的（97 条、99 条)、故障・不正行為調査（100 条）があげられている。トラフィックデータは、電話番号、接続の開始・終了に関する日付、時間、場所、データ量、ユーザ、設定・維持のためのデータをいうとされている（96 条)。

また、同法 111 条は電気通信事業者に対して、顧客の個人データ（氏名、住所及び生年月日等）の収集を義務付けている。

3 公権力の「通信の秘密」への関与に関する法的規定

3.1 G10 法に基づく犯罪捜査

G10 法に該当する犯罪[113]の場合、その阻止、解明、または訴追のため、電子メールも含めて連邦情報局（BND）に通信傍受を認めている。そこで得られた情報は、連邦及び州の憲法擁護庁、軍防諜部、税関刑事局、連邦輸出局、検察、警察に対する引き渡しを認めている。また、2006 年に連邦及び州の警察及び情報部局共通データベース設置法（BGBl I、S. 3409）で G10 法は改正され、それらの機関でデータが共有されている。この法律の範囲内で、通信内容も含めて記録を取り、関係省庁間で共有することができる。

G10 法 15 条で、10 条審査会（G10-Kommission）を設置し、G10 法に基づく通信傍受活動を統制することを目的とする。連邦議会に置かれる委員会である。情報の収集、加工及び利用等、通信の秘密を制限する措置の全体の統制にあたるとされ、広範な権限が明記されている。また、申立権者でもある憲法擁護局を規制する憲法擁護法第 12 条により、擁護局は、最長で 10 年の個人情報の保存期間を定めることができ、この期間を経過した場合

[113] カタログ犯罪（Katalogstraftat）と呼ばれ，G10 法では国際テロ（3 条 1 項 2 号)，兵器の国際取引（3 条 1 項 3 号)，ドイツへの薬物輸出（3 条 1 項 4 号)，外国での通貨偽造（3 条 1 項 5 号)，3-5 号の行為に関連した資金洗浄（3 条 1 項 6 号）を挙げられる。

は、データは消去される。

3.2 G10 法に基づかない犯罪捜査

(1) 司法傍受

刑事訴訟法（StPO）100 条 a1 項により、同条 2 項に規定する「重大な犯罪（39 類型）」を犯したとの「特定の事実（bestimmte Tatsache）」が存在する場合、当事者に知らせることなく通信を監視し、記録することができる。この場合、検察官の申立に基づく裁判所命令が必要とされる（同法 100 条 b1 項 1 文）。緊急の場合は、検察の判断で命じることもできる（同項 2 文）が、3 営業日以内に裁判所がこれを追認しなかった場合効力を失う（同項 3 文）。また、この命令は、3 か月以内に限られ（同項 4 文）、延長も 3 か月に限られる（同項 5 文）。以上の場合、通信の内容に関しても記録することができる。

刑事訴訟法 100 条 g で、上記犯罪の未遂、予備の段階、または、通信を利用した犯罪の場合は、トラフィックデータを取得することができる。上述した裁判所命令の規定が準用される（刑訴 100 条 g 2 項）。

(2) 電気通信法上の犯罪捜査協力規定

電気通信法 111 条はプロバイダに顧客の個人データの収集を義務付けているが、112 条と 113 条で、官庁への情報提供義務を定めている。112 条は「自動照会手続（Automatisiertes Auskunftsverfahren）と呼ばれる。通信事業者に対して、連邦情報局が裁判所、検察、警察、情報機関等の要求に応じて、通信事業者に分からないように事業者のシステムから個人データを抽出し、提供することができるようにする措置を義務付けている。113 条は個別照会手続（Manuelles Auskunftsverfahren）と呼ばれる。同条第 1 項第 1 文で、通信事業者に対し、危険防止や刑事訴追のために、所管機関の要求に応じた個人データの提供を義務付けている。更に、同条第 1 項第 2 文は、通信事業者に対し、警察等捜査機関の要求に応じた顧客の個人情報、パスワード、IP アドレスの提供を義務付けている[114]。

3.3 IP アドレス・トラフィックデータ・通信内容・個人情報に関して

通信内容（Inhalt der Kommunikation）とトラフィックデータ（Verkehrsdaten）[115]，通信者情報（Bestanddaten）が、区別され、通信傍受を除いては通信の内容を取得するこ

---

[114] 連邦憲法裁判所 2012 年 1 月 24 日の一部違憲判決（1 BvR 1299/05）を受けて，要件を厳しくした。2013 年 6 月 20 日通信法個人データ保護関連規定の改正法（Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl. I S.1602)による。詳細に関しては，渡辺 富久子，「【ドイツ】通信法の個人データ保護関連規定の改正」立法情報，外国の立法 (2013.10)，参照。

[115] トラフィックデータは，まず，電気通信法 3 条 30 号で規定され，以下のものがある（電気通信法 96 条 1 項，113 条 a)。利用された通信サービス，発信者･受信者の番号ないし標識，個人に与えられた利用番号, 顧客カード (Kundenkarte) を利用する場合のカード番号, (欧州サイバー犯罪条約では,「traffic Data」とされていない）携帯電話の位置情報，通話の日時，通信量。他に電気通信法 96 条, §113a (現在無効とされている。)，刑事訴訟法 100 条 g に規定があるが，それぞれの目的に応じて範囲が異なる。

とはできない。トラフィックデータは，電話番号，メールアドレス，IP アドレス等，それだけでは基本的に匿名のデータであり，範囲も，目的に応じて細かく規定されている。通信者情報は，電気通信法 111 条に定義される[116]。電気通信法では，通信内容の取得を認める条文はなく，トラフィックデータと通信者情報の取得に関してのみ規制している。

(1) IP アドレス

連邦データ保護法 3 条 1 項は、「(1) 「個人データ」とは、特定された、もしくは特定しうる自然人（データ主体）の個人もしくは重要な状況に関するすべての情報を意味する」と定義をしている。この定義によると、IP アドレスは個人データと関連しうる。しかし、ドイツでの電気通信法やテレメディア法は、IP アドレスを利用できる場合を詳細に定め、許容目的以外には利用できず、例外的に利用できる場合でも匿名化するか、利用後抹消されなければならないため、元の IP アドレスは再現できない。その範囲で、IP アドレスはデータ保護法の対象である個人データであるとはいえない。また、情報主体の同意がある場合は問題が生じない。規定を遵守しない場合については、IP アドレスがデータ保護法の対象となることはありうる。

(2) データ収集･利用・捜査協力

ISP が、一般的に上記のトラフィクデータを収集・利用する場合、その目的が細かく規定されている。電気通信法 100 条 1 項は、「必要な場合、サービス提供者は、機器の故障又は障害を突き止め、特定し、それらを解消するために、通信者情報、トラフィックデータを、取得し、利用することができる」と定めている。「故障」概念は非常に広汎なものとして解釈され、機械的技術的障害のみではなく、インターネットサービスに対する妨害、例えば、DDoS、マルウエア、ボットの利用も含むと解されている。データの保有および利用は故障を「知る目的」でも許される。現実に故障・障害が起きている必要はない。

通信事業者は、個々の通信でなく自動化された（Automatisiert）形でトラフィックデータにアクセスできることができる。その上で、その利用、第三者移転等を制限する規定を置いている。また、テレメディア法 15 条 a は、「保存した情報の内容、または利用データが不法（unrechtsmäßig）に送信されたものであること、または、その他の方法で第三者が不法に取得したものであること、あるいは利用者の権利または保護されるべき利益の重大な侵害の虞があると判断した場合、連邦情報保護法 42 条 a を準用」し、その内容に応じた監督官庁と利用者に通知しなければならないとしている。

トラフィックデータはその利用が許されている場合，目的終了後，遅滞なく消去されなければならないとされている。故障の際は最大 7 日間に限定され，料金請求の場合は，異

[116] 電話番号(1 項 1 号)，氏名及び住所（1 項 2 号），自然人の場合誕生日（1 項 3 号），DHCP でない場合，その IP アドレス（1 項 4 号），モバイル機器の番号（1 項 5 号）と，その契約開始日（1 項 6 号）

議申立期間終了後遅滞なくとされる[117]。故障が存在しないかまたは故障の除去のためにデータを保存する必要性がないときは、少なくともＩＰアドレスは消去または変更しなければならない。これによってIPアドレスの正確な復元は不可能となる。

同項によって、攻撃者の探知が許容されるのかという点について検討する。コミュニケーションログによりコミュニケーションの経過が判別される。したがって、ISPは、かかるコミュニケーションログによって分析する行為ということになる。この場合、上記「故障」概念に、抽象的な 攻撃者のトラフィックの探知が含まれるかということになる。コッファー博士によると、電気通信法100条1項の前提となっている許可された利用目的のためのトラフィックデータのデータの保管と利用と考えられ、その場合には通信の秘密に反しないとする。

場合によっては、複数のプロバイダを経由することもあり、通信時業者間での情報共有の是非が問題になり得る。この点に関しては、ドイツにおいては特に規定が存在していない。電気通信法92条（後述）の反対解釈により可能と考えられる。

ただし、データ保護法があるため、通信「内容」を他の通信事業者と共有することはできない。通信事業者二社への聞き取りによれば、通信内容を除いたトラフィックデータは、Dos攻撃等異常な通信が発生した場合は、発信元をたどることになるが、発信者と受信者のリレーの形になり第三者提供の問題は生じないため、データ保護法に抵触しないと理解している。また利用者の同意があれば可能で、あらかじめ契約約款に定められることができる。

電気通信における外国の民間組織に対するデータ移転は、電気通信法92条によって、電気通信サービス対応、請求対応、不正行為対応のため以外には、禁止されているが、そこでの個人データは、連邦データ保護法の定義によるとされている。

更に、また、後述するテレメディア法13条は、サービスプロバイダの義務として、欧州連合域外でデータを利用する場合、契約当初にその詳細について教示しなければならないことを定め、電子的同意を得るための要件、消費者保護の観点からの契約内容の文言等詳細な規定を置く。しかし、国境をまたぐ個々の通信に関しては規定がない。

(3) データ保存

EUデータ保持指令に対応し、ドイツ政府は、「通信の監視およびその他秘密裡捜査対策ならびに2006/24/EG指令の適用に関する法律 」を制定した。この法律により改正された電気通信法113条aは、6か月のトラフィックデータの保存義務を定める。記録は、電話（2項）、電子メールサービスの提供者（3項）、インターネット接続業者（4項）モバイル接続業者（7項）に区分されている。

電子メールサービスの提供者は、送受信の場合、電子メールアドレス、送信者のIPアド

[117] Leitfaden der StA München von 2011によると，ドイツテレコムの場合短く，受信に関しては保存せず，発信に関して4日から80日で，顧客の希望による。これに対して，Vodefoneは，全てのデータを92日間，TelefonicaO2は，全てのデータを1日から7日，料金請求用のデータを8日から30日保存し，プロバイダによってその対応が異なるという。

レス、メール受信者の電子メールアドレスを、インターネット接続業者（ISP）は、インターネット接続に利用されたIPアドレス、接続した者のユーザ名、接続の開始・終了時刻を記録しなければならない。

モバイル接続サービスを提供する者は、更に基地局のデータと場所および主要な電波の接続先を記録しなければならない。但し、同条8項で通信内容及びウェブサイトの閲覧履歴をこの記録に残すことは禁じられている。また、113条bで目的制限の原則が採られ、犯罪捜査、公共の安全に対する危険の排除等の、当初の目的以外に使用することを禁じている。

同法は、2008年1月1日より効力を有して、すべての通信のデータは、6月の間にわたって、データが保持されなければならないとした。しかし、2010年3月2日、連邦憲法裁判所は、この法律は、EU指令の求めるものをはるかに超越しており、人々が監視されているのではないかという気持ちを引き起し、通信の秘密を侵害するものとして、かなりの部分が憲法に違反するとし無効とされた。また、2012年1月24日連邦憲法裁判所判決（1 BvR 1299/05）は、電気通信法111条「通信事業者の顧客の個人データ（氏名、住所及び生年月日等）の収集義務」、電気通信法§112「連邦ネットワーク庁が検察や警察、情報機関等の要求に応じて、通信事業者に分からないように当該事業者のシステムから個人データを抽出し、提供することができるようにする措置の義務付」電気通信法113条1項1号「通信事業者に対し、危険防止や刑事訴追のために、所管機関の要求に 応じた個人データの提供を義務付け」、電気通信法113条1項2号「通信事業者に対し、検察等の要求に応じた顧客のパスワードの提供を義務付」に関して、一部の規定は情報の自己決定権を侵害しているとして違憲判断を下した。この判決に対しては、2013年6月20日電気通信法個人データ保護関連規定改正で織り込まれて、違憲状態は解消した[118]。しかし、113条aと113条bに関しては違憲として条項は無効とされているが、まだ改正はなされていない。

EUとの関係で、ドイツはEUのデータ保持指令を遵守できていないとして、1日30万ユーロを超える罰金を支払わなければならなくなるおそれがある[119]。2014年1月には、Maas司法大臣は、導入を延期すべきであるという意見を述べ、これに対して、CDU/CSUは、早急に、制定法をさだめるべきと考えている[120]。また、ヨーロッパ人権裁判所においては、データ保持指令の条項がヨーロッパ人権条約に反するではないかと争われており、法務官（Advocate General）が、そのような趣旨の意見を述べたということも報道されていた[121]。司法省は、ヨーロッパ人権裁判所の判決を待って対応することを予定していたが、2014年4月8日、ヨーロッパ人権条約に反するとの判決が出された[122]。電気通信法113条a、bが、この規定に従って制定された条文だが、条文自体が効力を失っているため、効力

---

118 パスワードの取得のみ，裁判所の命令が必要とされた。

119http://www.out-law.com/en/articles/2014/january/german-minister-seeks-to-further-delay-implementation-of-eu-data-retention-laws/

120 http://euobserver.com/justice/122636

121 http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf

122 C-293/12　Judgment ECLI:EU:C:2014:238　08/04/2014

を失ったまま残されている上記条文が削除されるか、より要件の厳しい保存義務が制定されることになると思われる。

4 テレメディア法 ― プロバイダ特権と民事責任

4.1 プロバイダ特権

刑事犯罪に関しては、電気通信法で非常に広範な通信の秘密に対する制限を、しかし、詳細な規定を設けることで、認めているが、民事責任に関しては、テレメディア法で別途規定している。同法 7 条に総則規定を置き、1 項で、プロバイダ自身が情報を発した場合は通常の法律の適用を受けることを明記している。同時に 2 項で、他人の情報を伝達・保存した場合は、当該情報に違法な行為がないかを監視・調査する義務がないことを定めている。また、同法 8 条で他人の情報の伝達、同法 9 条で情報伝達の高速化のための一時的な保存、同法 10 条でプロバイダ自身が揚げたものでない情報に対する責任に関して規定を置き、原則的に責任を負わない旨規定している。これら 7 条から 10 条の条文を差して、電気通信事業者や郵便事業者同様のプロバイダ特権（Providerprivileg）と呼ばれている。

4.2 プロバイダの民事責任

プロバイダのサービス（Funktion）によって責任を区分している。

(1) コンテンツプロバイダ（Content-Provider）、ホスティングプロバイダ（Hosting-Provider）[123]

両プロバイダとも、オフラインのメディア同様、自らアップする等、その内容に責任がある場合は責任を負う。他者のデータを中継し、あるいは保存した場合の不作為については上述した同法 7 条 2 項の責任除外規定が適用される。プロバイダがその違法性を認識していた場合、または、判例により確立された原則であるいわゆる調査義務（Prüfpflicht）に基づいて、その違法性を認識しなければならなかったと判断された場合に責任を負う。認識がなかった場合で、認識後、遅滞なくコンテンツの除去を行った場合は責任を負わない（テレメディア法 10 条 2 項）。

(2) インターネット接続業者（Internet Service Provider）

単に技術的にネットワークへの接続を仲介するのみで、原則として責任を負わない。停止請求権（Unterlassungsansprüchen – 日本の差止請求権に相当）に関しては、判例は未だ確定しているとは言えないが調査義務の原則（Grundsätzen der Prüfpflicht）から、調査義務があるかないかが議論されている。（後述テレメディア法 15 条 a 参照）

4.3 プロバイダの個人情報保護

[123] ホスティングプロバイダの「ホスティング」概念は，Web Hosting 等，情報のホスティングも含み，日本でのコンテンツプロバイダの概念と広く重複する。

同法 11 条から 15 条 a まで、プロバイダ特有の個人情報保護の規定を置いている。その中で、12 条に原則規定を置き、他の法律がテレメディア法を明示して、個人情報保護の制限を認めている場合、または利用者の同意がある場合を除いて、他の目的に使用してはならないことを定め、目的制限の原則、情報主体の同意権を定めている。また、15 条で利用者の利用データの使用に関して、営業目的で利用する場合に匿名化することを課す等の利用に関する制限を詳細に規定している。

反対に、同法 14 条 2 項で犯罪捜査の目的等で、警察等権限のある官庁からの照会があった場合、電気通信法 113 条の「個別照会」の規定に対応して、プロバイダに利用者の個人に関する情報を提供する義務を定めている。更に 15 条 a は、保存した情報の内容、または利用データが不法（unrechtsmäßig）ないし違法に送信されたものであること、または、その他の方法で第三者が不法に取得したものであること、あるいは利用者の権利または保護されるべき利益の重大な侵害の虞があると判断した場合､連邦情報保護法 42 条 a を準用し、その内容に応じた監督官庁（Aufsichtsbehörde）と利用者に通知しなければならないとする。

英米法がディスカバリ等、訴訟手続法を通じて情報の開示を進めるのに対し、ドイツ法は実体法に開示義務を定めようとする傾向がある。

発信者情報の開示に関しては､既に 1992 年 3 月 25 日連邦憲法裁判所第 1 法廷決定[124]で、迷惑電話ではあるが逆探知の結果を民事裁判の証拠として利用することが認められている。しかし、利用者がプロバイダに対して民事裁判の遂行のための発信者情報の開示を求めることは、個人情報保護の観点から争われていたが、テレメディア法 15 条 a の追加で、特定しやすくなることが期待されている。

5 自己規制と流通規制

青少年メディア保護州際協定 (Jugendmedienschutz-Staatsvertrag (以下 JMStV と略す。)) [125]は，元々，州に規制権限がある放送に関する「放送州際協定」（1987 年）に遡る。1997 年に，いわゆるマルチメディア立法によって，インターネット上の有害情報にも適用されるようになった。

5.1 流通規制

放送及びテレメディア提供事業者に対する規制内容は，青少年保護法第 15 条 2 項の

---

124 詳細に関しては，連邦憲法裁判所判例集 85 巻 386 頁以下，廣澤民生，「ドイツ連邦郵便による迷惑電話の監視と電気通信の秘密－迷惑電話逆探知事件－」ドイツ憲法判例研究会編，「ドイツの憲法判例 2 第 2 版」38，246 頁以下参照

125 「放送とテレメディアにおける人間の尊厳の保護及び青少年保護に関する州際協定」(Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien v. 10. September 2002（JMStV），2003 年 4 月 1 日施行
http://www.kjm-online.de/recht/gesetze-und-staatsvertraege/jugendmedienschutz-staatsvertrag-jmstv.html 参照

内容を更に膨らませている（JMStV 4 条[126]）。しかし，刑法上犯罪となる表現と戦争賛美，人間の尊厳を侵害するような形で描写する表現（JMStV 4 条 1 項）を除いては，その対処の基本は，自主規制と流通規制である。テレメディアでは，ユーザを成人に限定すれば提供が許される有害表現（例えばソフトポルノ）が規定されている（JMStV 4 条 2 項）。

テレメディア州際協定は、コンテンツプロバイダに対し、青少年の成長を阻害するコンテンツについて、青少年の年齢に応じてアクセスを限定する措置を配慮することを義務付けている（JMStV 5 条 1 項）。

具体的には，

1. 青少年の発達を損なう内容について、その享受に適さない年齢層の利用を技術的措置により排除又は困難にすること。（JMStV 5 条 3 項 1 号）
2. 提供時間を限定すること。（「青少年の利用禁止」の場合は 23 時～6 時、「16 歳未満利用禁止」の場合は 22 時～6 時　JMStV 5 条 3 項 2 号，4 項）

これらの措置が取られている場合，上記配慮義務を果たしたとされる。

5.2 青少年保護プログラム ― フィルタリング

さらに JMStV 第 11 条で「青少年保護プログラム（Jugendschutzprogramm）の規定を置いている。プロバイダは，青少年メディア保護委員会（後述 KJM）に対して，児童・青少年に有害であると考えられるコンテンツを青少年保護プログラムに登録し（JMStV11 条 1 項），適切性認定のための審査を受けることができる。年齢に応じたフィルタリング機能を有している場合，認定を受けることができる。認定有効期間は 5 年で延長も可能である（JMStV 11 条 2 項）。また，自主規制機関として州メディア委員会の認定を受けた機関は，委員会に代わって，青少年メディア保護州際協定の遵守について審査を行うことができる（JMStV 19 条 2 項）。

テレメディア州際協定に違反した場合，最長 1 年の禁固刑又は罰金（最高 50 万ユーロ）又は秩序違反金を科される（23 条，24 条）。過失も処罰（最長半年の禁固刑又は罰金）される（JMStV 23 条 2 文）。

5.3 青少年保護受託者（Jugendschutzbeauftragte）と自主規制機関登録

「有害情報」からの青少年保護のためのインターネット規制は，表現の自由と青少年保護のバランスをとるため，また，「法的規制」のみでの解決の困難さから，「メディアリタラシー」と「自主規制」を組み合わせる，いわゆる共同規制スキームが説かれるよ

126 いわゆる「闘う民主制」に反する宣伝（刑法 86），憲法違反の団体の標章の使用（刑法 86a 条），殺人、人間性に反する犯罪、傷害、強盗・脅迫，公の平穏を害する犯罪を促すもの（刑法 126 条 1 項），死につつある人又は心身に重い苦痛を受けている人をその尊厳を冒す方法で描写するもの，ポルノグラフィー、暴力ポルノ、児童・青少年の性的虐待、獣姦淫行為他。テレメディアについては、事業者が成人の利用に限定できる場合は、第 4 条 2 項の 1 に挙げる内容（その他のポルノグラフィー）の提供を許可する（第 4 条 2 項）。

うになっている。ドイツでは，州のメディア委員会に自主規制機関を認定させ，有害情報規制の実効性確保を，提供者であるプロバイダの自主規制に委ねている。「規制された自主規制（regulierten Selbstregulierung）[127]」と呼ばれる。

テレメディアのサービスプロバイダは，青少年保護受託者（Jugendschutzbeauftragte）を置かなければならない。ただし，従業員 50 人未満、又は月間アクセス 1,000 万件以下の規模の事業者は、自主規制機関として登録することにより，青少年保護受託者を置かずに済ませることが出来る（JMStV 第 7 条）。これによって，自主規制機関となることを促進していると言われている。

自主規制機関に関しては，同法 19 条が規定する。放送・テレメディアの領域において、自主規制機関を設立することができる。認可された自主規制機関は，この協定の遵守を自ら検証する（JMStV 19 条）。この自主規制機関は KJM により認定される。

5.4 青少年メディア保護委員会 (Kommission für Jugendmedienschutz (KJM))[128]

州メディア局（Landesmedienanstalten）のテレメディア州際条約の規定の遵守（JMStV 14 条 1 項）のために，「青少年メディア保護委員会（以下 KJM と略す。)」を設立する（JMStV 14 条 2 項）。委員会の権限は，テレメディア州際協定の遵守の監督，放送番組の放送時間帯の決定，自主規制機関の認可及び却下，コンテンツのレイティング及びフィルタリング技術の審査及び認定，連邦審議会による有害指定に関するアドバイス、秩序違反金の決定，青少年保護ソフトの認定等である（JMStV 16 条）。各州メディア局の事務局トップであるディレクターから 6 名，青少年保護の権限をもつ州上級行政機関から 4 名，連邦上級行政官庁から 2 名の合計 12 名の委員によって構成され（JMStV 14 条 3 項），連邦と州の調整も期待されている。

事業者は、KJM に対して，サービス内容と青少年保護のために実施している措置について報告する義務を有する。必要とみなされた場合は、無償でその提供サービスへのアクセスを確保しなければならない。また事業者は，監督行為の枠でのサービスへのアクセスや利用を阻害してはならない（JMStV 21 条）。

サービスプロバイダ（及び放送局）が同協定に定める規則に違反した場合，所轄の州メディア庁は KJM を通じて，上述したテレメディア法（Telemediengesetz, TMG）第 7～10 条の規定にもとづくテレメディア・サービス事業者に対する措置を決定する（JMStV 20 条 4 項）。

規則違反の場合の措置には、禁止、プロバイダの差し止め、最高 50 万ユーロまでの罰金があり、KJM が決定した措置の執行は所轄の州メディア庁が行う 。

---

[127] ハンブルグ大学ハンス・ブレドウ研究所（Hans-Bredow-Institut），「現代統治の形態としての規制された自主規制（Regulierte Selbstregulierung als Form des modernen Regierens）」 http://www.hans-bredow-institut.de/webfm_send/53 更に http://www.fsm.de/jugendschutz/anbieter-und-unternehmen/selbstregulierung-und-privilegierung 参照。

[128] http://www.kjm-online.de/

また、インターネットコンテンツの禁止，青少年保護法のリスト作成を担当するのは「連邦青少年有害メディア審査局（以下「BPjM と略す。」）[129]」であり、KJM は BPjM に禁止要請を行うことができる。コンテンツが禁止されているか否かについては、BPjM に問合せることができる。BPjM リストと呼ばれるリストが作成され，公立図書館青から無料で閲覧することができる。青少年保護の観点からネット上には公開していない[130]。

5.5 違反・不服申立

サービスプロバイダが自主規制機関として認定されている場合，または，事業者が認定自主規制の定款に従う場合，違反に対しては，4 条 1 項への違反の場合を除き，所属組織が実施する。KJM による対応は、認定自主規制による決定または決定の不作為が判断余地の法的限界を超えると判断された場合にのみ行われる（JMStV 20 条 5 項）。基本的に事業者・団体の自主的な対応を促し，義務付けている。

当該事業者が認定自主規制組織に所属していない場合，規制に対する不服申立ては KJM に対して行う。事業者が認定自主規制組織のメンバーである場合は、その組織に対し申立てることになる。

5.6 テレメディア州際協定 2010 年改正案[131]

テレメディア州際協定によって確立された自主規制の仕組みを強化するために, 州法務大臣は，2010 年 6 月 10 日，改正された協定を締結した。協定は 2011 年 1 月 1 日に発行するはずだったが，激しい反対運動に合い[132]，2010 年 12 月 16 日，ノルトラインヴェストファーレン州議会の承認拒否により，発効に必要な 16 州全部の承認を得ることができず頓挫した[133]。

法改正は頓挫したが，テレメディア州際協定と，その中心にある KJM は，KJM が審査して州メディア局等上位の組織が対策を実施するという複雑な構造に対する批判は別として，それ自体は高く評価されている。また，青少年保護プログラム（JusProg[134]）とドイツテレコム[135]が 2012 年に作った青少年保護ソフトは，徐々に普及してきているという[136]。

---

129 Bundesprüfstelle für jugendgefährdende Medien (BPjM)
http://www.bundespruefstelle.de/bpjm/Aufgaben/listenfuehrung.html

130 http://www.bundespruefstelle.de/bpjm/Aufgaben/Listenfuehrung/bekanntmachung.html

131 http://www.kjm-online.de/fileadmin/Download_KJM/Recht/JMStV_Stand_14_RStV_Lesefassung-Endversion_1_7_20103.pdf

132 ノルトラインヴェストファーレンの緑の党に関して,
http://www.zeit.de/politik/deutschland/2010-11/gruene-nrw-internet-jugendschutz
更に http://www.taz.de/!53842/,
http://www.henning-tillmann.de/2013/01/kritische-betrachtung-des-entwurfs-zur-novelle-des-jugendmedienschutz-staatsvertrages-20092010/ 参照

133 詳細に関しては，鈴木秀美前掲注(1)参照。

134 https://www.jugendschutzprogramm.de/

135 http://www.telekom.com/startseite

136 批判は，改正案が自主規制を萎縮させるというものであったが，特に問題視されたのが，細かい年齢区

6 まとめ

ドイツの規定は、実定法に詳細に規定を置き、通信事業者にとっては、何をしなければならないか、逆に何をしては行けないかが詳細に規定されているため、法的な判断をする場面が日本より遙かに少ないといえる。

ドイツは、電気通信事業者の問題としてではなく、情報化時代のネットワーク上の何を規制対象とするのかを考えた唯一の国ではないだろうか。「テレサービス」という概念を作り、「テレメディア」という概念に作り直し、変化に対応しようとしている。もちろん、放送がテレメディアに入っていないことへの批判はあり、また、大学も含めた意味での Interactive Service Provider の概念が、日本同様にない。十分とは言えないが、定義から考え直して時代に合わせようとするその姿勢自体は、日本に示唆する点と考えている。

分の下，5 条 2 項に，「コンテンツに，年齢指定に応じた表示をすることができる」という規定が新設されることを予定した点にある。年齢指定表示をすることができるという規定ではあるが，表示をしていない場合，フィルタリングソフトによってブロックされてしまう可能性が有り，事実上の表示義務になるとの批判がなされた。また，五段階に分けられた年齢区分も，サービスプロバイダの自主規制機関としての遵守義務が重くなり，誤表示した場合の責任が生じやすくなるという指摘もなされていた。
http://www.focus.de/kultur/diverses/hoerfunk-fortschritte-im-jugendschutz-auch-ohne-novelle-fuenfter-bericht-der-kjm-zum-jugendschutz-in-rundfunk-und-telemedien_aid_1014723.html 参照

第 4 章　フランス

曽我部真裕（京都大学）

1 「通信の秘密」に関する法的規定

1.1 憲法及びそれに準じる法規範の規定

(1) 憲法の規定

フランスでは有名な 1789 年のフランス人権宣言[137]以来，数え方にもよるが 15 以上の憲法が制定されてきた。これらの中には日本国憲法同様，人権に関する規定と統治機構に関する規定とからなっているものもあるが，後者のみを規定するものもある。人権に関する規定を含む憲法にあっても，通信の秘密を明文で保障するものは見当たらない。ただし，表現の自由を保障するフランス人権宣言（Déclaration des Droits de l'Homme et du Citoyen de 1789）11 条[138]によって黙示的に保障されているとする学説もある。

> 【フランス人権宣言】
> 11 条
> 思想と意見の自由な伝達は，人の最も貴重な権利の 1 つである。ゆえに，すべての市民は，自由に語り，書き，出版することができる。ただし，法律の定める場合には，この

現行憲法は 1958 年に制定された第五共和政憲法であるが，この憲法もまとまった人権条項を欠いている。ただ，人身の自由に関しては規定があり（66 条），憲法裁判所である憲法院の判例により，人身の自由の保障にはプライバシー権の保障も含まれるとされているため，通信の秘密がそこに含まれると考えることも可能である。

また，憲法院の判例[139]により，第五共和政憲法そのものと並び，1789 年人権宣言も同等の憲法レベルの法的効力を持っているとされているため，上記のように同宣言 11 条に通信の秘密の保障が含まれているのだとすれば，通信の秘密の保障は憲法的な保障を受けるということになる。

(2) 条約の規定

フランスでは，日本と同様，条約は法律よりも上位の法的効力を有している。そして，裁判所は，法令の規定が条約の規定に反するか否かを審査し，違反する場合にはその適用を排除する権限を有している。特に，ヨーロッパ人権条約（Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales）については，国内法令の規定がその規定に反しないか否かの審査が積極的に行われており，違憲審査類似の機能を営んでいるた

---

137 1789 年人権宣言そのものは，文字通りほとんどが人権に関する条文に尽きているが，この宣言は，フランス最初の成文憲法である 1791 年の憲法に編入され，その一部となっている。

138 「思想と意見の自由な伝達は，人の最も貴重な権利の 1 つである。ゆえに，すべての市民は，自由に語り，書き，出版することができる。ただし，法律の定める場合には，この自由の濫用に責任を負わねばならない。」

139 Conseil constitutionnel, décision n°94-352 DC du 18 janvier 1995.

めに重要である。

そして，ヨーロッパ人権条約８条１項は，次のような規定であり，通信の秘密を明文で保障している。

【ヨーロッパ人権条約】
８条
すべての者は，その私的及び家族生活，住居及び通信の尊重を受ける権利を有する。
②（略）

1.2 法令の規定

(1) 概観

(a) 刑法典（Code pénal）

ここでは，通信の秘密に関する主な法令の規定を紹介する。

まず，刑法典は，一般的な通信の秘密侵害罪を定める（226-15 条）ほか，事業者に関する通信の秘密侵害罪を定める（432-9 条）。その他関連する規定も含めて訳文を以下に掲げる。

【刑法典】
226-1 条１項
方法のいかんを問わず，次に掲げる行為により故意に他人の私生活の親密性を侵害する行為は，１年以下の拘禁刑又は 4 万 5,000 ユーロ以下の罰金に処する。
一　私的に又は秘密のものとしてなされた発言を，発言者の同意なく傍受し，録音し又は伝達すること。
二（略）

226-3 条
次に掲げる行為は，５年以下の拘禁刑又は 30 万ユーロ以下の罰金に処する。
一　226-15 条２項に定める罪に当たる行為を行うことを可能にする装置若しくは技術的手段，又は距離をおいて会話を検出する目的で考案され，226-1 条に定める罪を犯すことを可能にする装置若しくは技術的手段（中略）の製造，輸入，所持，陳列，提供，貸与又は販売。
二　226-1 条及び 226-15 条２項に定める犯罪を行うことを可能にする装置又は技術的手段のための広告であって，（中略）これらの犯罪の唱道に当たるものを行うこと。

226-15 条 1 項

目的地に到達したか否かにかかわらず，悪意をもって，第三者に向けられた通信を開示し，抹消し若しくは破棄し，遅延させ，若しくは方向をそらせる（détourner）する行為，又は不正にその内容を知る行為は，1 年以下の拘禁刑又は 4 万 5,000 ユーロ以下の罰金に処する。

432-9 条

公権力の受託者又は公役務を担う者が，その職務又は任務の遂行中又は遂行の機会にあって，法律に定められた場合を除き，通信の方向をそらせ，抹消若しくは開封又は通信内容の漏洩を命じ，実施し又はこれを容易ならしめる行為は，3 年以下の拘禁刑又は 4 万 5,000 ユーロ以下の罰金に処する。

公衆向けの電子コミュニケーション・ネットワークの運営者及び電気通信サービスの提供者の従業員が，その職務の遂行中，法律に定められた場合を除き，電気通信によって発せられ，伝達され又は受領された通信を傍受若しくは方向をそらせる行為，またはその内容を利用若しくは開示を命じ，実施し又は容易にする行為は，前項と同様の罪に処する。

(b) 郵便・電子通信法典（Code des postes et des communications eléctroniques）

郵便・電子通信法典は，郵便事業者や電子通信事業者に対して適用される業法であり，通信の秘密に関しても規定がある。電子通信における通信の秘密に関する基本的な規定としては，次のようなものがある。通信の秘密を遵守する義務に違反した場合，上記の刑法典による罰則のほか，監督機関である ARCEP（Autorité de régulation des communications électroniques et des postes）による行政処分がありうる。

【郵便・電子通信法典】

L32 条の 1 Ⅱ

電子通信を管轄する大臣及び ARCEP は，その管轄する権限の行使において，追求する目的との関係で合理的かつ比例的な措置を，客観的かつ透明性のある条件のもとでとるものとし，以下の点に配慮するものとする。

一～四（略）

五　電子通信事業者による通信の秘密，伝達されるメッセージの内容に関する中立性の原則及び個人情報の保護の尊重。

六以下（略）

L32 条の 3

電子通信事業者及びその従業員は，通信の秘密を尊重する義務を負う。

(c) 国内安全法典（Code de la sécurité intérieure）

国内安全法典は，テロ対策を始めとする治安維持に関する様々な規定を法典化したものであり，通信傍受に関する規定も含んでおり，その中で通信の秘密の保護の原則が宣言された上で，通信傍受は同法典の定める手続によってのみ行いうるとされている。

【国内安全法典】
L241-1 条
電子通信によって発せられる通信の秘密は，本法によって保障される。
通信の秘密に対する制約は，本法律の定める公益上の必要のある場合に限り，本法律の定める限度において，公権力によってのみ行いうる。

(2) 通信の秘密に関する情報の区分

(a) データの種類

電気通信事業者が取り扱う個人に関するデータの種別としては，トラフィックデータ（données relatives au traffic，donnés de connexion）と通信内容，および加入者に関するデータについても区別される（郵便・電子通信法典 L34 条の 1）。

他方，これらとは異なる観点からの分類として，「コンテンツの制作に寄与した者を識別するためのデータ」（以下，「発信者情報」という。）についての規律も存在する。

以下では，トラフィックデータと発信者情報の保存義務について概観する。通信内容については，原則として保存義務はないが，例外的に保存要請が認められる（3.1.1 参照）。

(b) トラフィックデータ

トラフィックデータは「電子通信ネットワークによる通信の伝達またはその課金のために取り扱われるあらゆる情報」と定義されている（郵便・電子通信法典 L32 条 18 号）。

トラフィックデータの取り扱いの原則は，消去または匿名化である（同法典 L34 条の 1 Ⅱ）。しかし，広範な例外が定められており，犯罪捜査等の必要性から，所定のトラフィックデータについて，その消去・匿名化を最長 1 年間延期することができる。「延期することができる」という文言からは，データの保存は任意であるかのようにも思われるが，概説書によっても現地調査によっても，実際には義務であると理解されているようである[140]。保存する義務の対象となるデータの具体的な内容はデクレ（政令）に委ねられているが，法律レベルでは，これらのデータは信書の内容に及んではならない旨確認されている（同

[140] なお，この規定は 2006 年のいわゆる EU データ保存指令（2006/24/CE）を国内法化したものであるが，2014 年 4 月 8 日，ヨーロッパ司法裁判所は同指令の規定が私生活の尊重に対する権利の過度の侵害であるとして無効とした（CJUE, le 8 avril 2014, C-293/12 et C-594/12）。この判決に対するフランス政府の対応について，ある下院議員から司法大臣に対して質問がなされているが（Question N° 54368 au Ministère de la Justice），本稿執筆段階ではまだ回答がなされていない。

法典 L34 条の 1 Ⅵ)。デクレでは以下のように定められている（同法典 R10 条の 13 Ⅰ）。

a) 利用者の識別を可能にする情報。

b) 通信に用いられた端末に関するデータ。

c) 個別の通信の日時・通信時間等の技術的な明細。

d) 要求され又は用いられた補完的なサービスに関するデータ及びその提供者。

e) 通信の相手方の識別を可能にするデータ

さらに，電話に関して事業者は上記のデータのほか，通信の発信者と位置を識別するデータも保存するものとされる（同条Ⅱ）。

また，法律では上述の通り「最長 1 年間」と定められているが，デクレでは記録の日から 1 年間保存するものとされている（同条Ⅲ）。

このようにして保存されたデータへのアクセスについては，後述する。

なお, トラフィックデータの取り扱いについては個人情報保護法（1978 年 1 月 6 日法〔Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés〕）に従わなければならないとされ（郵便・電子通信法典 L34 条の 1 Ⅳ 3 項），個人情報保護の枠内の問題であることが示されている。

(c) 「コンテンツの制作に寄与した者を識別するためのデータ」（発信者情報）

他方，公衆向けオンラインコミュニケーションにおいては，「コンテンツの制作に寄与した者を識別するためのデータ」という概念もあり，後述の通り，接続プロバイダやホスティングプロバイダ等は，これらのデータを取得・保存し，必要に応じて公権力に提供する義務を負う（2004 年 6 月 21 日法（デジタル経済信頼法〔Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique〕） 6 条Ⅱ）。

この発信者情報の取得・保存義務は，本来は公衆向けオンラインコミュニケーション（概ね，日本でいう「公然性を有する通信」に対応すると思われる）に関する義務であるが，主たるまたは従たる業としてインターネットへのアクセスを提供する者にも準用されているため（同法典 34 条の 1 Ⅱ），その限りでは狭義の通信についても適用される。

発信者情報の具体的な内容はデクレ（2011 年 2 月 25 日デクレ〔Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne〕）に規定があるが，そこでは接続プロバイダとホスティングプロバイダ等とで区別されている。具体的には下記のとおりである。

接続プロバイダ	**a）接続の識別子** **b）接続プロバイダが契約者に割り当てた識別子** **c）接続に用いられた端末の識別子** **d）接続の日並びにその開始及び終了時刻** **e）契約者の回線の種別**
ホスティングプロバイダ等	a）発信元の接続の識別子 b）情報システムが処理対象のコンテンツに割り当てた識別子 c）サービスへの接続及びコンテンツの伝送に用いられたプロトコルの形式 d）処理の種別 e）接続の日並びにその開始及び終了時刻
両者共通	契約またはアカウント開設時に提供された下記の情報も保存義務がある（同デクレ1条1項3号）。 a）アカウント開設の際の接続の識別子 b）氏名または名称 c）住所 d）ハンドルネーム e）電子メールアドレスまたは関連するアカウント f）電話番号 g）最新のパスワードを確認またはそれを変更するためのデータ サービスが有料である場合には，下記の情報も保存義務がある（同デクレ1条1項4号）。 a）用いられた支払い方法 b）支払いの照会番号 c）金額 d）取引の日時

以上から分かるように，発信者情報は，トラフィックデータと契約者情報にまたがる内容となっている。

データの保存期間は１年間である（同デクレ３条）。このようにして保存されたデータへのアクセスについては，後述する。

データの提供先は司法機関であり，その要求に応じて提供が行われる（デジタル経済信頼法６条Ⅱ３項）。犯罪捜査の場合に限らず，民事訴訟について，日本でプロバイダ責任制限法による発信者情報開示の問題となるような場面においても（フランスには発信者情報開示について個別に定める法律はない），この規定に基づいて発信者情報が開示される。具

体的には，仮処分（レフェレ）等で発信者情報開示を裁判所に申し立て，裁判所がこの規定に基づいてデータ提供を求めることになる。

2 ISP の「通信の秘密」への関与に関する法的規定

2.1 迷惑メールフィルタリング

デフォルトオンでの迷惑メールフィルタリングサービスは，フランスでも実施されている。例えば，プロバイダ最大手のフランステレコム（オレンジ）の電子メールサービス約款[141]を見ると，デフォルトオンでの迷惑メールフィルタリングを実施され，この機能は解除できないこと，また，受信するすべてのメールが機械的に分析されるのをユーザーが承諾する旨の文言が規定されている。

こうしたサービスについて法的には，刑法典 226-15 条及び 432-9 条 2 項の通信の秘密侵害罪との関係が問題となる。

通信の秘密の保障範囲（通信内容のみか，接続データも含むか）については不明確であり，刑法の概説書等にもこの点に触れるものは見当たらず，また，この点に関する議論はフランスでは特に行われていない。通信内容を中心に考えられていることは間違いないが，接続データが排除されていると明言する文献，判例は見当たらないようである。

ただ，少なくとも実務上は，後者は通信の秘密の問題としては意識されていないようであり，接続データの利用が通信の秘密侵害の問題として議論されることはなく，個人情報保護，あるいは帯域制御のような場合には，インターネットの中立性の問題として議論されている。

また，刑法典 226-15 条の通信の秘密侵害罪が成立するためには，主観的な要件として，単なる故意のみならず悪意が要求されている。したがって，悪意がなければ，日本でいうところの構成要件該当性もないということになる。現

地調査においては，例えばウェブメールの内容をスキャンした上でのターゲティング広告表示は，約款での説明やオプトアウトを認めることなどにより，悪意を欠き通信の秘密侵害罪に該当しないと理解されているとの説明を受けた 。

他方，刑法典 432-9 条 2 項には悪意の要件はなく，このような議論は成立しないが，どのように正当化されるのか，十分な整理がなされていないようである。前述のように，オレンジの約款では同意について記載があり，同意による正当化が図られているようにも思われるが，今回の調査では詳細に立ち入ることができなかった。

2.2 帯域制御

帯域制御は，通信の秘密の問題ではなく，インターネットの中立性の問題と捉えられている。これは，前述のように，少なくとも刑法典 226-15 条との関係では，正当な目的で行われる帯域制御は，通信の秘密侵害罪の要件である悪意が欠けるという前提に立っている

[141] Conditions Générales d'Utilisation de la Messagerie électronique

ものと思われる。

他方，ネットワークの中立性については，郵便・電子通信法典により法律上の原則とされ，監督機関（ARCEP）がその遵守を監督するものとされる（同法典 L36-6 条）。そして，インターネットでの帯域制御に関する ARCEP の見解（2010 年）[142]によれば，ネットワークの混雑対策や安全対策のために帯域制御を行うことは以下の条件のもと認められる。

・対策目的との適合性
・有効性
・必要最小限性
・透明性
・差別の禁止

2.3 DDoS 攻撃等情報セキュリティに関する攻撃に対するトラフイック遮断

これについては，帯域制御と同様の取り扱いであるようである。

2.4 違法コンテンツに対するアクセスブロッキング

(1) 裁判所の判決に基づく個別サイトのブロッキング

明文の根拠のあるものとして，無許可オンラインギャンブルサイトのブロッキング。無許可サイトのアクセス停止を裁判所が命じた場合，プロバイダは DNS ブロッキングを実施する義務がある（2011 年 12 月 30 日デクレ（Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de l'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée） 1 条）。その他，知的財産権の保護，消費者保護目的でのブロッキングについて法規定がある（知的財産法典（Code de la propriété intellectuelle）L336-2 条，消費法典（Code de la consommation）L141-1 条Ⅷ 3 号）。

ただし，こうした明文の根拠がなくても，違法有害サイトについて個別に判決によってブロッキングを命じることは可能である。

(2) 裁判所の判断を介さないブロッキング

児童ポルノのブロッキングに関しては，2011 年 3 月 14 日法（国内安全大綱法〔loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure（LOPPSI 2）〕）により義務付けがなされた[143]。

この規定について，憲法院は合憲としたが[144]，裁判官の判断を介さない点などで批判も強く，施行令が制定されないまま店晒しになっており実施されていない。ほかにブロッキングを認める法令はなく，結局，フランスでは裁判所の判断を介さないブロッキングは実

[142] ARCEP, Neutralité de l'internet et des réseaux Propositions et recommandations, septembre 2010(http://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010.pdf).
[143] 同法 4 条により，デジタル経済信頼法 6 条Ⅰ7 項にブロッキングに関する規定が追加された。
[144] Conseil constitutionnel, décision n°2011-625 DC du 10 mars 2011.

施されていない。

以上の通り，フランスでは概して，裁判所の判断に基づくブロッキングについては許容されているが，逆に，裁判所が介在しないブロッキングについては強い抵抗が示される傾向にある。

2.5 行動ターゲティング広告

行動ターゲティング広告については，主として個人情報保護法（1978 年 1 月 6 日法律）との関係が問題となる。

IP アドレスについていえば，プライバシーコミッショナーである CNIL（Commission nationale de l'informatique et des libertés）は，その個人識別性を認めている[145]。また，2013 年に出されたクッキー及びその他の追跡子に関する CNIL の勧告[146]によると，法律で求められている同意の実質化のため，利用者は，サイトにアクセスした際にすぐに気づくようなバナーでクッキーの存在を知らされなければならない。また，そのバナーには，①クッキーの目的，②クッキーを拒否できること，そして，バナーに表示されているリンク先をクリックすることで設定を変えることができること，③ネット閲覧を続けることが同意とみなされること，を示す必要があるとしている。

また，同意の有効期限は 13 ヶ月であり，その後は新たな同意取得が必要であるとされる。その他，ブラウザ上で Do Not Track の設定にした場合には，事業者はそれに従ってユーザーや端末のプロフィール作成が禁止される旨も定める。

3 公権力の「通信の秘密」への関与に関する法的規定

3.1 法執行機関等のアクセスの仕組み

(1) 犯罪捜査のためのアクセス

本章では，必ずしも網羅的ではないが，データへのアクセスが認められる場合について述べる。通信事業者等が保存しているデータ（通信傍受については３．２で述べる。）に対して，犯罪捜査のために捜査機関がアクセスする場合については，アクセスの局面ではデータの種別にかかわらず同じ取り扱いがなされている。

ただし，保存に関する規律が異なるため，この点で捜査機関にとってのアクセスの難易が生じることになる。すなわち，前述のように，トラフィックデータは恒常的に保存されているためにアクセスしやすいのに対し，内容については恒常的には保存されていない。そこで，一定の場合に捜査機関が保存要請を行うことが認められており，それにアクセスすることになる。

---

145 Délibération n° 2006-294 du 21 décembre 2006 autorisant la mise en oeuvre par l'association de lutte contre la piraterie audiovisuelle d'un traitement de données à caratère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles.

146 Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.

犯罪捜査のためのデータへのアクセスの手続であるが，検察官または検察官の許可を受けた警察官は，捜査に関係する書類（情報システム内にあるものや個人情報を含む。）を保有していると思われる公私の団体や行政組織に対して，特にデジタルデータの形式で提出を求めることができる（刑事訴訟法典 77-1-1 条）。この要求を正当な理由がなく拒否した場合，3,750 ユーロの罰金に処される（同法典 77-1-1 条・60-1 条２項）。換言すれば，捜査機関にはデータの提出を直接強制することはできず，事業者側の正当な理由のない拒否に罰金を科すことで実効性を確保している。また，更に言い換えれば，この提出手続には事前の統制（令状等）がない代わりに，罰金を科す刑事手続において事後的な統制が図られているということが言える。

次に，前述の通信内容の保全要請については，勾留担当裁判官（juge des libertés et de la détention） の許可を受けた警察官は，通信事業者に対し，当該事業者のサービスの利用者が閲覧した情報内容を，1 年を超えない間保全（préservation）する措置を遅滞なくとることを要請することができるとされている（同法典 77-1-2 条１項・60-2 条１項）。ただし，現行犯に関しては勾留担当裁判官の許可は不要である（同法典 60-2 条１項）。上述のように，こうして保全された情報内容への捜査機関のアクセスについてはトラフィック・データと同様である。

以上のように，検察官や勾留担当裁判官の許可という形で手続的統制がなされている。なお，日仏の刑事訴訟の構造が異なることもあり，検察官の位置づけも日本とフランスで若干異なっている。フランスの検察官は刑事訴訟の一方当事者というよりは，司法官として裁判官と並ぶ存在で，ある程度中立的な位置づけとなっている。

(2) 行政機関によるアクセス

(a) 原則的な手続

行政機関によるアクセスについては，２つの手続が区別される 。

原則的な手続は，首相（例外的に防衛大臣又は内務大臣）に，電子通信ネットワークを運営する者又は電子通信サービスの提供者に対して，必要な情報の提供を求めることができるとするものである（国内安全法典 L244-2 条）。

この手続は，条文の文言だけからは判然としないが，次に述べる通信内容の傍受の準備段階に位置づけられているものである 。すなわち，トラフィック・データの収集のみで目的が達成できるのであれば内容を傍受するまでもないことから，通信傍受の前段階としてこうした権限が認められている。したがって，情報提供を求めることのできる目的も，通信傍受の場合と同様，国家の安全，フランスの科学及び経済的な潜在力の重要な要素の保護またはテロ，組織犯罪若しくは解散命令を受けた団体の再建等の防止のための情報収集といったものが求められる。

この手続によるアクセスの統制は，独立行政機関である国家治安傍受統制委員会（Commission nationale de contrôle des interceptions de sécurité）により行われる。同

委員会は，コンセイユ・デタ副委員長および破毀院院長が共同で作成する候補者名簿から大統領が任命する委員長と，下院議員及び上院議員各１名の合計３名からなる独立行政委員会である（同法典 L243-1 条，L243-2 条）[147]。

(b) 例外：テロの予防のための情報提供

テロ対策に関する 2006 年１月 23 日法（Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers）によって郵便・電信電話法典 L34 条の１の１が新設された。それによれば，テロの予防（したがって既になされた犯罪の捜査とは区別される。）のため，警察及び憲兵隊のテロ対策専門部署の職員であって，適格を有するとして個別に指定された者は，事業者が保存及び処理したデータの提供を請求することができる（同条１項）。

請求対象となるデータは，電子通信サービスの契約者番号又は接続番号の識別，指定された者の契約又は接続番号全体のリスト，利用された端末の位置情報，通話履歴（相手の番号，通話日時，通話時間）であり（同条２項），提供にかかる費用については国が負担する（同条３項）。

請求には理由の付記を要し，内務省に置かれた専門官の決定が必要である。この専門官は，内務大臣が提案した３名の候補者から，国家治安傍受統制委員会が選任（任期３年）する（同条４項）。また，同委員会は適法性を監視し（提供されたデータにアクセスして調査可能），違反の場合には内務大臣に勧告することによって濫用の防止が図られている（同条５項）。

3.2 通信傍受

(1) 通信傍受の種類

通信傍受には，犯罪捜査の一環として行われる司法傍受と治安等を目的とする行政傍受とがある。司法傍受は，1991 年法制定までは真実発見に有用な一切の処分を予審判事に認める刑訴法の一般規定に基づく司法傍受がなされ，批判もあったが，判例は適法性を承認していた。

他方，行政傍受は，1950 年代のアルジェリア戦争等を背景に，法令の明文の根拠なく秘密裏に幅広く実施されていたが，1970 年代になって発覚し，議論になった。

こうした中，ヨーロッパ人権裁判所がフランスによる司法傍受を人権条約８条違反と判断したため[148]，1991 年７月 10 日法（電子コミュニケーションによる通信の秘密に関する 1991 年７月 10 日法律第 91-646 号〔Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques〕）が成立，電気通

147 現在の構成は，委員長である破毀院の名誉部長のエルベ・ペルチエ（Hervé Pelltier），ジャン＝ジャック・イスト（Jean-Jacques Hyest）上院議員，ジャン＝ジャック・ユルボア（Jean-Jacques Urvoas）下院議員である。

148 1990 年 4 月 24 日判決（クルスラン判決〔CEDH, le 24 avril 1990, Kruslin c. France, n°11801/85〕）

信における通信の秘密の原則を定めるとともに，一定の条件・手続のもとで司法・行政傍受を承認している。以下では，両者についてその概要を述べる。

⑵ 司法傍受

司法傍受には，上記 1991 年法で規律される通常の司法傍受と，2011 年に新たに設けられた組織犯罪に関する司法傍受とがある。まず前者について，1991 年法の司法傍受に関する改正内容は，刑事訴訟法典 100 条以下に当たる。

それによれば，法定刑が懲役２年以上の重罪および軽罪について，捜査の必要性がある場合には，予審判事が書面による決定により，電気通信による通信の傍受，録音および書き起こしを命じることができる（同法典 100 条）。傍受等の期間は４ヶ月であり，同一条件で更新可能である（同法典 100 条の２）。

対象となる犯罪の範囲が比較的広い点，傍受を認める要件が緩やかである（傍受以外の手段では捜査が困難であることが要求されていない）こと，事後通知など，傍受の対象者の権利保障への配慮がないことなどの批判がある。

次に，組織犯罪に関する司法傍受は，所定の組織犯罪に関する現行犯捜査又（enquête de flagrance）は予備捜査（enquête préliminaire）の際に必要と認められる場合，検察官の請求により，勾留担当裁判官が傍受等を許可することができる（同法典 706 条の 95）。この場合の傍受期間は最長１ヶ月間であり，１度のみ更新可能である 。

事業者の協力については，予審判事又はその委任を受けた警察官は，傍受装置の設置のために事業者の従業員を徴用することができるとされる（同法典 100 条の３）。また，通信が暗号化されている場合には，暗号を提供する自然人又は法人は，傍受の命令権者の求めにより，協力義務を負う（国内安全法典 L244-1 条）。

⑶ 行政傍受

1991 年法の行政傍受に関する改正内容は，国内安全法典 L241-1 条以下に該当する。

それによれば，国家の安全，フランスの科学及び経済的な潜在力の重要な要素の保護またはテロ，組織犯罪若しくは解散命令を受けた団体の再建等の防止のための情報収集を目的とした電子通信の傍受が例外的に認められる（同法典 L241-2 条）。

行政傍受の許可は，国防大臣，内務大臣若しくは税関を管轄する大臣又はこれらの大臣から特に委任を受けた２名のうちの１名の理由を示した書面による提案に基づき，首相又は首相から特に委任を受けた２名のうちの１名によって理由を示した書面によって与えられる（同法典 L242-2 条）。

傍受の期間は最長４ヶ月であり，同一条件で更新可能である（同法典 L242-3 条）。

行政傍受の濫用の統制については，まず，同時に実施可能な件数の上限を首相が定めることとされている（同法典 L242-2 条）ほか，前述の国家治安傍受統制委員会が統制を行う。すなわち，首相の傍受決定の適法性に疑義がある場合，および傍受開始後に自ら又は関係

人の申立によりそれが違法であると判断した場合に，それぞれ傍受の中止を首相に勧告することである（同法典 L243-8 条，L343-9 条）。

事業者の施設内における行政傍受の実施は，コミュニケーション担当大臣等の命令に基づき，この事業者の従業員によって行われる（同法典 L242-9 条）。

3.3 2013 年 12 月 18 日法による改正

上記の行政機関によるアクセスに関する２つの制度は，実質上，2013 年 12 月 18 日法（Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale）によって改正を受けた。

同法は未施行（2015 年１月１日施行）なので，ごく簡単にのみ述べると，まず，国内安全法典の行政による通信傍受について定める編の中の１章として「接続データに対する行政のアクセス」と題する章が新たに設けられ，所要の規定がおかれている。

国内治安，防衛，経済及び予算を担当する大臣部局の職員のうち，個別に指定され適法に授権された者は，行政傍受を正当化する目的（国家の安全，フランスの科学及び経済的な潜在力の重要な要素の保護またはテロ，組織犯罪若しくは解散命令を受けた団体の再建等の防止のための情報収集〔国内安全法典 L241-2 条〕）のため，電子通信事業者，ISP やホスティング事業者に対し，電子通信サービスの契約や接続に関する番号の識別，特定人の契約・接続番号，端末の位置情報，電場番号リストにある契約者の通信，通信時間，日付等の情報を含む，ネットワーク又は電子通信サービスにおいて取り扱われ又は保存された情報（informations）や文書（documents）の提供を求めることができる（同法典 L246-1 条，L246-2 条Ⅰ）。上記の職員の要求には，国家治安傍受統制委員会によって任命され，首相のもとに置かれる専門官の許可が必要である（L246-2 条Ⅰ）。

以上の制度は，実質的には，上述のテロ予防のための情報提供の仕組みをテロ予防目的以外のものに拡大したものであり，手続についてもそれとやや類似している。また，この仕組みの導入に伴い，上述のテロ予防のための情報提供の規定（郵便・電信電話法典 L34 条の１の１）は廃止される。

これに対して，2013 年 12 月 18 日法には，行政機関の権限を更に拡大し，リアルタイムでのアクセスを認める規定も含まれている。すなわち，国内治安，防衛，経済及び予算を担当する大臣又はその特に指定する者の書面による理由を付した要求と，首相又は首相により特に指定された者の決定により，30 日以内の間，L246-1 条所定の情報を事業者からリアルタイムに収集することが認められた（国内安全法典 L246-3）。

2013 年 12 月 18 日法の定める以上の２つの制度には，収集される情報の範囲の曖昧さ（接続データにとどまらず内容も含まれるおそれがあるのではないか）やリアルタイム収集を認めるのは行政権限の過度の拡大ではないかなどの批判がなされている。

第5章　オーストラリア

吉田一雄（清和大学）

1 「通信の秘密」に関する法的規定

1.1 憲法上の規定

オーストラリア連邦憲法（An Act to constitute the Commonwealth of Australia [9th July 1900](63 & 64 Victoria - Chapter 12)）はいわゆる連邦の統治機構だけを定めた憲法であり、人権規定を含んでいない。

しかし、オーストラリアは、国際人権規約（B規約）（International Covenant on Civil and Political Rights）を1976年3月23日から施行しており、同第17条第1項によれば、「何人も、その私生活(privacy)、家族、住居若しくは通信(correspondence)に対して恣意的に若しくは不当に干渉され又は名誉及び信用を不法に攻撃されない」とあるところに、プライバシー保護の根拠があるとされている。(注：ここでcorrespondenceに「通信」の語を当てたが、古典的な意味における「信書」の意味以上に情報通信一般に適用範囲があると考えるのは危険であり、ここではプライバシー保護の根拠にとどめるのが妥当である。)

1.2 1988年連邦プライバシー法(Privacy Act 1988)

(1) プライバシー法の所管

1988年連邦プライバシー法により、上位機関として、情報委員会(Information Commissioner)（1988年法による)、また下位機関としてオーストラリア情報委員会(The Australian Information Commissioner)および苦情処理機関であるオーストラリア情報委員会局(The Office of Australian Information Commissioner)（オーストラリア情報委員会法2010年(The Australian Information Commissioner Act 2010による)、同じく下位機関として、情報公開担当である自由情報委員会(Freedom of Information Commissioner)（自由情報修正（改正）法2010年(Freedom of Information Amendment (Reform) Act 2010）がそれぞれ設置されており、不服申し立てにより、情報委員会は、プライバシー保護のために必要な、または便宜なあらゆることを行う権限がある（2010年法第10条第2項)。

(2) プライバシー法のルール変遷

当初プライバシー法は公的部門のみを対象として、情報プライバシー原則(Information Privacy Principles（IPPS）（連邦プライバシー法第14条Schedule1）)が規定されたが、2001年12月1日から、国家プライバシー原則(National Privacy Principles（NPPS）)として、民間部門に適用が拡大された。その後、統合プライバシー原則案（Proposed Uniform Privacy Principles（UPPS）（オーストラリア法改革委員会(Australian Law Reform Commission (ALRC) Discussion Paper 72: Review of Australian Privacy Law)）が提案さ

れていたが、現在は、それをさらに修正して、2014 年 3 月 12 日施行のオーストラリア連邦プライバシー原則(Australian Privacy Principles (APPS) (2012 年プライバシー保護を拡張するプライバシー修正法(Privacy Amendment Enhancing Privacy Protection) Act 2012, Schedule 1))が現行法である。

オーストラリア連邦プライバシー原則適用主体(APP entity、以下「APP 主体」)はこの APPS を遵守しなければならない。ただし、刑事罰はないものの APPS への違反は個人のプライバシー侵害とされ(第 13 条)、侵害が深刻または繰り返される場合には、2000 ユニット(現在 1 ユニット＝170 オーストラリアドル)の民事罰(civil penalty)が課される(第 13G 条)。

APPS の 13 原則と特徴は以下の通り。

原則 1 公開性と透明性(open and transparent management of personal information)APPS を遵守した、運用の公開性と透明性を要求。

原則 2　匿名性(anonymity and pseudonymity)

原則として、個人は個人情報を提供する際に個人を特定されないか、匿名を用いる選択権を有する。

原則 3　求められた(solicited) 個人情報の取得

我が国のいわゆる「直接取得」に対応する個人情報収集の手続きについて規定。

原則 4　求められていない(unsolicited)個人情報の取り扱い

我が国のいわゆる「直接取得以外」の個人情報収集の手続きについて規定。

原則 5　個人情報取得の通知

第 5.1 条　APP 主体が、個人情報を取得すると同時または前、または、実務的でない場合には事後実務的となるや直ちに、同適用主体は、状況に照らして以下の合理的な手段を（手段がある場合には）取らなければならない。すなわち、

a. 第 5.2 条に言及されている事項（注：通知項目）につき、状況に照らして合理的であれば、個人に通知すること、または、

b. そうでなければ、その個人がその状況について知っていることを確認すること。

原則 6　利用と開示

個人の明示または黙示の同意で、構わないが、容易な退会方法が準備されていることを要する。

原則 7　ダイレクトマーケッティング

第 7.1 条でダイレクトマーケッティングのための情報の利用と開示を禁止する。

例外として第 7.2 条で、a.個人から取得、b.個人が合理的に利用または開示を予見でき、c.ダイレクトマーケティングの中止につき簡易な手段が用意されており（オプトアウトでよい)、d.中止の申し込みがない場合、にはダイレクトマーケッティングは許される。

但し更に例外の例外として利用と開示が禁止されるものに、機微情報（第 7.4 条）と請負サービス提供者(Contracted Service Providers（注：medicade などに関わる事業者）)(第 7.5 条)）とがある。

原則 8　個人情報の域外開示
オーストラリアの域外に情報を開示する場合、情報の受け手が APP の要件を満たしていることを確認することを要求。
原則 9　政府関連識別子の借用、利用または開示
原則禁止、ただし例外として認められる場合を規定。
原則 10　個人情報の正確性
取り扱われる個人情報については、正確、最新かつ完全なものであることを要求。
原則 11　個人情報のセキュリティ
第 11.1 条　APP 主体は、
(a) 濫用、干渉、および喪失、 および
(b) 不当なアクセス、改変、または開示の場合には、
情報保護のために状況に照らして合理的な手段をとらなければならない。
第 11.2 条
(a) APP 主体が、個人情報を保持し、かつ、
(b) 同主体が本附則に基づき利用または開示することが許される目的の情報は必要でなく、かつ、
(c) その情報が連邦記録(Commonwealth record)に含まれておらず、かつ、
(d) 同主体が、オーストラリア法、または裁判所命令によりまたは基づきその情報を保持することが求められていない場合には、
同主体は、その情報を廃棄するか、または、その情報を個人識別不能にするために、状況に照らして合理的な手段を取らなければならない。
原則 12　個人情報へのアクセス
原則として、個人は自己の情報にアクセスする権利があるが、APP 主体が組織である場合には、公共の安全や、他者のプライバシーへの影響や、取るに足らない要求や、法執行機関との関係等で要求を拒絶できる場合を規定。
原則 13　個人情報の修正
APP 主体は保持する個人情報について、自発的または個人の要求により、正確、最新、完全、適切かつ誤解を生じないように個人情報を修正しなければならないが、それをめぐる手続きを規定。

(3) プライバシーの定義に関する参考事項

オーストラリア法改革委員会（The Australian Law Reform Commission）による提案(Privacy　REPORT 108　For Your Information:　Australian Privacy Law and Practice (ALRC 2008 年 5 月 30 日))がプライバシーの定義に関して参考になる。以下の通り。

1.29 プライバシーは、別々ながら関連したいくつかの概念に分けられると提案する。すなわち、情報プライバシー(Information privacy) : 信用情報や医療および政府記録のような個

人データの収集と取り扱いに関するルールの確立を含む。これはまた「情報保護(data protection）」として知られる。

身体的プライバシー(Bodily privacy)：遺伝子検査、薬物検査および口腔検査などの侵襲的な手段に対しする肉体自身の保護に関する。

コミュニケーションのプライバシー(Privacy of communications)：手紙、電話、e-mailおよびその他の形のコミュニケーションの安全とプライバシーを包含する。

地域的プライバシー(Territorial privacy)：家庭と、仕事場または公共空間のようなその他の環境への侵入に制限を設けることに関するもの。これには、捜索、ビデオ監視およびID チェックが含まれる。

1.3 刑法典(Criminal Code Act 1995)の規定

刑法典第 10.6 章に通信サービスに関する犯罪が規定されているが、「通信の秘密」を保護法益と想定していると解されるものとしては、第 474.4 条があり、傍受装置の製造、広告、販売、所持を犯罪行為として、法定刑 5 年の拘禁刑が科されている。

2 ISP の「通信の秘密」への関与に関する法的規定

2.1 1997 年電気通信法（Telecommunication Act1997）による規制

「通信の秘密」の保護と逆行する規定と解されるが、1997 年電気通信法は、第 14 条において、通信事業者は、電気通信ネットワークおよび施設が犯罪の遂行に用いられることを妨げ、刑事捜査の強行（罰金刑の執行、および公的歳入の保護の場合も同様）に合理的に必要である援助を連邦と州の官吏及び当局に対して行う義務を負うと規定する。

その上で「通信の秘密」に関して、キャリア、通信サービスプロバイダ(以上第 276 条)、ナンバー・データベース運用者(第 277 条)、緊急通報担当者(第 278 条)、およびそれぞれの従業者に、(a)通信内容(contents of communications)、(b)通信サービス(carriage services)、および(c)他者の事項または人的特徴に関して情報の秘密性を保護しなければならないと規定しており、それぞれ第３項で違反の場合には、２年以下の拘禁を罰則として規定する。この「通信の秘密」への言及は、上記(a)(b)(c)が併記されており、「通信内容」と「通信データないしトラフィックデータ」という区別は特に行われておらず、遵守義務の程度や開示手続きに違いはないと解される。

1997 年電気通信法では、免許制である通信事業者に対するオーストラリア通信およびメディア当局(Australian Communications and Media Authority (ACMA)) の監督に関して、あらかじめ登録されているそれぞれのサービスプロバイダー規定の違反の場合に、第 102 条で、書面による救済的な指示(remedial direction)、または第 103 条で正式な警告(Formal warnings)という 2 段階の監督権を行使すると規定されている。

2.2 1979 年電気通信(傍受およびアクセス)法 (Telecommunication (Interception and

Access) Act 1979)(2013 年改正)による規制

第 7 条第 1 項　何人も電気通信システムを通過する通信を、

(a)傍受し、

(b)傍受することを他の者に許可し、または

(c)他の者が傍受することを可能ならしめる行為を、してはならない。

第 2 項　第 1 項は次の場合には適用されない。

(a)キャリアの被用者がその義務の過程でなす行為で、キャリアの被用者が効果的にその義務を果たすことが合理的に必要である場合、

(i)電気通信サービスに関して利用され､または利用されることが意図されている通信回線架設、または設備、または

(ii)電気通信システムの運用または維持、または

(iii)刑法典第 10.6 編の条項（注：通信サービス関連犯罪）に違反し、または違反の恐れがあるか違反しそうな者を特定または追跡、または、

(aa)設備または回線の架設、接続または維持に関して、適法に義務に関わるものによる傍受で、そのような義務を効果的に行うために通信を傍受することが合理的に必要である場合、または

(aaa)通信の傍受が、

(i)ネットワークに関してそのネットワークの保護義務に関わる責任ある者から書面で権限を与えられており、かつ

(ii)そのような義務を効果的に行うために通信を傍受することが合理的に必要である場合、または

(ab)令状に基づく通信の傍受に用いられる架線､接続または設備の維持に適法に義務を負う者による通信の傍受、または

(ac)(i)特定の場所に使用されている盗聴装置の有無を発見し、または

(ii)盗聴装置の位置を決定する目的で、適法な義務の履行の際に、当局の管理によってなされる行為から生じる通信傍受、または

(b)令状に基づく通信傍受、または

(c)第 31 条第 1 項または第 2 項（注：逆探知の緊急要請）に基づきなされる要請に従った通信傍受、または

(d)第 31 条(注:公安当局の被用者に対する法務長官の許可)に基づき正当化される通信傍受。

(第 3 項以下略)

従って、この第 2 項に依拠すると、通信事業者は、そのシステムの円滑な運用を確保する義務を果たすため合理的であると考えられれば、通信の傍受が広く許されているように解される。

一方、令状に従い適法に傍受された通信に関して、第三者への伝達、使用、または記録することに関しては、同法第 63 条で、禁止されている。

上記第 7 条第 1 項、または第 63 条違反に関しては、第 105 条において 2 年以下の拘禁刑が規定され、令状捜査の妨害または不協力の場合には、6 か月以下の拘禁刑が規定されている(第 106、107 条)。

2.3 オーストラリア通信委員会(Australian Communications Authority (ACA)) によるスパムメール禁止規制

2003 年スパム法(Spam Act 2003)は、スパムメールを規制しているが、その主な内容は以下の通り。

・受信者の同意なしに商業目的で電子メールを送信することを禁止（第 16 条)。
・違反者には罰金刑を命ずることができる（第 24-29 条)。
・違反者にはビジネスの差し止めを命ずることができる（第 32-36 条)。
・商用メールには送信者のコンタクト情報を必ず明記する（第 17 条)。
・容易に退会できる手段を講ずること（第 18 条)。
・スパム送信先リストを作成するメールアドレス自動抽出ソフトなどの利用禁止（第 20-22 条)。
・国際協力体制の必要（第 45 条)。

従って、少なくともスパムメールの受信者はともかく、発信者に関しては、「通信の秘密」の保護の対象外であり、発信者情報を追跡すること等は違法ではないと解される。実際には、そのようなスパムメールを排除することをプロバイダーがサービス提供規約(Terms of Service)において、スパムメールの受信者に予め明示してスパムメールを排除することが実務上多いと思われる。

3 公権力の「通信の秘密」への関与に関する法的規定

3.1 令状を要する場合

(1) 公権力による通信傍受に関して、1979 年電気通信(傍受およびアクセス)法は令状を要する場合

次のように規定する。

まず、国家安全保障に属する内容に関して、傍受に関しては、第 9 条ないし 11D 条で、防衛長官(Director-General of Security)の要請基づく、法務長官の令状(telecommunication service warrant)による手続きが定められており、また保存資料へのアクセスに関しても第 108 条で同法第 9 ないし 11D 条の適用ありとする、行政傍受であると解される。

他方、警察をはじめとする当局の通信傍受に関しては、第 39 条により、有資格の裁判官または、行政訴訟裁判所(Administrative Appeals Tribunal)のメンバーで法務長官が登録した者による令状(telecommunication service warrant)発給が規定されているが、保存資料等へのアクセスに関しては、第 110 条で当局が令状(stored communication warrant)を請求することになっており、先の行政傍受とは明確に区別される司法傍受が規定されている。

(2) 司法傍受に関してより進んで監視装置を設置するなどの場合

2004 年監視装置法（Surveillance Devices Act 2004）が次のように規定する。

同法の目的は刑事捜査及び児童の取り戻しに関して、令状、緊急認可およびトラッキング装置の認可を官吏が得るための手続きを確立し、監視装置の使用によって得られた情報の利用、伝達および公表を制限し、監視装置運用に関して、記録の安全な保持と廃棄および報告書の作成の要件を課すことを目的とする（第 3 条)。

令状には、監視装置令状(surveillance device warrant)と、検索令状(retrieval warrant)とがあり（第 10 条)、有資格の裁判官（法務長官から書面で授権された裁判官（第 12 条)、この場合裁判所でなく、裁判官個人）か、または行政訴訟裁判所(Administrative Appeals Tribunal)のメンバーで法務長官が登録した者(第 13 条)によって発給される。

3.2 令状を要しない場合

令状なしに通信傍受が認められる緊急事態に関して、1979 年電気通信(傍受およびアクセス)法第 30 条では、死亡または深刻な侵害の恐れがある場合に、相手方の位置を知らない、警官または救済できそうな通信の一方当事者の緊急要請が令状なしに認められるとされている。

3.3 通信事業者側の協力

(1) 自発的開示

1997 年電気通信法によれば、キャリア、通信サービスプロバイダー、ナンバーデータベース運用者、および緊急通報担当者は通信に関わる情報または文書を開示しまたは使用することを禁じられている（第 276 ないし 278 条）が、職権(functions)を有する組織との関係では、当該組織に対して自発的に開示することが禁じられていない(第 174 条第 1 項)（但し、国家安全保障関連の場合には、個別の担当官に開示することは許されず(同条第 2 項)、承認(authorization)手続きが必要となる(第 175 ないし 176 条))。

また刑事捜査、罰金刑の執行、および公的歳入の保護の場合には、開示が合理的に必要である場合には、当局に対して自発的に開示することが禁じられておらず、担当官は特定された情報に関しては、事後承認できる。(第 177 ないし 180 条。但し適切な当局の担当者の要請がある場合を除く(第 177 条第 3 項))。

(2) 通信事業者の開示手続きと罰則

1997 年電気通信法は、第 279 条において、キャリア、通信サービスプロバイダ、ナンバーデータベース運用者、緊急通報担当者、およびそれぞれの従業者であれば、情報を開示または利用することを禁ずるものでないとし、第 280 条で、令状による法執行機関の運用（刑事捜査、罰金刑の執行、および公的歳入の保護の場合等)、または、法によりまたは法

に基づく正当化事由がある場合には承認されることが規定されている。

また第 306 条によれば、通信事業者が開示した場合には 5 日以内に開示記録を作成（通信事業者の従業者である場合には 5 日以内に通信事業者に写しを提出(第 306A 条)）し、3 年間保存しなければならないとし、違反した場合には 300 ユニット（現在、1 ユニット＝170 オーストラリアドル）以下の罰金、また、不正確な記録を作成した場合（第 307 条）には、6 か月以下の拘禁刑を規定する。

(3) 通信事業者の積極的行為

開示より一層積極的な行為に関して、1979 年電気通信（傍受およびアクセス）法第 63B 条は、通信傍受の場合、電気通信事業者の従業員は、従業員の義務として、通信傍受に必要な通信、または情報の使用を妨げないと規定する。

また、保存資料の開示の場合についても、第 128 条は、通信事業者の従業員は、技術的な助力を官吏に対して供与することは妨げないと規定する。

（参考）傍受関係処罰規定の現状

1979 年電気通信(傍受およびアクセス)法第 7 条・第 105 条	電気通信システム(もっぱら無線のみによるものを除く)を通じて伝送される会話その他の通信の傍受	2 年以下の拘禁刑
同法第 63 条・第 105 条	傍受された通信の第三者への伝達、使用、記録	
同法第 106、107 条	令状捜査による傍受の妨害または不協力	6 か月以下の拘禁刑
1995 年刑法典第 474.4 条	傍受装置の製造、広告、販売、所持	5 年以下の拘禁刑

第 6 章　韓国

小向太郎　大久保康成（情報通信総合研究所）

1 「通信の秘密」に関する法的規定

1.1 憲法上の「通信の秘密」の保護

韓国の憲法[149]第 18 条（通信の秘密）は「全ての国民は、通信の秘密を侵害されない。」と規定している。本条を通じて、個人または法人が信書、郵便物、電気通信等の通信手段によって意思を伝達、交換する場合、その通信形態、通信の当事者、配達の方法などの秘密性が侵害されないことを保障している[150]。すなわち、「通信の秘密」を国民の基本権として保護している。

1.2 法律上の「通信の秘密」の保護

通信の秘密に関係する法律の概要は、図表 1 のとおりである。

［図表 1. 通信の秘密の保護に関連する制度の概要］

対象情報	対象者	禁止・制限行為	禁止・制限の例外規定	罰則
電気通信[151]の内容（音響、文言、符号、映像）	何人も	監聴[152]（通信秘密保護法 3 条 1 項）	捜査機関、情報捜査機関の長等が、裁判所の許可等を得て行う通信制限措置、緊急通信制限措置（通信秘密保護法第 5 条～第 9 条）等	監聴する行為、内容を公開・漏洩する行為：10 年以下の懲役と 5 年以下の資格停止[153]（通信秘密保護法第 16 条第 1 項各号）
通信事実確認資料[154]	何人も	提供（通信秘密保護法第 3	・捜査や刑の執行に必要な場合に管轄地	第 13 条第 4 項[155]（通信事実確認資料の要請

149 http://www.law.go.kr/lsInfoP.do?lsiSeq=61603#0000

150 「通信の秘密保障に関する研究(2010)、Kang Tae Su(慶熙大学教授)」、「韓国憲法論（2010、博英社）」

151 「電気通信」とは、電話、電子メール、会員制情報サービス、ファクシミリ伝送、無線呼び出しなどのように有線·無線·光線およびその他の電子的方式により、あらゆる種類の音響·文言·符号または映像を送信したり受信することをいう（通信秘密保護法第 2 条第 3 号）。

152 「監聴」とは、電気通信に関わる当事者間の同意なしに、電子機器·機械装置等を使用して通信の音響·文言·符号·映像を再生·共読し、その内容を知得または収録したり、電気通信の送·受信を妨害することをいう（通信秘密保護法第 2 条第 7 号）。

153 法律によって一定期間の間、国が認めた一定資格の全部もしくは一部を停止する名誉刑の一つであり、例えば、警察や検事などの公務員や事業免許などがあたる。

154 「通信事実確認資料」とは、電気通信の日時・開始終了時間、発着信番号等相手方加入電話番号、使用度数、コンピュータ通信やインターネットのログ記録資料等をいう。（通信秘密保護法第 2 条第 11 号）

155 第 13 条第 4 項（通信事実確認資料提供の要請は要請理由、当該契約者との関連性、必要な資料の範囲記載した書面を通じて行う。但し、書面で要請できない緊急な理由がある場合は通信事実確認資料の提供を要請後、遅滞なく電気通信事業者に通信事実確認資料提供要請書を提出しなければならない）は、2005 年 5 月 26 日に削除されている。仮に、電気通信業務に携わっている者等が、該当の禁止・制限行為に違反

		条第 1 項)	方裁判所の許可等をうけた捜査機関から要請があった場合（通信秘密保護法 13 条) ・裁判所が裁判上必要な場合(法第 13 条の 2)等	手続き）に違反して、通信事実確認資料を提供したり提供した者:5 年以下の懲役または 3 千万ウォン以下の罰金（通信秘密保護法第 17 条第 6 号)
公開されていない他人との間の会話	何人も	録音、聴取（通信秘密保護法 3 条 1 項)	捜査機関、情報捜査機関の長等が、裁判所の許可等を得て行う通信制限措置、緊急通信制限措置（通信秘密保護法第 5 条～第 9 条）等	会話の録音・聴取、内容を公開・漏洩する行為：10 年以下の懲役と 5 年以下の資格停止(通信秘密保護法第 16 条 1 項 1 号)
端末固有番号[156]	何人も	提供、受領（通信秘密保護法第 3 条 3 項)	端末の開通処理・修理等、正当な業務の履行（通信秘密保護法第 3 条第 3 項)	3 年以下の懲役または 1 千万ウォン以下の罰金（通信秘密保護法第 17 条 2 項 1 号)
不法検閲した郵便物と不法監聴した電気通信の内容	何人も	証拠としての使用 (通信秘密保護法第 4 条)	無し	無し
電気通信事業者[157]が取扱う通信	何人も	侵害、漏洩（電気通信事業法第 83 条第 1 項)	捜査機関、情報捜査機関の長等が、裁判、捜査、刑の執行や国家安全保障に対する危害を防止するため	3 千万ウォン以下の過料（電気通信事業法第 104 条第 4 項 13 号)

した場合、電気通信事業法第 83 条第 2 項が適用され、94 条第 4 号により処罰されるものと思われる。

156 「端末固有番号」とは、移動体通信事業者との利用契約が締結された個人の携帯電話端末機に付与された電子の固有番号をいう（通信秘密保護法第 2 条第 12 号)。

157 電気通信事業者は「電気通信事業法」に基づき、①基幹通信事業者（電気通信回線設備を設置し、電話、インターネット接続等の公益性の高い基幹通信サービスを提供する事業者、②別定通信事業者（基幹通信事業者の通信回線設備等を利用し、基幹通信サービスを提供したり、大統領令で定める構内に電気通信設備を設置し、電気通信サービスを提供する事業者)、③附加通信事業者（基幹通信事業者から通信回線設備を賃貸し、基幹通信サービス以外の電気通信サービスを提供する事業者）の 3 つに分類される。(世界情報通信事情「韓国」(総務省 http://www.soumu.go.jp/g-ict/country/korea/pdf/082.pdf) を参考に作成)

			の情報収集目的で行う通信資料[158]の提供要請に従う場合（電気通信事業法第83条第3項）	
在職中、通信に関して知った他人の秘密	電気通信業務に携わっている者または携わった者	漏洩（電気通信事業法第83条第2項）	無し	5年以下の懲役または2億ウォン以下の罰金（電気通信事業法第94条4号）
情報通信網によって処理・保管または伝送される他人の情報、秘密	何人も	毀損、侵害、盗用、漏洩（情報通信網利用促進法第49条）	無し	5年以下の懲役または5千万ウォン以下の罰金（情報通信網利用促進法第71条）

(1) 通信秘密保護法[159]

通信秘密保護法は、通信と会話の秘密と自由に対する制限に対して、その対象を限定し、厳格な法的手続きを経るようにすることで、通信の秘密を保護し、通信の自由を伸長することを目的としている（第1条）。

第3条（通信と対話の秘密の保護）第1項は、「何人も、この法律、刑事訴訟法または軍事裁判所法の規定によらないで、郵便の検閲・電気通信の監聴や通信事実確認資料の提供をしたり、公開されていない他人との間の会話を録音または聴取できない。」と規定している。

また、第3条第3項は、「何人も、端末機器の固有の番号を提供したり、提供を受けてはならない。」と規定し、端末固有番号の授受を禁止している。なお、本項は、不法傍受のための機器の販売が盛行し、携帯電話に対する盗聴を懸念する声が高まったことから、2004年1月29日の改正により、不法傍受機器探知[160]業の放送通信委員会への登録制度導入（第10条の3新設）と同時に新設された規定である。

---

158 「通信資料」とは、利用者の氏名、住民登録番号、住所、電話番号、ID、登録日または解約日をいう（電気通信事業法第83条第3項）

159 http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%86%B5%EC%8B%A0%EB%B9%84%EB%B0%80%EB%B3%B4%ED%98%B8%EB%B2%95

160 「不法傍受機器探知」とは、この法律の規定によらないで行う監聴や会話の聞き取りに使用される設備を検出することをいう（通信秘密保護法第2条第8号の2）。

電気通信の内容、通信事実確認資料[161]および端末固有番号等に関する禁止・制限行為に違反した者に対しては、刑罰が科せられる（第 16 条等）。

(2) 電気通信事業法[162]

電気通信事業法第 83 条（通信秘密の保護）第 1 項は、「何人も、電気通信事業者の取扱い中の通信の秘密を侵害したり、漏えいしてはならない。」と規定している。本項に違反した者に対しては、刑罰が科せられる（第 104 条第 4 項 13 号）。

また、同第 2 項は、電気通信業務に従事する者または従事した者に対して「その在職中に、通信に関して知り得た他人の秘密を漏えいしてはならない。」と規定している。本項に違反した電気通信業務に従事する者または従事した者に対しては、刑罰が科せられる（第 94 条第 4 項）。

(3) 情報通信網利用促進および情報保護に関する法律[163]

情報通信網利用促進および情報保護に関する法律（以下「情報通信網利用促進法」という）第49条（秘密等の保護）は、「何人も、情報通信網によって処理・保管、または伝送された他人の情報を毀損したり、他人の秘密を侵害・盗用または漏洩してはならない。」と規定している。本条に違反した者に対しては、刑罰が科せられる（第71条）。

2 ISP の「通信の秘密」への関与に関する法的規定

2.1 迷惑メールフィルタリング

韓国で電子メールサーバーを運営する主なポータル事業者（例：Naver、Daum、Nate）は、ユーザが受信するメールに対して迷惑メールフィルタリングを実施している。

情報通信網利用促進法 50 条の 4（情報伝送サービスの提供などの制限）第 1 項は、情報通信サービス提供者[164]は、①広告性情報の伝送または受信によってサービス提供に障害が起きたり、起きる恐れがある場合、②利用者が広告性情報の受信を求めない場合、③利用契約を通じて情報通信サービス提供者が利用者に提供するサービスが不法広告性情報の伝送に利用されている場合にサービスの提供を拒否する措置を講じることができる旨を規定している。そのため、電子メールサーバーを運営するポータル事業者が実施する迷惑メールフィルタリングについては、法的な問題は生じないと考えられている。

また、情報通信網利用促進法第 50 条の 4 第 2 項は、「情報通信サービス提供者は、第 1 項による拒否措置を講じる場合、そのサービスの拒否に関する事項をサービス利用者と締

---

161 脚注 7 参照

162 http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95

163 http://www.law.go.kr/lsInfoP.do?lsiSeq=111970#0000

164 「情報通信サービス提供者」とは、電気通信事業法第 2 条第 8 号に定める電気通信事業者および営利を目的とし電気通信事業者の電気通信役務を利用して情報を提供したり、情報の提供を媒介する者をいう（情報通信網利用促進法第 2 条第 1 項第 3 号）。

結する情報通信サービス利用契約の内容に含めなければならない。」と規定していることから、利用規約による包括同意で提供することができると考えられる。

但し、迷惑メールをフィルタリングする前に、サービス利用者等の利害関係人にその事実を知らせなければならず、事前に告知することが難しい場合は、迷惑メールをフィルタリングした後遅滞なく受信者に告知しなければならない（同条第 3 項)。

2.2 帯域制御

韓国においてトラヒックの制御は、主にモバイルインターネットを中心に多量利用制限（データの使い放題プランに適用）や mVoIP（Mobile Voice Over Internet Protocol)サービスの制限といった形で提供されている。最近では、ネットワーク過負荷を起こすサービスやコンテンツのトラヒック制御に範囲を拡大し、また、効果的なトラヒック管理をするために DPI（Deep Packet Inspection）を利用しようとする動きもある。

情報通信網利用促進法第 15 条（インターネットサービスの品質向上）第 3 項は、「情報通信サービス提供者は、第 2 項の規定による基準（知識経済部長官[165]が定めて告示するインターネットサービス品質の測定・評価に関する基準）に基づいて自律的にインターネットサービスの品質状況を評価」することができると規定している。

未来創造科学部は、2013 年 12 月に「通信網の合理的管理・利用とトラヒック管理の透明性に関する基準」（以下「ガイドライン」という）を発表[166]しており、インターネットサービスプロバイダ（以下「ISP」という）のトラヒック制御を認めている[167]。

また、ガイドラインは、「ネットワーク事業者はトラヒック管理情報に関する事項を利用約款に規定しなければならず、インターネットホームページなどユーザのアクセスが容易な方式で案内しなければならない」と規定していることから、利用約款による包括同意で提供することができると考えられる。

但し、ISPがトラヒック管理に必要な措置を取る場合は、その事実を当該ユーザに電子メール、SMS（short message service）などを通じて告知しなければならず、個別的な告知が難しい場合に限ってISPのインターネットホームページなど様々な手段を通じてその事実をユーザに知らせる

---

165 2013 年 2 月朴大統領就任後の行政組織再編により、未来創造科学部へ、放送通信委員会や知識経済部等の業務のうち、科学技術、情報通信技術、放送・通信等に関する業務が移管された。（国立国会図書館調査および立法考査局，「外国の立法」（2013.5）
http://dl.ndl.go.jp/view/download/digidepo_8205979_po_02550208.pdf?contentNo=1

166 合理的なトラヒック管理の種類として、①DDos、マルウェア、ハッキング、通信障害対応などネットワークの安全性と信頼性確保のために必要な場合、②ネットワークの混雑から多数の利用者を保護し、全ての利用者の公平なインターネット利用環境を確保するため、必然的に限定的なトラヒック管理をする場合、③関係法令の執行のために必要なまたは法令や利用規約等に基づく利用者の要請がある場合を挙げている。（「未来部、合理的なトラヒック管理基準の制定」（2013.12.4）
http://www.korea.kr/policy/pressReleaseView.do?newsId=155931604）

167 ガイドラインでは、トラヒック制御を行う場合、関係法令を守るよう規定していることから、例えば、通信の秘密に関して、「監聴」を禁止する通信秘密保護法 第 3 条(通信および会話の秘密の保護)との適用関係が問題となる可能性がある等、解釈に疑義が生じている。そのため、現在、政府側からの明確な基準の提示が求められている。

ために努力しなければならない。また、ISPは個別ユーザの自己統制権の保障と合理的インターネットの利用のために技術的に可能な範囲内でユーザが自分のトラヒック使用現状を確認できるようにしなければならない(ガイドライン)。

2.3 大量通信等に対する通信遮断

韓国の通信キャリアやISPは、自動探知・遮断システムを活用して、発生したDDoS攻撃を探知・遮断している。

情報通信網利用促進法第46条の2(集積情報通信施設事業者の緊急対応)第1項は、「集積情報通信施設事業者[168]は、次の各号のいずれかに該当する場合には、利用規約に定めるところにより、そのサービスの全部または一部の提供を中断することができる。」と規定している。中断することができるのは、集積情報通信施設を利用する者(以下 「施設利用者」という。)の情報システムで発生した異常現象によって、他の施設利用者の情報ネットワークや集積された情報通信施設の情報ネットワークに深刻な障害が発生するおそれがあると判断される場合等(同項各号)である。そのため、通信キャリアやISPが実施する大量通信等に対する通信の探知、遮断については、法的問題は生じないと考えられている。

また、「利用規約に定めるところにより、そのサービスの全部または一部の提供を中断することができる。」と規定していることから、利用規約による包括同意で提供することができると考えられる。

但し、サービスの提供を中断する場合は、中断事由、発生日時、期間、内容などを施設利用者に直ちに通知しなければならず(同第2項)、中断事由がなくなった場合は直ちに、そのサービスの提供を再開しなければならない(同第3項)。

2.4 不正・有害サイトへのアクセスブロック

(1) 実施状況

主なISP(例:KT、SKブロードバンド)は、自社のブロードバンド契約者向けに契約者のPCに追加的な設定をせずに不正・有害サイト(猥褻、暴力、自殺、賭博など)へのアクセスをブロックするサービスを有料(月3千ウォン)で提供[169]しており、当該有料サービスを利用するユーザが不正・有害サイトへのアクセスを試みた場合、「当該サイトへのアクセスをブロックする」旨のメッセージを画面で通知している。また、ISPは、ユーザが放送通信委員会およびサイバー警察庁に登録された不正・有害サイトへアクセスしようとした場合、警告サイト[170]へ誘導し、アクセスしようとしているサイトが不正・有害サイトであることを通知している。

情報通信網利用促進法第44条の7(不法情報の流通禁止)第1項は、「何人も、情報ネット

---

168 「集積情報通信施設事業者」とは、他人の情報通信サービス提供のために集積された情報通信施設を運営・管理する事業者をいう(情報通信網利用促進法第46条第1項)。

169 当該サービスに契約するとインターネット通信網上で不正・有害サイトへのアクセスが遮断される。主なISPの発表資料(例:http://internet.olleh.com/web.html?int-zone-clean-serviceinfo)によると遮断率は98%に至っている。

170 http://www.warning.or.kr/

ワークを介して、次の各号のいずれかに該当する情報を流通してはならない。」と規定している。流通してはならない情報として、卑猥な情報、誹謗中傷・名誉を毀損する情報、法令で禁止されている行為に該当する内容の情報等（同項各号）を規定している。また、放送通信委員会は、当該情報に対して、審議委員会の審議を経て情報通信サービス提供者または掲示板の管理・運営者にその取り扱いを拒否・停止または制限するように命じることができる（同条第 2 項）。そのため、ISP が実施する不正・有害サイトへのアクセスブロックについては、法的な問題は生じないと考えられる。

2.5 行動ターゲティング広告

Web サイトを利用してビジネスを行っている事業者は、自社の顧客向けのマーケティング、サービス競争力強化などのために、行動ターゲティング広告を実施している。

韓国では、行動ターゲティング広告を禁止する法的規定はない。また、政府レベルのガイドライン、自主規制ガイドラインも発表されていない。

ユーザの行動履歴情報は、非識別個人情報にあたり、識別個人情報と組合わせていない状態で匿名で処理されている場合は、公開および活用が禁止された個人情報に当たらない（情報通信網利用促進法第 2 条[171]、個人情報保護法第 2 条[172]）。また、当該事業者がサービスを提供する過程で生成されるアクセスログやクッキーの情報等を収集する行為は、監聴とは見られない。そのため、当該事業者が実施する行動ターゲティング広告については、法的な問題は生じないと考えられている[173]。

また、ユーザの行動履歴情報の行動ターゲティング広告への利用については、利用者の同意は不要と考えられる。

3 公権力の「通信の秘密」への関与に関する法的規定

3.1 法執行の概要

通信秘密保護法は、捜査機関等による通信制限措置・通信事実確認資料の要請が認められる場合および電気通信事業者の通信秘密保護法による法執行に対する協力義務について規定している。また、電気通信事業法は、捜査機関等による通信資料の提出の要請が認められる場合および電気通信事業者がこれに応じることができる旨について規定している。

法執行の概要は、図表 2 のとおりである。

---

171 「個人情報」とは、生存する個人に関する情報で氏名・住民登録番号などにより特定の個人を認識できる符号・文字・音声・音響や映像などの情報（その情報だけでは特定の個人を認識することができなくても、他の情報と容易に結合して認識可能な場合は、その情報を含んでいる）をいう。

172 「個人情報」とは、生存する個人に関する情報として、氏名、住民登録番号、映像等を通して、個人を認識できる情報（その情報だけでは特定の個人を認識できなくても他の情報と容易に結合して調べることができるものを含む）をいう。

173 インターネット振興院，未来創造科学部へのインタビューによる。

［図表 2. 法執行の概要］

法執行等の内容	法執行機関等	目的	要件	手続等	条文
通信制限措置[174]	捜査機関	犯罪捜査	通信秘密保護法第 5 条第 1 項各号の罪の計画・実行している場合等で、他の方法では、所定の犯罪の実行を阻止したり、犯人逮捕や証拠の収集が困難な場合	裁判所（軍事裁判所含む）へ許可を請求し、裁判所が承認	通信秘密保護法第 5 条、第 6 条
	情報捜査機関の長	国家安全保障	国家安全保障に対する重大なリスクが想定され、その危害を防ぐために、情報収集が特に必要があるとき	通信の一方または双方の当事者が内国人の場合：高等裁判所首席部長判事の許可 【例外】敵対する国家等の場合および軍事電気通信の場合、大統領の承認	通信秘密保護法第 7 条
緊急通信制限措置	捜査機関または情報捜査機関の長	国家安全保障、犯罪捜査	国家安全保障を脅かす陰謀の計画等緊迫した状況にあり、所定の手続きを踏むことができない場合	裁判所の許可なく実行可。但し電気通信事業者に対し、36 時間以内に裁判所の許可書の提出要	通信秘密保護法第 8 条
通信事実確認資料の提供の要請	捜査機関	捜査や刑の執行	捜査や刑の執行のために必要な場合	管轄裁判所（軍事裁判所を含む）、支院の許可 【例外：許可を	通信秘密保護法第 13 条

174 「通信制限措置」とは、郵便の検閲または電気通信の傍受をいう（通信秘密保護法第 3 条第 2 項）。

				受けることができない緊急の事由があるときは、要請後遅滞なく許可を得る】	
	捜査機関、情報捜査機関の長	国家安全保障	国家安全保障に対する危害を防止するために情報収集が必要な場合	通信制限措置等の手続きを準用	通信秘密保護法第13条の4
電気通信事業者の協力義務	裁判所、捜査機関、情報捜査機関の長	通信秘密保護法による法執行	裁判、捜査、刑の執行又は国家安全保障に対する危害を防ぐための情報収集	①通信制限措置、通信事実確認資料の提供の要請への協力 ②通信事実確認資料の保管期間 ・タイムスタンプ発着信日時等：12ヶ月 ・通信ログ：3ヶ月　等	通信秘密保護法第15条の2、通信秘密保護法試行令第41条
電気通信事業者の、通信資料の閲覧および提出要請への協力	裁判所、捜査機関、情報捜査機関の長	刑の執行および国家安全保障	裁判、捜査、刑の執行または国家安全保障に対する危害を防ぐための情報収集	所定の内容を書面上にて要請【例外：緊急な理由があれば書面上でなくても要請可[175]】	電気通信事業法第83条第3項～第9項

3.2 電気通信事業者の捜査機関等へ協力状況

(1) 通信制限措置および緊急通信制限措置

電気通信事業者は、通信秘密保護法第5条、第6条または第7条に従い捜査機関または情報捜査機関の長から裁判所の許可等に基づく通信制限措置の要請があった場合、または通信秘密保護法 第8条に従って裁判所の許可無しで緊急通信制限措置の要請があった場合

[175] 年2回未来創造科学部長官に通信資料の提供現状の報告義務がある。

は、当該要請に協力しなければならない（通信秘密保護法第 15 条の 2 第 1 項）。なお、緊急通信制限措置の要請を行った捜査機関もしくは情報捜査機関の長は、電気通信事業者に対し、36 時間以内に裁判所の許可書を提出しなければならない。

2011 年から 2013 年上半期までの通信制限措置および緊急通信制限措置の件数は、表 3 のとおりである。

［図表 3.通信制限措置および緊急通信制限措置の件数[176]］

	2011 年		2012 年		2013 年
	上半期	下半期	上半期	下半期	上半期
通信制限措置	444	263	267	180	255
緊急通信制限措置	0	0	0	0	0
合計	444	263	267	180	255

(2) 通信事実確認資料の要請件数

電気通信事業者は、通信秘密保護法第 13 条または第 13 条の 4 に従い捜査機関または情報捜査機関の長から裁判所等の許可に基づく通信事実確認資料の提供要請があった場合、または裁判所等の許可を受けることができない緊急の事由があり裁判所の許可を受けずに通信事実確認資料の提供要請があった場合（但し、事後遅滞なくその許可を受けて送付しなければならない）は、当該要請に協力する義務がある。

2011 年から 2013 年上半期までの通信事実確認資料の要請件数は、表 4 のとおりである[177]。

［図表 4.通信事実確認資料の要請件数[178]］

	2011 年		2012 年		2013 年
	上半期	下半期	上半期	下半期	上半期
通信事実確認資料	124,658	111,058	119,306	120,002	133,789

3.3 通信資料をめぐる議論動向

(1) 通信資料に関する訴訟

(a) 2012 年 10 月 18 日に、ポータルサイトの Naver を運営する NHN が令状無しにユーザの身上情報を警察に提供した件に対してそのユーザが提起した損害賠償請求訴訟で 50 万ウォンの賠償判決が下された[179]。現在、最高裁判所で争われている。

それまで、電気通信事業者は、電気通信事業法 第 83 条 第 3 項および第 4 項に基づき裁判所の令状が要らない通信資料の提供要請に応じていたが、2012 年 11 月より Naver、Nate、Daum、Kakaotalk など主なポータルサイトや ISP は、令状のない通信資料の要

176 出典：未来創造科学部

177 裁判所の許可を受けずに要請した通信事実確認資料の件数は集計されていないが極めて少ないと思われる（未来科学創造部へのインタビュー）。

178 出典：未来創造科学部

179 http://www.fnnews.com/view?ra=Sent0901m_View&corp=fnnews&arcid=201210180100160070009792&cDateYear=2012&cDateMonth=10&cDateDay=18

請を拒否している。

(b) 情報通信網利用促進法第 30 条は、情報通信サービスのユーザは個人情報を利用したり第三者への提供状況について閲覧や情報提供を要求することができる旨を規定している。しかし、実際ユーザが電気通信事業者に通信資料の提供現況について閲覧を要求したが当該事業者が当該要求を拒否したことから、2013 年 4 月 16 日に、市民団体が移動通信 3 社（SK テレコム、KT、LG 電子ユープラス）を相手に損害賠償の訴訟を提起した[180]。

(2) 通信資料の捜査機関への提供とユーザへの通知に関する議論動向

通信秘密保護法は、第 13 条の 3 の条項に従って、捜査機関が通信事実確認資料の提供を受けた事件に対して処分を下した日から 30 日以内に通信事実確認資料の提供を受けた事実と提供要請機関および通信事実確認資料の提供を受けた期間を書面にてユーザに通知することとなっている。しかし、電気通信事業法で規定する通信資料は通知の義務が規定されていない。

通信資料は、ユーザに関する重要な情報であるにもかかわらず、照会があったことを当該ユーザに通知しないことが制度上の問題として指摘されている。そのため、通信信資料も通信事実確認資料と共に電気通信事業法ではなく通信秘密保護法によって取扱うべきとの主張がある。他方、通信資料の提供を通信秘密保護法によって取り扱う場合、法的手続きが複雑になり初動捜査が円滑に進まず犯罪捜査が適切に行われなくなるとの懸念も指摘されている。 通信資料の取扱いについては、現在国会で議論が行われている[181]。

［図表 5.通信事実確認資料と通信資料との差異］

	通信事実確認資料	通信資料
根拠法	通信秘密保護法	電気通信事業法
提供範囲	電話番号、通話日時および時間、発着信番号、接続地資料、インターネットログ記録、基地局の位置追跡情報	氏名、住民番号、住所、電話番号、ID、登録・解約日付
要請機関	捜査機関、情報捜査機関の長、裁判所	捜査機関、情報捜査機関の長、裁判所
要請手続き	地方裁判所の許可が必要	4 級以上の公務員(捜査官署長)の決裁が必要
通知義務	捜査機関が控訴提起/未提起/立件/不立件/などの処分後 30 日以内に資料の提供を受けた事実と提供要請機関および期間について通報	無し

180 http://www.lawissue.co.kr/news/quickViewArticleView.html?idxno=14691
181 未来創造科学部へのインタビューによる。

第 3 部　付属資料

1 参加者名簿

区分	所属組織	氏名
構成メンバー	エヌ・ティ・ティ・コミュニケーションズ株式会社	中ノ堂　哲也
同	株式会社 KDDI 総研	泉　健太郎
同	株式会社 KDDI 総研	村上　陽亮
同	ソネット株式会社	大竹　淳朗
同	ソネット株式会社	山本　丈敏
同	ニフティ株式会社	林　一司
同	ニフティ株式会社	岡本　明
同	ビッグローブ株式会社	神場　知成
同	ヤフー株式会社	島田　健太郎
同	ヤフー株式会社	古閑　由佳
同	Telecom-ISAC	飯塚　久夫
調査メンバー	桐蔭横浜大学	笠原　毅彦
同	情報通信総合研究所	小向　太郎
同	情報通信総合研究所	大久保　康成
同	米国弁護士	城所　岩生
同	京都大学法科大学院	曽我部　真裕
同	弁護士	高橋　郁夫
同	駒澤大学	松前　恵環

同	清和大学	吉田　一雄
同	モバイルコンピューティング推進コンソーシアム・モバイルセキュリティ委員会	代表:山澤　昌夫 事務局:横尾　俊夫
協賛メンバー	キヤノングローバル戦略研究所	鈴木　倫夫
事務局	情報セキュリティ大学院大学	林　紘一郎
同	情報セキュリティ大学院大学	田川　義博
同	桐蔭横浜大学	橋本　清貴

2　研究会、調査会開催状況

日時	会合名	議事概要	場所
2013年9月25日	調査グループ（予備）会合	・ 調査グループへの参加意思の確認と分担の相談 ・ ヤフー様に依頼する質問状の検討 ・ 手持ち資料の共有	情報通信総合研究所
11月1日	第1回全体会合	・ メンバー紹介 ・ 第２期重点テーマの確認 ・ 質問状の紹介	キヤノングルーバル戦略研究所
11月6日	第1回調査グループ会合	・ ヤフー様経由の回答の紹介 ・ スケジュールの確認 ・ 国別分担の決定	機械振興会館会議室（MCPC 提供）
11月26日	第2回調査グループ会合	・ プロバイダ概念の再検討 ・ 関連情報の共有	機械振興会館会議室（MCPC 提供）
12月27日	第3回調査グループ会合	・ プロバイダ概念の整理に関する補足 ・ 韓国を例にした調査事項の整理 ・ 国別報告 ① イギリス	機械振興会館会議室（MCPC 提供）
2014年1月29日	第4回調査グループ会合	・ 国別報告 ② アメリカ ・ ヤフー様経由の第２次調査の進捗状況 ・ 各国調査の共通事項の検討	機械振興会館会議室（MCPC 提供）
2月19日	第5回調査グループ会合	・ 国別報告 ③ フランス ・ 国別報告 ④ ドイツ	機械振興会館会議室（MCPC 提供）
3月6日	第2回全体会合	・ プロジェクトの進捗状況 ・ ヤフー様経由の第２次調査に見る各国比較 ・ 各国調査の共通事項	情報セキュリティ大学院大学
3月24日	第6回調査グループ会合	・ 国別報告 ⑤ 英連邦 ・ 国別報告 ⑥ 韓国 ・ 各国調査の共通事項の合意	機械振興会館会議室（MCPC 提供）
4月15日	第7回調査グループ会合	・ 各国調査の共通事項の確認 ・ 報告書の提出期限・様式等の合意	機械振興会館会議室（MCPC 提供）

5 月 14 日	第3回全体会合	・ 国別調査結果報告会	青 学 会 館 Ivy Hall 会議室
5 月 29 日	第4回全体会合	・ 報告書最終確認	キヤノングルーバル戦略研究所