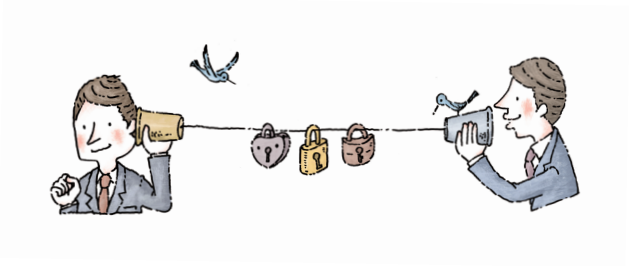
情報通信の現在と未来を展望する

Vol.16
2013 Winter
ネクストコム

Nextcom

特集 インターネット時代における 通信の秘密



Feature Papers

論文
インターネット媒介者の役割と「通信の秘密」
高橋 郁夫 BLT法律事務所所長・弁護士／宇都宮大学 講師

論文
通信の秘密の憲法解釈論
曽我部 真裕 京都大学 大学院 法学研究科 教授

論文
国家安全と通信の秘密
石井 夏生利 筑波大学 図書館情報メディア系 准教授

Report

学会リポート
「International Communication Association（ICA）Annual Conferences」参加報告
米谷 南海 慶應義塾大学 大学院 政策・メディア研究科 後期博士課程

Articles

すでに始まってしまった未来について
奇妙な感覚の麻痺
平野 啓一郎 作家

情報伝達・解体新書
もてるクジャクは声で勝負
高橋 麻理子 東京大学 大学院 総合文化研究科 附属進化認知科学研究センター 特任研究員

やさしいICT用語解説
4K・8K

明日の言葉
ガリレオの言い訳
髙橋 秀実 ノンフィクション作家

明日の言葉

それでも地球は回っている。
……ガリレオ・ガリレイ

イタリアの天文学者ガリレオ・ガリレイは、
地球は動くということを記した『天文対話』を発刊。
その罪に問われ、1633年に開かれた第2回目の異端審問で有罪となり、
地動説を放棄する宣誓をする。
その時、彼はこうつぶやいたと伝えられる。「それでも動く」と。

INDEX
winter
2013

Nextcom ネクストコム

特集

インターネット時代における
通信の秘密

写真©FELIX PHARAND-DESCHENES, GLOBAIA/SPL/amanaimages
夜のユーラシア大陸

すでに始まってしまった未来について ―― ⑯

文：平野啓一郎
絵：大坪紀久子

「奇妙な感覚の麻痺」

元CIA職員のエドワード・スノーデンが暴露したアメリカのNSA（国家安全保障局）の情報収集活動が世界中の顰蹙を買っている。以前からNSAは、アメリカに加えて、イギリス、カナダ、オーストラリア、ニュージーランドの5カ国で地球規模の通信傍受システム〈エシュロン〉を運用しているだとか、PRISMなる通信監視プログラムを使用しているといった噂があったが、真相は謎のままだった。

今回、NSAの活動の実体が初めて証拠とともに明らかになったわけだが、最初のショックの後、スノーデン情報の分析が進むにつれて、騒ぎはますます大きくなってきている。

その疑惑は、オバマ政権が強調するテロ計画の未然防止のみならず、各国大使館の通信傍受から、クレジットカードの国際決済情報収集（シュピーゲル紙）、NSAの職員を「一般的なユーザーがネット上でするほぼすべて」にアクセスさせ得るX-Keyscoreなるソフトの存在（ガーディアン紙）と、留まるところを知らない。

ネットが一般に普及して、せいぜい15年ほどだが、その間、ほとんど同期的に、これほどまでの監視体制が構築されていた。元々、インターネットが軍事技術の応用であったことを考えるなら、さもありなんということなのかもしれないが、私が気になるのは、この報道に接した私たち自身の感覚の麻痺である。

このニュース以降、ネットのやりとりで秘密の話を一切止めたという人が、一体どれくらいいるだろうか？　テロリストや活動家は警戒しているのだろうが、その他の人は、恐らく以前と何ら変わらずネットに接している。一ユーザーである自分に、一体何が出来る？　文句を言ってみたところで、NSAはこう言うに違いない。「世界中の膨大な情報を処理しなきゃならんのですよ。なんであんたの不倫の証拠や同僚の悪口なんかにいちいち構ってられます？」と。

そうしてNSA事件は、一般にはどこか他人事である。そこに状況の不気味さがある。

Keiichiro Hirano

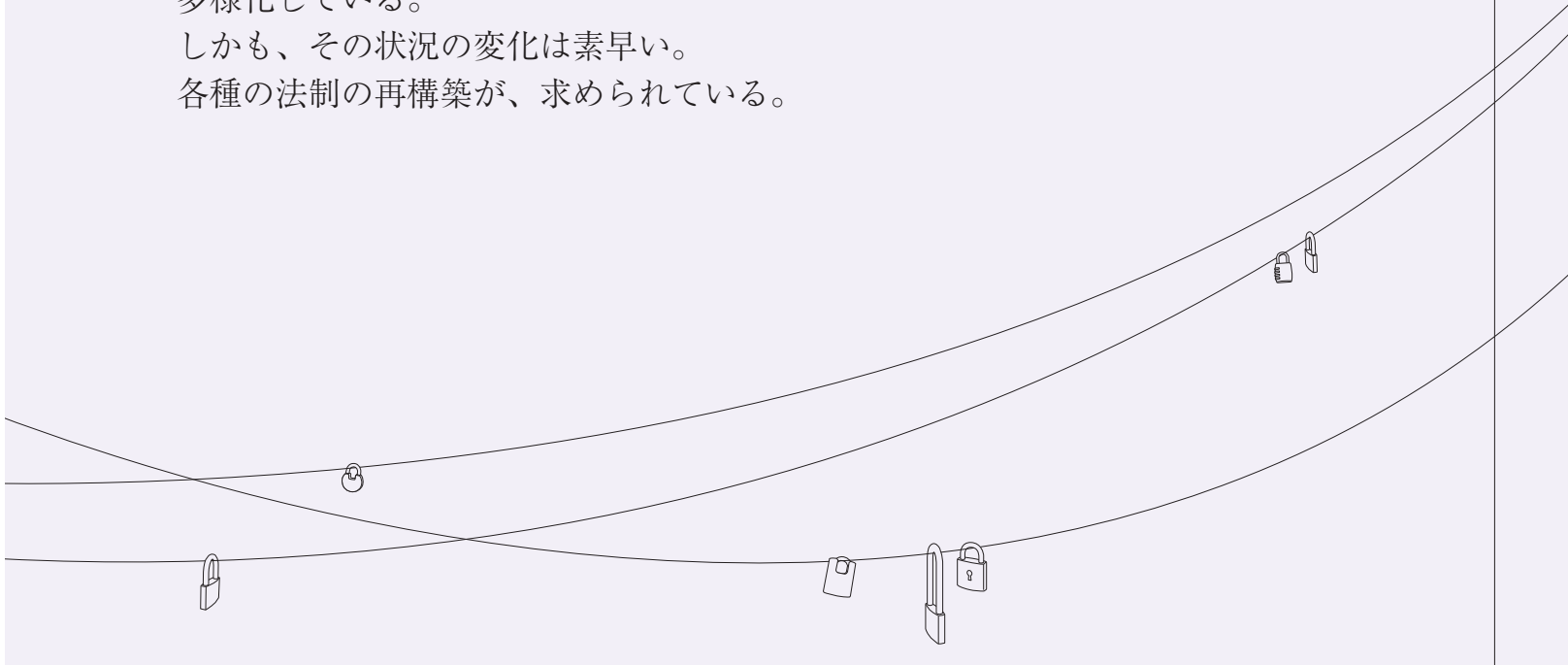
小説家。1975年生まれ。1999年京都大学在学中に『日蝕』により芥川賞を受賞。
以後、『葬送』、『ドーン』、『かたちだけの愛』など、数々の作品を発表し、各国で翻訳紹介されている。
近著は『私とは何か ―「個人」から「分人」へ』（講談社現代新書）。最新刊は『空白を満たしなさい』（講談社）。

特集

インターネット時代における

通信の秘密

「通信の秘密」として保護されるべき部分が、
多様化している。
しかも、その状況の変化は素早い。
各種の法制の再構築が、求められている。



インターネット時代における
通信の秘密1

インターネット媒介者の役割と「通信の秘密」

BLT 法律事務所所長・弁護士／宇都宮大学 講師

高橋 郁夫 Ikuo Takahashi

安全・安心なインターネットを健全に利用する環境を提供するという観点から、
現代社会において「インターネット媒介者」のなすべき積極的な役割は、極めて増大している。
対応すべき分野は、発信者情報の開示、ボットネット探知と削除推奨、
分散型サービス拒否攻撃（DDos）対応、などの情報セキュリティ分野、
DPI（Deep Packet Inspection）技術による広告配信分野、
違法有害情報対応など多岐にわたっている。このような状況の下、
「通信の秘密」の保護の合理的な期待とのバランスを念頭におきつつも、
それらの活動を肯定し、促進できるように「通信の秘密」は、現代的に展開される必要がある。

キーワード
通信の秘密　情報セキュリティ　ボットネット　DDoS　違法有害情報対策

1. インターネット媒介者の概念の役割の増大

1.1　インターネット媒介者の概念

現在、ISPを始めとする「インターネット媒介者」（Internet　Intermediaries）が、インターネットの通信で重要な役割を果たすべきではないかという議論が盛んに行われている。経済協力開発機構（OECD）は、インターネット媒介者を「インターネットの第三者間の通信を伝達し、または、促進するものであって、インターネットにおいて、第三者によって行われるコンテンツ、製品、サービスに対して、アクセスさせ、ホストし、送信し、指し示す、若しくは、インターネットのサービスを第三者に提供するものをいう」と定義している[1)]。この定義の下、ISP、サーチエンジン、ドメイン名レジストラーなどが、インターネット媒介者に該当すると考えられている。

現代においては、ISPは、単なる土管として通信を送

り届け、または、そのために貢献するという業務に尽きるわけではなく、利用者がより良いインターネットを経験できるように積極的な役割を果たすべきではないかと考えられる。そして、この理は、ISPのみならず、サーチエンジン、ドメイン名のレジストラーなどインターネットに関わるインターネット媒介者一般にも適用され、そのような中間者が積極的に活躍すべき場所が増大していると考えられる。

その一方で、従来、通信法制は、無線、電報、電話を念頭に発展してきたものと考えられるが、それらにおける「通信の秘密」をそのまま、インターネットの通信に適用するとき、上記のような「インターネット媒介者」のなすべき積極的な役割の増大という社会の要請に応えられないのではないかという懸念も大きいものと考えられる。

本稿は、このような「インターネット媒介者」の果たすべき役割が増大している状況、並びに従来の憲法・電気通信事業法を基にしたどのような解釈論的な対応がなされているのかを客観的に把握するものとする。そして、かかる対応の限界を把握するとともに、今後の解決に向けての方向性を考察するものとする。

1.2　インターネット媒介者の役割の増大

現在、具体的に、インターネット媒介者の活躍すべき場面は、名誉毀損（きそん）メッセージの削除、フィッシングメールのテイクダウンと言われる手続き、スパムサイトの遮断、DDos対応、違法有害情報についてのフィルタリング、児童ポルノ遮断、知的財産権侵害通信についての制御などに広がっている。これらの分野における「通信の秘密」との関係を包括的に考察する[2)]ことが検討の最初ということになる。

2. インターネット媒介者の活動と「通信の秘密」との関係

2.1　従来の解釈について

日本国憲法は、第21条2項において、「通信の秘密は、これを侵してはならない」と定めている。この規定において、「通信」とは、一般的に郵便・電信・電話などによって意思や情報を伝達することをいうと解釈されている。そして、その「通信の秘密」の保護する範囲については、保障の対象となる『すべての形式の通信』は、通信の内容にとどまらず、差出人・発信人・受取人・受信人の氏名・住所はもとより、通信配達の日時や、郵便物ないし電信・電話の差し出し個数など通信に関わる全ての事実に及ぶとされている。また、このような規定の効力は、自然人間においても効力を有すると考えられている。また、一般的な解釈においては、関連する制定法として、電気通信事業法4条・有線電気通信法の定めを挙げ、これらは、21条2項の確認としての意味を持つものとしている。

電気通信事業法4条は、電気通信に関する秘密の保護との関係を一般的に定めている。具体的には、（秘密の保護）とのタイトルの下、1項で、「電気通信事業者の取扱中に係る「通信の秘密」は、侵してはならない」としており、2項で電気通信事業従事者が「通信に関して知り得た他人の秘密を守らなければならない」としているのである。また、この「通信の秘密」の侵害については、刑事罰が準備されており（同法179条1項）、電気通信事業従事者については、刑が加重されている（同2項）。この「侵してはならない」という行為については、「積極的な取得の禁止・窃用の禁止・漏えいの禁止」を意味するものと考えられている。実務的には、「窃用」が、単に「用いること」と同義であると解釈されている。また、「通信の秘密」の当事者は、両当事者と考えられており、片側の通信当事者が同意

をなしたとしても、その秘密の利益は、奪われることはないということも留意されなければならない。

また、電気通信事業法は、電気通信役務の提供について差別的な取り扱いをしてはならないことをも定めている（同法6条）。この「差別的取扱の禁止」の条文と「秘密の保護」の条文とが相まって、電気通信事業者は、通信の伝達のみに関わっていれば足りる、そして、通信それ自体について差別的な取り扱いをしてはならないというモデル[3]を構築しているということが言えるであろう。そして、このモデルがインターネット媒介者にも適用されたものの、安全・安心なインターネットを健全により多くの人に提供すべきだという現実の考えの下に、修正を余儀なくされていると把握するのが筆者の立場である。

上述の一般的な解釈を前提の下、既に紹介したインターネット媒介者の活動が、どのように法的意味付けがなされているかという点についてまとめてみることにしよう。

2.2　インターネット媒介者の活動の分類の視点

インターネット媒介者の行為で、具体的な問題となる実務的な活動を、問題となる通信構成要素との関係で、分類して論じてみることにしよう。

なお、この分類にあたって、インターネット媒介者が、了知し、利用する行為の対象が、通信の内容に関わるのか否かという点を配慮すべき要素としている。これは、筆者が、「通信の秘密」と言われてきた特定通信に関する通信の構成要素に関する秘密のものの中に

図表　インターネット媒介者の活動に関する具体的な問題

内容か否か	問題	具体例など
非	発信者情報の開示	匿名掲示板での発信者のIPアドレス・プロバイダと契約者間の契約者情報など
非	ボットネット化の探知と削除推奨	サイバークリーンセンターの実務
非	DDoS対応	大量通信等ガイドライン
非	スパムサイトの遮断	特定電子メール法
内容	フィッシングメールのテイクダウンなど	ISPのテイクダウン活動 米国におけるマイクロソフト社のプロジェクト
非／内容	DPIを用いた分析・宣伝行為	
内容	有害情報フィルタリングなど	青少年インターネット環境整備法など
内容	名誉棄損サイトの削除	プロバイダ責任制限法など
内容	児童ポルノ遮断	児童ポルノ排除総合対策
内容	知的財産権侵害通信など	プロバイダ責任制限法商標権関係ガイドラインなど

は、通信の内容に関する「通信の秘密」と通信データに関する「秘密」の二つの種類があり、しかも、かかる種別は、電気通信事業法の4条1項の「通信の秘密」と同2項の「他人の秘密」に対応すると考えることも関連する[4]。インターネット媒介者がどのような情報を基に、どのような行動をとっているのか、その取得されている情報、利用される態様、共有される範囲には、どのようなものがあるのか、ということをまとめることは、インターネット媒介者の役割の法的な位置付けを考えるときに大いに役立つものと考えられる。

2.3 具体的な活動と法的な位置付け

インターネット媒介者の活動に関して具体的に問題となる事案・活動をまとめると左の図表のようになる。

これらの事案・活動やそれらとの法律との関わりを実際に詳述すると以下のようになる。

(1)発信者情報の開示

これは、匿名掲示板での発信者のIPアドレスや契約者情報を開示させる活動である。法的には、いわゆるプロバイダ責任制限法によって、権利の侵害が明らかであり、正当な理由があるときに、被害を受けたものは、ISP等に対して開示の請求をなすことができるとされている（同法4条1項）。この具体的な発信者情報開示について、同法の逐条解説[5]は「発信者情報は、発信者のプライバシー及び匿名表現の自由、場合によっては「通信の秘密」として保護されるべき情報であるから、正当な理由もないのに発信者の意に反して情報の開示がなされることがあってはならないことは当然である。」として、「通信の秘密」を発信者情報の開示に厳格な要件が求められる一つの理由としている。また、「裁判外での開示請求については、とりわけ慎重に対応することを要請されることとなる。」としており、実質上、裁判以外での開示を認めないかのような表現がなされていた[6]。

このような規定及び実際の運用についての解説は、例えば、名誉棄損の被害者などに対して、裁判による発信者情報の開示を強いていたとも評し得るものであって、我が国のインターネットでの発言の匿名的な性格をさらに強くしたのではないかというように考えられる。

(2)ボットネット化の探知と削除推奨

コンピュータが、悪性プログラムに感染すると悪意を持った第三者が、コンピュータを外部から遠隔操作することができるようになり、そのような操作されるコンピュータをボットと呼び、そのようなコンピュータからなるネットワークをボットネットという。一般のインターネットユーザーのコンピュータが、セキュリティ上の弱点に対する対応をしないでいると、上記の悪意あるプログラムに感染し、ボットネットになってしまう場合がある。このような場合に、ISP等が、ユーザーに対して、そのPCが感染していることを通知し、削除プログラムなどの導入を支援する活動がある。これの代表的な活動として、2006年より2011年まで行われたサイバークリーンセンターを挙げることができる[7]。

また、同様の活動は、海外でも活発になってきている。ドイツでは、我が国の動きから影響を受けて2010年9月より官民連携ボット対策プロジェクトが導入されており、また、オーストラリアでもicode[8]というボットネット対応プログラムが導入されている。

ISP等は、技術的には、ユーザーのPCのトラフィックを、シグネチャ、ネットワークトラフィック異常、C&C セッションの応答時間、制御コマンド等の異常やボットの協調動作による検出など[9]から、ボットネットへの感染を確認することができる。また、前述のサイバークリーンセンター[10]では、検体等の分析か

ら、感染ユーザーを特定するのに役立てており、感染が疑われる場合に、ボットプログラム削除ツールなどを提供している。

上述のような技術的に可能な探知行為を活用する場合には、我が国の従来の「通信の秘密」に関する考え方を適用すると、「通信の秘密」に関する積極的な取得であり、また、通信の伝達に必要な限りを越えて利用するものであって、電気通信事業法に違反するとされる可能性が存在する。

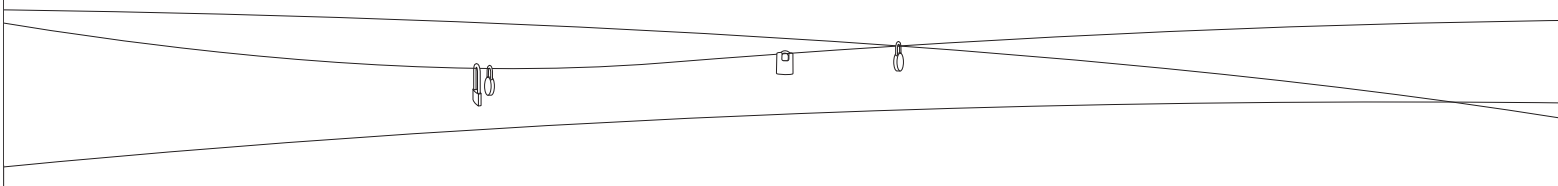
(3) DDos攻撃対応

DDos攻撃とは、ネットワーク上の関係のない複数のコンピュータに攻撃プログラムを仕込んでおき、それらの分散している複数のコンピュータから一斉に特定のサーバーを標的とした攻撃をいう[11]。IPA報告書においては、国内、国外の著名なDDos攻撃の例が紹介されている。特に近時は、金銭的動機に基づく攻撃、政治的背景を動機とした攻撃などが目立つようになってきている。このような攻撃に対して、ISP等は、DDoS対策装置により、ユーザー回線へのDDosトラフィックを遮断するという仕組みを備えるようになってきている。また、韓国においては、2009年7月7日に大規模なDDoS攻撃を受け(7.7大乱と言われている)、それを基に防御の体制を整え[12]、2011年3月4日に発生した、より巧妙かつ大規模な攻撃からの被害を極めて小規模に押さえ込んだとされている。

このDDos攻撃対応を始めとして、その他、マルウェアの感染拡大、迷惑メールの大量送信及び壊れたパケット等の通信をもまとめて「大量通信等」と呼び、その際のISP等の活動で、「通信の秘密」との衝突等の問題を整理したのが、社団法人日本インターネットプロバイダー協会他の「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」[13]である。具体的にDDos攻撃対応に関して言えば、被害者からの申告・同意がある場合の遮断、事業者側に支障が生じる場合の遮断・DNS(Domain Name System)の変更、送信元不正使用の場合の遮断、壊れたパケットの廃棄などについて、「通信の秘密」との整理が行われている。ここでは、取得・窃用の問題のみならず、攻撃情報の交換等の漏えい(共有)の問題も整理されている。詳細については、当該ガイドラインを参照いただきたいが、従来の解釈の枠組みを基に正当防衛、緊急避難、正当業務行為などの解釈により許容される活動等が記載されている。もっとも、通信秩序に影響を及ぼすような攻撃、または、インフラに対する重要な影響を及ぼす攻撃などについてどのように整理するかという点については、いまだ触れられていないということがいえる。

(4)スパムサイト(迷惑メール)／ボットネットの遮断／フィッシング対応

スパムメールとは、受信者の意向を無視して、無差別かつ大量に一括して送信される電子メールであって、迷惑メールとも言われている。スパムサイトの遮断というのは、スパムサイトを、何らかの形で、ネットワークからの接続ができないようにすることをいう。



世界的には、2008年11月に当時、世界のスパムの50－70％を占めていたと考えられるMcColoという米国におけるホスティングプロバイダが、そのバックボーンとしていたHurricane Electricなどから、遮断されたという事件[14]がある。

我が国においては、迷惑メールに対する法的な規制手段において、このような対応が準備されている。「特定電子メールの送信の適正化等に関する法律」11条は、「送信者情報を偽った電子メールの送信がされた場合」において「電子メールの送受信上の支障を防止するため電子メール通信役務の提供を拒むことについて正当な理由があると認められる場合」には、電子メール通信役務の提供を拒むことができるとしている。

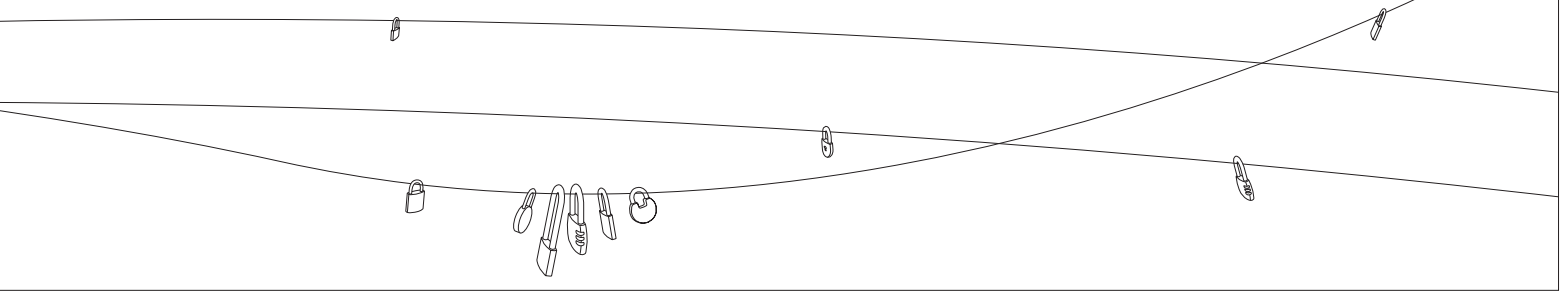
また、ボットネットを遮断するということも行われている。世界的には、マイクロソフト社が、裁判所の決定等を基にWaledac、Rustock、Citadelなどのボットネットを遮断した事件がある[15]。この事案においては、マイクロソフト社が、多大な労力をかけて、ボットネットの管理者を明らかにしようと努め、その上で、同社は(1)コンピュータ詐欺及び不正使用法(合衆国法典18巻1030条)(2) CAN-SPAM法(同15巻7704条)(3)ランハム法(同15巻1125条(a))に基づく商標侵害などを根拠に、差止などのエクイティ上の救済及び損害賠償を求め、シアトルのワシントン州西地区地方裁判所に訴訟を提起した。裁判所は、被告氏名不詳者が、操作し、ボットネットをコントロールをしていたIPアドレスとドメイン名を利用不能にする仮差止命令等を発令し、それを基に、そのようなボットネットが遮断されている。

フィッシングとは、実在する組織を騙(かた)って、ユーザーネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人の情報を詐取することをいう。一般的には、実在する組織と紛らわしいサイトを構築し、そのサイトに誘導する電子メールを送付し、それに引っかかって誘導したサイトにおいて、個人の情報を詐取する。フィッシングに対しては、ドメイン名の登録者が、フィッシングの誘導先のドメインを利用できなくするという活動もなされている(フィッシングサイトテイクダウン活動)。メールの名義を詐称された実在する組織は、具体的な誘導先のサイトを把握し、そのドメインを利用することができなくなるように、管理しているISPや一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)に対して、テイクダウンを依頼[16]する。この場合、テイクダウンを担当したISPやドメイン管理者が、その実際のドメインの利用者から、フィッシングではないと争われた際に法的な問題が起きることはあり得る。

これらの活動から、もはや従来の電気通信事業者のモデルが変更を余儀なくさせられており、安全・安心なインターネットの利用にインターネット媒介者が積極的に活動しているということが明らかになっている。

(5)行動ターゲティング広告と「通信の秘密」

(2)から(4)までが、情報セキュリティ目的のための「通信の秘密」の取得／利用／共有の問題であったが、別の目的のための「通信の秘密」の取得／利用／共有



の問題を提起しているのが、いわゆるDPI技術を用いた行動ターゲティング広告の問題である。DPI技術は、IPパケットの内容のデータ部分（ペイロード）の情報を基に、フィルタリングなどの処理方法を決める機能をいう。このような機能は、情報セキュリティ的な目的にも利用し得るし、帯域制限などに利用することも可能である。また、プロバイダのサービス向上にも利用することが可能である。もっとも、インターネットにおいてDPIが議論されるのは、これを広告宣伝目的に利用することができるのではないかという議論に関連してである。ISPは、このDPI技術を利用するときに、利用者のHTTP（Hypertext Transfer Protocol）リクエスト及びレスポンスに係る全てのパケットを解析して利用者の興味・嗜好を分析し、これにマッチした広告を利用者に配信することができ、この仕組みは、行動ターゲティング広告の一つとされている。「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第二次提言」は、このようなDPI技術を利用した広告目的での利用について詳細な分析を加えている（同54頁以降）[17]。分析によれば、かかる行為は、「通信の秘密」を侵害するものであり、それ自体で許容されるという正当性は考えられないこととされる。そして「利用者の同意が明確かつ個別のものである」場合に限って認められ、「同意に当たっての判断材料を提供するという意味で、利用者に対してサービスの仕組みや運用について透明性が確保されるべきである。よって、DPI技術を用いた行動ターゲティング広告については、各事業者は、透明性の確保に向けて運用に当たっての基準等を策定し、これを適用することが望ましい。」とされている（同58頁）。

(6)違法有害情報対応について

違法・有害情報というのは、違法な情報（権利侵害情報・その他の違法な情報）や有害情報（違法ではないが公序良俗に反する情報・青少年に有害な情報）を意味する。表現の自由が保護されるとはいえ、これらの違法・有害情報が自由に流通するような状況は、インターネットに負の側面を与えているというように考えられる。

具体的には、名誉棄損サイトの削除の問題、知的財産権侵害情報の削除の問題、青少年に有害な情報の問題、児童ポルノの問題、一般のポルノの問題などがある。

青少年インターネット環境整備法と閲覧防止措置、児童ポルノのブロッキングにおける具体的な「通信の秘密」との関係については、注2）の宍戸論文に譲る。また、その他の問題については、「インターネット上の違法な情報への対応に関するガイドライン」など[18]が参考になる。表現の自由や「通信の秘密」などへの配慮から、第三者機関が設立され、その判断を基にインターネット媒介者が積極的に活動をなすという枠組みがとられている。

3. 今後の通信の秘密の解釈について

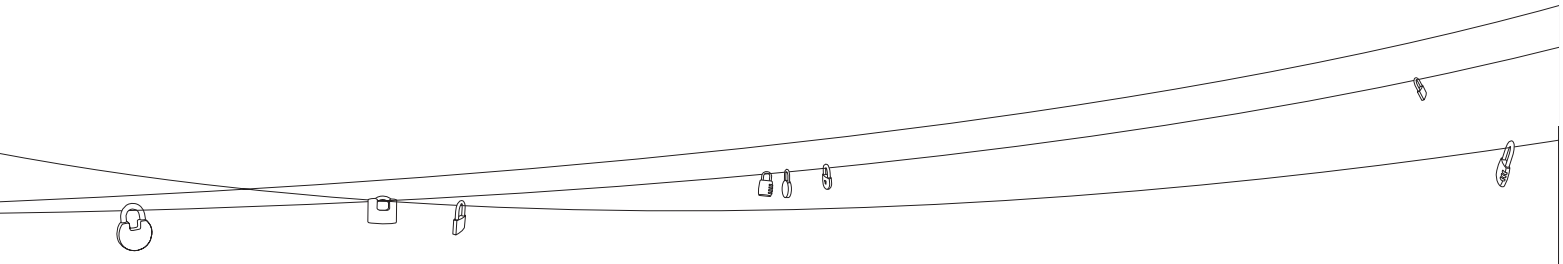
3.1　現状の問題点

現状のインターネットにおいて、インターネット媒介者が、極めて多様な活動をなしていること、とりわけ、安全・安心なインターネットの健全な利用のために、極めて多様な、そして、重大な役割を果たしていることを見てきた。そして、それらの具体的な活動の許容性の根拠、許容される活動について、「通信の秘密」の解釈が極めて大きな役割を果たしていることも明らかになった。しかしながら、本稿のような整理をするとき、現在の「通信の秘密」の解釈が、現代社会に十分に対応できるものとなっているのかが極めて疑わしいということがいえる。

具体的な問題点としては、(1) そもそも、インターネット媒介者において、安全・安心なインターネットの健全な利用のために行う行為が、違法であるという前提からスタートするために、かかる活動を行いたいと思っていても、インターネット媒介者がこれをなすと法規制の対象となるとされており、萎縮的効果があるのではないか、いわば、「通信の秘密」は肥大化していると評することができるのではないかということ (2) 諸外国においては、通信データと通信の内容についての区別に対応して保護の程度が異なっている場合があるが、通信データの取得・利用と「通信の秘密」との整理・国等の積極的な関与が、違法・有害情報対応という通信内容の取得・利用という問題と比較して、遅れているように思えること　(3) 上記のような活動が、いわば、敵視されてきた (それが、やっと認容されるに至った) という状況であるために、かかる活動にかかるコストを社会的に負担するという意識につながりにくくなっている。実際には、積極的に促進しなければならないのに、インターネット媒介者にとっては、コストのみがかかり、その活動に対するインセンティブ設計が十分に働いていないこと　(4)「通信の秘密」について、そのプライバシーの合理的な期待がどのようなレベルで保護されるべきかという議論がなされておらず、その上で、種々の活動とのトレードオフに注目がなされていないこと (その代表例が、DPI技術の広告利用問題であろう)、などが挙げられるであろう。

3.2　今後の解釈の方向性

インターネット媒介者が、通信の内容に関わる場合はともかくとして、通信データ部分に関わる場合をも、そもそも違法であると構成することが、実質的に[19]問題を生んでいるように思える。そもそも、歴史的には、「偶然目に触れ、または適法にこれを知得したるものは、これをもって秘密の侵害というを得ず。」[20]とされ、適法な伝達自体「通信の秘密」の侵害とは考えられていなかったのであり、上記でみた各種「通信の秘密」との関係の整理においてなされる「通信伝達時において必然的になされる通信データ取得自体も「通信の秘密」侵害をしているのにもかかわらず、正当業務行為で許される」という趣旨の解釈は、伝統的な枠を越えているとしか評し得ない。また、解釈論的には、(ア) 取得には、



「積極的に」(イ)利用には、「自己または他人の利益のために」というそれぞれ限定の文言が付されていたにもかかわらず、それらの限定の文言が無視されている状況である。プライバシーの期待に対してどれだけ制限を受けたかと通信当事者の感じる程度は、その処理者の処理目的によって影響を受けるものと考えられる。そうである以上、通信に関する利用者のプライバシーの合理的な期待の保護が、「通信の秘密」の保護の一つの要素であるのであるから、安全・安心にインターネットを健全に利用をしてもらう目的の下のインターネット媒介者の行為は、係る媒介者に求められる一定の行動規範を遵守(じゅんしゅ)している限り、「積極的な取得」ともいえない／「自己または他人の利益を図るため」とはいえないので、「通信の秘密」を「侵す」ということはいえないという方向性に解釈論が展開する必要があるものと考えられる。比較法的には、通信の内容と通信データの区別を前提に、そのプライバシーの保護に程度の違いを設けている法制も多数あるのであるから、そのような法制度の下で、どのような定めがなされているのか、実際に、媒介者の行動規範的な定めはなされているのか、その場合、どのような点に留意が図られているのか、プライバシー侵害に対する安全弁はないのか、などの論点をこのような解釈論を念頭において比較調査をなし、そのような調査を基に、上記の「通信の秘密」の解釈論の発展を期すことは我が国のインターネットの将来に極めて重要なことのように思われる。

Ikuo Takahashi
高橋 郁夫

BLT法律事務所所長・弁護士、株式会社ITリサーチ・アート代表取締役、宇都宮大学 大学院 工学部講師
情報セキュリティ／電子商取引の法律問題、特に、脆弱性情報の責任ある流通体制・ネットワークにおけるプライバシーとセキュリティのバランスなどを専門として研究する。法律と情報セキュリティに関する種々の報告書に関与し、多数の政府の委員会委員(総務省「次世代の情報セキュリティ政策に関する研究会」など)を務める。平成24年3月情報セキュリティ文化賞を受賞。

注

1) OECD "THE ECONOMIC AND SOCIAL ROLE OF INTERNET INTERMEDIARIES" 9頁、(http://www.oecd.org/dataoecd/49/4/44949023.pdf)

2) 宍戸常寿「通信の秘密について」(http://www.win-cls.sakura.ne.jp/pdf/35/02.pdf)は、プロバイダ責任制限法と通信履歴の保存、刑事訴訟法改正と通信履歴不消去の要求、青少年インターネット環境整備法と閲覧防止措置、児童ポルノのブロッキングについて論じる。

3)「ユーザー、コンテンツ、サイト、プラットフォーム、アプリケーション、接続している装置、通信モードによって差別あるいは区別することなく、インターネットサービスプロバイダや政府がインターネット上の全てのデータを平等に扱うべきだとする考え方」を根拠にしているということがいえるであろう。このような考え方を維持すべきかどうかという点について、米国においてはネットワーク中立性という概念の下、議論がなされている。

4) 通信の内容と通信データの区別については、高橋郁夫「『通信の秘密』の比較法的研究・序説」(総務省「次世代の情報セキュリティ政策に関する委員会」の第8回配布資料(http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/next_generation/080523_2.html))を参照。また、かかる解釈論の根拠については、高橋郁夫・吉田一雄(平成18年)「『通信の秘密』の数奇な運命

注

（憲法）」情報ネットワーク・ローレビュー（第5巻）（情報ネットワーク法学会、商事法務）44頁以下、高橋郁夫ほか（平成21年）「『通信の秘密』の数奇な運命（制定法）」情報ネットワーク・ローレビュー（第8巻）（同）、1頁以下を参照のこと。

5）総務省「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律－逐条解説－」平成14年5月（http://www.soumu.go.jp/main_sosiki/joho_tsusin/chikujyokaisetu.pdf）

6）もっとも、その後、「プロバイダ責任制限法発信者情報開示関係ガイドライン」（初版 平成19年2月）（http://www.telesa.or.jp/consortium/provider/pdf/provider_hguideline_20110921_1.pdf）によって、裁判外でも開示される準備がなされた。

7）「サイバークリーンセンターは、インターネットにおける脅威となっているボット（略）の特徴を解析するとともに、ユーザのコンピュータからボットを駆除するために必要な情報をユーザに提供する活動を行っています。また、ISP（略）の協力によって、ボットに感染しているユーザに対し、ボットの駆除や再感染防止を促すプロジェクトの中核を担っています」（https://www.ccc.go.jp/ccc/index.html）

8）http://iia.net.au/userfiles/iiacybersecuritycode_implementation_dec2010.pdf

9）阿部義徳・田中英彦「C&C セッション分類によるボットネットの検出手法の一検討」電子情報通信学会・情報処理学会 , FIT2007（http://lab.iisec.ac.jp/~tanaka_lab/publications/pdf/taikai/taikai-07-02.pdf）

10）サイバークリーンセンター運営委員会「ボット対策事業運用ポリシー」（https://www.ccc.go.jp/ccc/pdf/ccc_policy.pdf）

11）情報処理推進機構「サービス妨害攻撃の対策等調査　-報告書-」（以下IPA報告書という）http://www.ipa.go.jp/files/000014123.pdf

12）国家サイバー危機総合対策（2009年8月）、コントロールタワーの整備、感染パソコンサイバー駆除体系、DDOSサイバー待避所などの政策が採用されている。

13）初版 2007年5月30日（非公開）、第2版 2011年3月25日公開（http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf）

14）この部分については、HostExploit.com“McColo-Cyber Crime USA”（http://fserror.com/pdf/McColo.pdf）による。

15）一連の事件については、「マイクロソフト、ボットネット対抗でAzureを使ったグローバル情報網を整備へ」https://securityinsight.jp/report/368-20130612microsoftにまとめられている。

16）具体的な内容については、フィッシング対策協議会「フィッシング対策ガイドライン」（http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf）22頁。

17）「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第二次提言」（http://www.soumu.go.jp/main_content/000067551.pdf）

18）http://www.telesa.or.jp/consortium/illegal_info/pdf/20100907guideline.pdf

19）法律理論的には、違法性阻却事由があるとして違法ではないとされようが、通信の秘密を侵していないから、違法にはならないということは、同様だということがいえるとしても、インターネット媒介者（特にISP）の活動に及ぼす影響としては、極めて実質的な違いがあると考えるべきであるというのが筆者の意見である。

20）もともとは、『電信法要義』（明治33年）155頁の立場であり、その後、金光昭・吉田修三『公衆電気通信法解説』（日信出版、昭和28年）も、かかる解釈を踏襲している。

インターネット時代における
通信の秘密2

通信の秘密の憲法解釈論

京都大学 大学院 法学研究科 教授
曽我部 真裕 Masahiro Sogabe

本稿は、従来の学説と近年の批判論を踏まえ、通信の秘密条項（憲法21条2項）の解釈論を試みる。
従来の解釈論は通信事業が国営であることを前提としたものであるが、
民営化・自由化後の今日では、民間事業者に憲法の拘束は及ばず、
民間事業者の義務は憲法の趣旨等を踏まえた法律によって創設されたものと位置づけられる。
他方、国家に対する憲法的な要請としては、通信の秘密を侵害しないという不作為義務が中心であり、
近時主張されている通信制度の設営義務といった
広汎な作為義務を憲法から引き出すことには慎重であるべきである。

キーワード
通信の秘密　通信の自由　表現の自由　国家の通信制度設営義務　憲法

1. はじめに

本稿では、日本国憲法[1)]21条2項後段の規定（「通信の秘密は、これを侵してはならない。」 以下「通信の秘密条項」と言う。）の解釈論を試みる。

どの憲法の教科書を見ても、通信の秘密条項に関する解説は掲載されている。しかし多くの場合、その内容は通り一遍のものにすぎない。また、1946年の憲法制定以来、通信をめぐる状況は劇的に変化したにもかかわらず、最新の文献であってもそれを踏まえた記述には必ずしもなっていない。そもそも、教科書だけではなく研究論文レベルでも、憲法学における通信の秘密をめぐる業績は散発的にみられる程度で、蓄積は必ずしも十分ではなく、地味な論点にとどまってきた。

しかし、従来の解釈では現在の情報通信ネットワークに関わる問題に対処できないとして、近年、情報通信政策関係者や情報通信法の実務に携わる弁護士等から、通信の秘密条項あるいはそれを受けた法令の解釈の再考が主張されてきており、これらの中には、本格的な憲法解釈に立ち入るようなものも現れてきている。

しかし、こうした動きに対する専門の憲法研究者の反応は一部を除いては鈍いと言わざるを得ない[2)]。こうした状況を踏まえ、本稿では、最近の通信の秘密条項

に関する解釈論を参照しつつ、検討を行うこととする。

2. 従来の議論の確認

(1) 通信の秘密の保護法益は、主としてプライバシーであること

まず、通信の秘密条項に関する従来の通説的な解釈を確認しておきたい。

通信の秘密の保護法益については、主としてプライバシーであるとされる。しかし、それ以上の点については見解が分かれている。まず憲法の教科書の中には、通信の秘密条項を含む21条は、全体としては主として表現の自由に関わる規定であるにもかかわらず、通信の秘密に関しては表現の自由とは別に、住居の不可侵（35条）と並べてプライバシー関連の項目で解説するものがある[3]。

次に、通信の秘密と表現の自由との関係については、論者によって立場は異なる。そもそも、諸外国の憲法では、通信の秘密と表現の自由とは別個の条文で規定されることが一般的であり、明治憲法でも同様であった[4]。そこでは、通信の秘密の保護法益はプライバシーであることは比較的明瞭である[5]。

他方、同じ条文で両者を規定する日本国憲法は例外的であるとされており、その趣旨をどのように説明するかが問題となる。この点、通説的見解は両者を「同居」させていることの意味をも重視し、通信の秘密条項はプライバシー保護の一環としての性格を有するが、同時に表現の自由との密接な関わり合いもあるとする[6]。しかし、一方では、本項冒頭に挙げた教科書のように両者が「同居」していることにあまり拘泥せずに諸外国の憲法と同様、プライバシー保護の文脈に純化して解釈をする立場[7]があり、他方では「通信は表現の自由の保障の一環として位置づけられている、と端的に理解すべきである。」[8]とする見解もみられる。

この点については、本特集にも寄稿されている高橋郁夫弁護士からの問題提起がある。これについては後に触れるが、まずは日本国憲法の通信の秘密条項の位置が議論を招いている原因であることを確認しておく。

(2) 通信の秘密と通信の自由との関係については曖昧であること

通信の秘密条項の明文で保障されているのは「通信の秘密」だけであるが、この条項は通信の自由の保障も含まれるとする見解もある。この見解の理由づけには複数の筋があり、前項で述べたように通信を表現の自由の一環であるとすれば、通信の自由は表現の自由の一部として保障されることになる[9]が、通信と表現を区別するという前提をとったとしても、通信の秘密は通信の自由を論理的前提とする、という説明が可能である[10]。

しかし、通信の自由は通信の秘密の論理的前提ないし反射であるという曖昧（あいまい）な説明をする論者も少なくない[11]。通信の秘密の論理的前提であれば通信の自由も憲法上の基本権として保障されるという趣旨であると理解される。しかし、反射であるというのは、通信の秘密が憲法上保障されている結果として事実上通信の自由が保護されているという意味であって、通信の自由は基本権ではないということである。

この点については、憲法制定時には通信（郵便、電信電話）は国営事業であったことに留意すべきかもしれない[12]。通信は国家による給付（サービス）であったのであり、そのサービスを利用する権利があった[13]としても、それは基本権としての自由権ではなく、サービスの受給権である。さらに、明治憲法下では通信の秘密（当時は「信書の秘密」）について、「各人は国家を信頼して通信を委託するものなるが故に国家は其の信頼に背くを得ざるを当然と為す」[14]という説明がさ

れていたが、これも、通信の自由を権利として認めるというような理解に基づくものではなさそうである。

したがって、通信の秘密は通信の自由を当然に含むというような端的な理解が通説化していないことには、一定の理由があると思われる。

しかし、当然ながら今日では通信は民営化されており、前提が全く変わっている。また、例えば、外国で導入されている著作権侵害を反復した場合にインターネット接続契約を解除するような規制をも想定すると、通信の自由を基本権として認める必要性も高まっている[15]。この点についても後に触れる。

(3) 憲法上の通信の秘密と法律上のそれの関係については曖昧であること

周知のように通信の秘密は、憲法の通信の秘密条項に加えて、様々な法律でも罰則つきで保障されている（電気通信事業法4条、179条、有線電気通信法9条、14条、電波法59条、109条、郵便法8条〔信書の秘密〕、民間事業者による信書の送達に関する法律5条、44条〔同〕など）。

憲法の通信の秘密条項とこれらの法律規定との関係については、後者は前者の趣旨を具体化するものであるというのが従来の一般的説明であり、それ以上に立ち入った説明はあまりみられなかった。特に、法律上の通信の秘密の規定は、単に国会が憲法の規定の趣旨を自発的に立法政策として定めたに過ぎないものか、それとも、憲法は国会に対してこうした立法を多少とも要請しているのか、という点については曖昧であった[16]。

このような曖昧さの理由としては、通信が自由化された後も、国営化時代の議論の見直しが行われなかったことが考えられる[17]。国営事業であれば、憲法の拘束を受けるのであり、法律上の通信の秘密の保障は、憲法の通信の秘密条項の確認に加えて罰則という具体的な保障を与えるという意義をもった。

現在においては、民間事業者の通信の秘密不可侵義務を法律上定めること、あるいはより一般的に、通信制度を法律で定めるに際して、憲法の通信の秘密条項から国家に義務づけられる事柄があるのかどうか、ということが問題になると思われる。最近の議論はこの点についても論じている。

(4) 通信の秘密の範囲については、通信内容に加えて外形的事項も含まれること

最後に、従来の議論においては、通信の秘密に言う「通信」とは、通信内容に加えて、通信の当事者の身元、日時、発受場所などの外形的事項（本特集の高橋論文では「通信データ」という表現であり、また、最近では「メタデータ」と呼ばれる場合もある。）も含まれるとされる。従来、こうした理解は、憲法上の通信の秘密条項と法律上の通信の秘密に関する規定とを通じて、ほぼ確立したものであった[18]。さらに言えば、明治憲法の「信書の秘密」条項下においても同様の解釈がなされており[19]、現行憲法の解釈はそれを引き継いだものであろう。

しかし、本特集の他の論考でも論じられている通り、こうした解釈は今日、情報通信政策の関係者や実務家から強く批判されており、通信の秘密に関する実際上もっとも重要な論点となっている。そこで、この論点については今後議論を深める必要があるが、本稿の目的は今後の法律解釈や立法論の前提となる憲法解釈を示すことであるため、本稿では通信の秘密の範囲に関する法律解釈の検討には立ち入らないこととする。

3. 最近の批判論の検討

(1) はじめに

ここまでは従来の憲法解釈論の特徴を整理してきた

が、こうした憲法解釈やそれを前提とした法律解釈は、上述のように、近年、インターネット時代に適合しないとして強く批判されるようになってきている。その具体的な諸相は、本特集の他の論考に譲り、ここでは、これらの批判論のうち、憲法解釈に関わる点について検討を行う。

(2) 通信の秘密条項の趣旨の再考

高橋郁夫と吉田一雄は、憲法制定時の通信の秘密条項成立史の詳細な調査を踏まえて、通信の秘密条項は「意思伝達におけるプライバシー権」を保障する趣旨であるとし、それを踏まえた解釈論を展開する[20]。

高橋らの論旨は以下のようなものである。すなわち、まず、21条2項の「通信の秘密」に該当する英文は、GHQで作成された草案以来、secrecy of any means of communicationというものであって、日本語訳もある段階までは「通信手段の秘密」というものであったが、途中で「通信の秘密」に修正された。

憲法制定過程を通じて、通信の秘密条項(に結実する規定)の具体的な解釈を示す資料は見当たらなかったが、高橋らは、GHQの起草者は「意思伝達におけるプライバシー権」を保障するアメリカのコモンローを参照したものとして、secrecy of any means of communicationは「意思伝達の機密性」と訳すべきものであったとする。

「意思伝達におけるプライバシー権」とは、「コモンローは、各個人に対して、通常、自己の思想や感情をどの範囲で他人に表示すべきか決定する権利を保障している。」という意味での「自己の思想や感情をどの範囲で他人に表示すべきかを決定する権利」であるとされる。

以上を踏まえて高橋らは、通信の秘密条項について以下のような解釈論的帰結を引き出す[21]。

① 憲法のいう「通信」は、隔地者間での連絡に限らない。
② 通信の秘密の保障は、通信の内容の保護を意味する(通信の外形的事項の保護は含まない)。
③ 意思伝達後も、発意者が、公表を禁じた内容については、発意者は、内容を探索されることはなく、また、公表を強制されることはない。
④ ただし、その発意者の公表を禁じたといえるかどうかは、社会的にその期待が合理的といえるかどうかにかかる。

この見解は、通信の秘密条項が表現の自由を保障する21条におかれていることを重視し、通信の秘密を表現の自由の一部として位置づけるものである。上述のようにこうした見解は従来も存在していた[22]が、高橋らの議論はこうした解釈を憲法制定過程の丹念な検証によって裏づけた点で重要である。

ただし、高橋らの見解について、疑問がないわけではない[23]。まず、高橋ら自身も指摘する通り、制定過程においては通信の秘密条項(に結実する規定)の具体的な解釈論は行われていなかったのであり、高橋らの主張する解釈論は、GHQの担当者らの知的背景という間接的な証拠に基づくものである。もう一方の起草者ともいうべき日本政府での作業では、secrecy of any means of communicationを初めは「通信手段の秘密」と訳していたが、後に「通信の秘密」と修正している。その際にはおそらく、明治憲法、さらにはそれに影響を与えたヨーロッパの憲法の定める「信書の秘密」が念頭にあったものと思われる。

次に、通信の秘密条項について高橋らの主張するような解釈論をとるとしても、最大の関心事項である通信の秘密の範囲について、通信内容の秘密に限られるという解釈は論理必然ではないと思われる。高橋らはウォーレンとブランダイスの見解に依拠してこのような解釈を行っているが、理屈としては、通信の外形的

事項が知られることによって意思伝達におけるプライバシーが害される場合もあることを理由に外形的事項も保護されるという考え方もありうる[24]。

(3) 通信の秘密条項が国家に要請する内容の再構成論

次に、通信の秘密条項が国家に要請する内容の再構成を図るのが海野敦史である。従来の議論では、通信の秘密条項は、まずは通信の秘密を国家(公権力)が侵害しないという不作為を求めるものと理解されていた。そして、それ以上に、国家が法律によって民間事業者による通信の秘密侵害を禁止することも憲法上要請されるかということについては曖昧であった。

これに対して海野は、インターネット等による通信が一般化し、それに伴って通信管理主体が多様化している今日においては、もっぱら公権力に対する不作為を求めるのみでは、「不可侵」の趣旨が充足されないとする。そこで、通信の秘密条項は、通信の秘密が容易に侵されることとなる制度的環境を形成又は放置してはならないという公権力に対する義務を含意しており、上記のような公権力による通信の秘密侵害の禁止はその前提となると理解すべきであるとする。さらに、こうした公権力に課される義務に対応して、国民各人においては、「通信の秘密を侵されない権利」が認められるとする[25]。

さらに海野は、上述の「通信の秘密が容易に侵されることとなる制度的環境を形成又は放置してはならないという公権力に対する義務」の存在、および各人の「通信の秘密を侵されない権利」の実効的保障の必要から、憲法適合的な通信制度が立法によって具体化される必要があるとする[26]。

海野の議論は大変周到かつ詳細であり、かなりの説得力をもっているものと思われる。実際、憲法研究者の中にも、通信の秘密条項は、通信の自由や秘密に対応する民間事業者の責務を法令上具体化するように求めているとしたり[27]、通信の秘密条項は、通信制度を、公的にか私的に(民間企業として)かは別にして、維持する責務を負わせた規定と読むべきであるとする見解もある[28]。これらの見解からは、電気通信事業法を始めとする通信関係の法律の少なくとも基本的な部分は、単に立法政策として制定されたものと理解されるべきではなく、憲法上の要請に基づくものと理解されることになる。

海野の見解は、こうした議論を現代の状況に合わせつつ精緻(せいち)化したものといえ、その限りでは特異なものでもない。しかし、ここでは、敢えて若干の疑問を指摘しておきたい。

海野は、通信の秘密条項から広汎な国家の作為義務を導き出すものであるが、その理由については次のように捉えているようである。すなわち、通信を行うためには当然ながら通信制度、すなわち、国民が安全・安心に通信サービスを利用することを可能とする基盤となる通信に関する制度・システムが必要であるが、こうした制度が確立されていない限り、国民は通信の秘密等が侵害される危険性と隣り合わせとなり、通信の秘密を侵されない権利が実効的に保障されない。そこで、このような通信制度の保障ないし安定的設営は、憲法上の要請とされる[29]。

確かに、通信制度の安定的設営が国民生活に不可欠であり、それゆえに重要な政策課題でありうることは一般論としては異論の余地はないだろう。しかし、だからといってそれが直ちに憲法上の具体的な要請となるわけではない。このことは、電気やガス、水道は通信と同様、国民生活に不可欠なライフラインであるが、これらに関する制度の設営が国家の具体的な憲法上の義務とはされていないことと同様であろう[30]。

また、自由権であっても実効的な行使のためには関係の制度を法律によって整備することが必要な場合がある。放送の自由(21条1項)における放送法、結社の

自由（同）における一般社団法人法、営業の自由（22条1項）における独占禁止法などは、それぞれ意味合いが異なるが、こうした例であろう。しかし、これらの自由権の根拠規定が公権力に対して制度設営の作為義務を課しているという議論は憲法学説上、少なくとも一般的ではないと思われる。

他方、表現の自由（21条1項）について、単に自由権を保障するだけではなく、その客観的側面として情報の多元性・多様性を保障する義務が公権力に課せられているとする見解があるのは確かであり、筆者としてはこうした見解に与したいところではあるが、これも通説となるには至っていないし、作為義務を認める見解であってもその内容は独占の排除などであって、それほどには広汎ではない。

要するに、日本の憲法学は一般に、自由権の規定から国家の作為義務を導くことには慎重であったように思われる。こうした傾向を踏まえれば、通信の秘密条項から広汎な国家の作為義務を導き出すのではなく、当面、通信の秘密条項はあくまでも基本的には国家の不作為義務を定めたものと理解した上で、通信制度を構成する各種法律や、民間事業者の通信の秘密不可侵の義務は、憲法の趣旨や通信というものの当然の性質[31]を踏まえつつ国会が各種事情を考慮して定めた立法政策に基づくものと位置づけておくのが妥当ではないかと思われる[32]。

なお、通信制度設営に関する広汎な国家の作為義務を認めることについては、自主規制や共同規制との関係をどう考えるかという問題点もありうる。通信をめぐる今日の複雑化した環境においては、民間事業者の自主的な規律の重要性が増しているが、共同規制のような法的な枠組みを構築した上であれば別として、このような枠組みをとることなく不透明な形で民間事業者に委ねることが作為義務の不履行と評価される可能性についても考慮が必要かと思われる[33]。

4. 通信の秘密条項の解釈

最後に、以上の検討を踏まえ、また、今日の状況をも考慮しつつ、本稿での憲法の通信の秘密条項の解釈をもう少し敷衍（ふえん）しておきたい。その際、従来の議論のうちそれほど問題がないと思われるものについては継続性を重視しつつ、再考を要する点については現段階での試論を提示する。

まず、通信の秘密条項の保護法益については、比較憲法や明治憲法の「信書の秘密」以来の解釈を踏まえると、従来の通説に従い、表現との関連性は認めつつも、主として通信におけるプライバシーであると考える。今日の憲法解釈においては一般的なプライバシー権が13条で保障されるとされているが、通信の秘密条項はその特別規定として、より定型的かつその意味で手厚い保護を行うものである。

その前提として、通信を表現の一部と見ることはせず、両者は憲法上区別されると解する。ただし、憲法上の通信と表現との区別は、法律上の両者の区別とは異なるので、ホームページでの表現のように、法律上は電気通信事業法が適用されるものであっても、憲法的評価としては表現にあたる場合がありうる。

これに対して、通信の秘密条項を表現と切断すると、匿名表現の自由が保障されなくなるのではないかという批判がありうる。しかし、匿名表現の自由はそれ自体表現の自由として21条1項で保障されると考えることができる[34]。また、通信の秘密条項は隔地者間の通信に適用されるものであり、対面の会話の秘密は、13条で保障される一般のプライバシー権によって保障されると考える。

次に、通信の自由についてであるが、先述のように、通信事業が国営の時代にあっては、憲法の基本権として通信の自由を観念する余地は乏しかった可能性があ

る[35]。しかし、通信事業が自由化された後は、民間の通信サービス利用を公権力に妨げられないという意味での通信の自由は重要な基本権として保障されるべきである。その根拠条文としては、「新しい人権」の一般的根拠であるとされている13条とするか、あるいは、その関係の密接さを強調して、通信の秘密条項に改めて位置づけるということも考えられる[36]。

第3に、通信の秘密が保障される「通信」の範囲について、確かに保障の核心は通信内容の秘密であるといえるだろうが、外形的事項からそれが推測できる場合がある以上、外形的事項についても「通信」の範囲に含まれると考えるべきだろう。ただし、通信の秘密といっても絶対的な保障ではなく法律による制約が許される場合があることはもちろんであり、その合憲性を考える際には通信内容と外形的事項とを区別して考える余地はあると思われる。

第4に、通信の秘密条項の名宛人は、公権力（国家、地方公共団体）及びそれと同視できる存在である。旧電電公社は後者（「それと同視できる存在」）に該当したが、現在の日本電信電話株式会社（NTT）はそれには該当せず、憲法の通信の秘密条項に拘束されることはないと考えられる。いわば純粋の民間事業者はなおのこと通信の秘密条項には拘束されないが、ただ、例えば仮に児童ポルノブロッキングが法律上インターネット・サービス・プロバイダ（ISP）に義務づけられたような場合のように、法律上通信の秘密を侵害するような行為を義務づけられる場合には、その限りでISPは公権力と同視されることになる[37]。

第5に、通信の秘密条項は公権力に対して不作為を求めるものであって、通信制度の設営といった作為を求めるものではないと考える。その結果、憲法の通信の秘密条項と各種法律の通信の秘密条項との関係は切断され、法律の条項は憲法の要請を確認したものというよりは、憲法の趣旨や通信というものの当然の性質を踏まえた立法政策に基づくものとなる。したがって、法律の内容あるいは解釈については必ずしも憲法の通信の秘密条項に準じたものである必要はなく、具体的なサービスのあり方に応じて一定程度柔軟な制度設計が可能であると解される。もちろん、どのような制度設計も可能というわけではなく、通信におけるプライバシー（通信の秘密）や通信の自由と、対抗利益（通信事業者の営業の自由や財産権、ネットワークの安定的運用による利用者一般の利益、第三者の権利利益など）との調整の範囲内でなければならない[38]。

実は、こうした調整は、現行の例えば電気通信事業法4条・179条の下でも実質的には行われている。現在、本特集の高橋論文や石井論文でも紹介されている迷惑メール対策やブロッキング等の正当な目的のために通信の秘密を侵害せざるを得ない場合には、正当業務行為（刑法35条）や緊急避難（同36条）の法理を用いて違法性が阻却されるという判断を行っている。しかし特に緊急避難構成については、恒常的な枠組みをこのような緊急の法理で説明しようとする点でやや違和感があり、実質的な利益衡量を緊急避難という形式を借りて正当化しているという側面がある。

このようなやり方は現行法を前提とすればやむを得ない側面もあるが、高橋論文[39]が指摘する通り、通信事業者にとっては分かりにくく、萎縮効果を生む懸念もあるかもしれない。本稿では、法律レベルでは柔軟な制度設計が可能であることを指摘したが、このことは逆に言えば、現在、通信の秘密との関係が問題になっている各種の措置については、法律でもう少しきめ細かく定めることが筋であるということを示唆している。

Masahiro Sogabe
曽我部 真裕

京都大学 大学院 法学研究科 教授
1974年生まれ。京都大学法学部、同法学研究科修士課程修了、同博士課程中退。司法修習生、京都大学大学院法学研究科准教授などを経て2013年より現職。BPO（放送倫理・番組向上機構）放送人権委員会委員、EMA（モバイルコンテンツ審査・運用監視機構）諮問委員会委員など。専門は憲法、情報法。主著に『反論権と表現の自由』（有斐閣、2013年）、『憲法論点教室』（共編、日本評論社、2012年）など。

注

1）以下、憲法の条文については、単に「○条」とのみ表記する。

2）憲法研究者の反応として、宍戸常寿「通信の秘密について」企業と法創造9巻2号（2013年）14頁以下。

3）佐藤幸治『日本国憲法論』（成文堂、2011年）320頁、初宿正典『憲法2（第3版）』（成文堂、2010年）365頁、松井茂記『日本国憲法（第3版）』（有斐閣、2007年）513頁、大石眞『憲法講義Ⅱ（第2版）』（有斐閣、2012年）126頁。

4）通信の秘密の比較憲法史的については芦部信喜（編）『憲法Ⅱ』（有斐閣、1978年）637頁以下［佐藤幸治］、齋藤雅俊「憲法21条の『通信の秘密』について」東海法科大学院論集3号（2012年）113頁以下など参照。

5）ただし、明治憲法がモデルとした1831年ベルギー憲法や1850年プロイセン憲法においては、信書の秘密の規定は言論等の自由や請願権の規定と並んで配置されていたため、信書の秘密はむしろコミュニケーションの自由に関わるものとして把握されていたという指摘もある。他方、明治憲法はこれらと異なり、信書の秘密規定を住居の不可侵の規定の次に置いたため、（当時はこうした概念はないが）プライバシーに係るものとしての位置づけが明瞭である（以上、齋藤・前掲注（4）119-120頁）。

6）佐藤・前掲注（3）321頁、芦部信喜『憲法学Ⅲ（増補版）』（有斐閣、2000年）541頁、棟居快行「通信の秘密」法学教室212号（1998年）44頁。

7）大石・前掲注（3）126頁。

8）阪本昌成『憲法理論Ⅲ』（成文堂、1995年）140頁。なお、通信の秘密に関する阪本の見解についてより詳細には、阪本昌成「『通信の自由・通信の秘密』への新たな視点」同『プライヴァシー権論』（1986年、日本評論社）229頁以下参照。

9）阪本・前掲注（8）（『憲法理論Ⅲ』）140頁、高橋和之『立憲主義と日本国憲法（第3版）』（有斐閣、2013年）236頁、園部敏・植村栄治『交通法・通信法（新版）』（有斐閣、1984年）207頁。

10）赤坂正浩『憲法講義（人権）』（信山社、2011年）80頁、佐藤・前掲注（3）321頁。

注

11)芦部・前掲注(6) 541頁、初宿・前掲注(3) 367頁。なお、通信の秘密に関する憲法論について重要な貢献を行ってきた佐藤幸治は、かつては本文のような曖昧な見解をとってきた(芦部(編)・前掲注(4) 636頁[佐藤幸治]、佐藤幸治『憲法(第3版)』(青林書院、1995年) 577頁)ところ、最近の体系書では通信の自由の憲法的保障を認める立場に転じたこと(佐藤・前掲注(3) 321頁)が注目される。

12)この点に限らず、通信の秘密条項の解釈は、電気通信事業・郵便事業の民営化、自由化以前の状態に確立し、それが基本的には現在も引き継がれている(宍戸・前掲注(2) 16頁、齋藤・前掲注(4) 116頁)。

13)田中二郎『新版行政法(下Ⅱ)(全訂第二版)』(弘文堂、1974年) 352頁。

14)美濃部達吉『憲法撮要(改訂第5版)』(有斐閣、1932年) 171-172頁(原文のカタカナはひらがなに改めた〔以下同様〕)。

15)なお、フランスの違憲審査機関である憲法院は、インターネットへのアクセスの自由を基本権として承認し、裁判所が関与せずに行政機関が著作権侵害への制裁としてネットへの接続契約を解除させることは違憲であると判断した(2009年6月10日判決〔Décision n° 2009-580 DC〕)。

16)明確に前者の立場に立つものとして、松井・前掲注(3) 516頁、後者として阪本・前掲注(8)(『憲法理論Ⅲ』) 141、143頁。

17)関連して、憲法の通信の秘密条項に拘束される主体の範囲についても曖昧なところがあった。特に、NTTなど旧公社については、民営化後も憲法に拘束されることが当然視されてきた(芦部・前掲注(6) 545頁など)が、その根拠は自明ではないと思われる(阪本・前掲注(8)(『憲法理論Ⅲ』) 143頁)。

18)この点の詳細について参照、高橋郁夫ほか「通信の秘密の数奇な運命(制定法)」情報ネットワークローレビュー8号(2009年) 1頁以下。また、最近の憲法学者の主張として例外的にこの点に疑問を呈するものとして、高橋・前掲注(9) 224頁。

19)美濃部・前掲注(14) 171頁。

20)高橋郁夫・吉田一雄「『通信の秘密』の数奇な運命(憲法)」情報ネットワークローレビュー5号(2006年) 44頁以下。

21)高橋・吉田・前掲注(20) 67頁。

22)阪本・前掲注(8)(『憲法理論Ⅲ』) 140頁。

23)宍戸・前掲注(2) 25頁も参照。

24)実際、表現の自由の文脈で通信の秘密条項を理解する阪本昌成も、通信内容のみならず外形的事項についても秘密が保障されるとする(阪本・前掲注(8)(『憲法理論Ⅲ』) 142頁)。

25)海野敦史「憲法上の通信の秘密に対する『侵害』の射程」公益事業研究64巻1号(2012年) 2頁。

26)海野・前掲注(25) 2-3頁。

27)阪本・前掲注(8)(『憲法理論Ⅲ』) 141頁。

28)高橋・前掲注(9) 224頁、齋藤・前掲注(4) 131頁(「経営主体の公私を問わず、あまねく公平に提供され、かつ、秘密が保障された基本的通信手段の確保のための制度の整備を、憲法は国に求めている」)。

29)海野敦史「通信管理主体の通信関連設備に関わる財産権の現代的射程」公益事業研究63巻1号(2011年) 24頁注6。

30)なお、郵便に関し、また異なる意味合いで「制度」を語るものとして、石川健治「ラオコオンと

注

トロヤの木馬」論座145号（2007年）67頁以下。

31）齋藤・前掲注（4）127頁、宇賀克也・長谷部恭男（編）『情報法』（有斐閣、2012年）68頁［長谷部恭男］。

32）この点に関連していわゆるコモン・キャリア論の位置づけが問題となるが、これを憲法上の国家の義務と関連させて理解したとしても、その射程はごく基礎的なサービスに限られ、インターネットも含む広汎な領域における国家の作為義務には結びつかないと思われる。

33）なお、筆者は、世界的なネット企業による国家横断的な「支配」という事態がさらに進行した場合には別の議論の可能性も考えられることを示唆したことがある（拙稿「自由権――情報社会におけるその変容」法学セミナー688号（2012年）12頁以下）。このことは、インターネットの国際的なガバナンス体制が「暴走」して国民の通信の自由や秘密が脅威にさらされるようになった場合なども同様であろうが、しかし、これらは本文での当面の議論とは別次元のものである。

34）宍戸・前掲注（2）26頁。

35）ただし、国営事業であったとしても、給付請求権を自由権的に再構成するパブリック・フォーラム論と同様の構成で、通信の「自由」を語りうる可能性も理論的にはありうる。

36）後者の場合、結果的に前述の「論理的前提」論と一致することになる。

37）より正確には、民間事業者の行為であるということを理由に当該法律が憲法の拘束を免れることはできない、と言うべきだろうか。

38）この点では、本文の議論と海野の議論（例えば、海野敦史「『通信の自由』の現代的意義」社会情報学研究15巻2号（2011年）77頁とはそれほどの違いはないと思われる。

39）高橋・本誌11頁。

インターネット時代における
通信の秘密3

国家安全と通信の秘密

筑波大学 図書館情報メディア系 准教授

石井 夏生利 Kaori Ishii

2013年6月、PRISM問題が発覚し、世界的な注目を集めた。
その根拠規定とされている1978年外国諜報監視法の2008年改正法は、最長1年間、
国外に居る「合衆国人」以外の者を標的とする外国諜報情報の取得を認めている。
日本でも、政府機関に対する標的型攻撃等を受け、情報保全体制を強化する方針が打ち出されているが、
通信の秘密の保護との関係が問題となる。
国家安全の大義名分の下で、事実上無制限の侵害行為が容認されることのないよう、
保護すべき情報の範囲、技術的な制限手段の在り方を含め、
解釈の再構成や立法措置を含めた適切な運用ルールの制定に向けた全体的な合意形成が求められる。

キーワード
PRISM　外国諜報監視法（FISA）　通信の秘密　秘密保全　違法性阻却事由

1. PRISM問題の発覚

2013年6月6日、米国ワシントン・ポスト紙は、国家安全保障局（NSA）によるPRISM計画を報道し、世界的な注目を集めた。これは、テロ対策の名目の下、マイクロソフト、ヤフー、グーグル、フェイスブック、アップルを含む9社から、国外の標的が利用する電子メール、チャット（動画、音声）、ビデオ、写真、蓄積データ、VoIP、ファイル交換、ビデオ会議、ログインなど標的の活動に関する通知、ソーシャルネットワーキングの詳細などをNSAと連邦捜査局（FBI）が収集するという計画である。PRISMの仕組みは必ずしも明らかではないが、NSAやFBIが各社のサーバーに直接アクセスする方法で収集したと報じるものもあれば、これらの機関から電子的に送信されたと報じるものもある。

ワシントン・ポスト紙によると、この計画は、2007年9月11日にマイクロソフトが参加したことに始まり、2012年10月までの間には上記各社が参加を済ませた。2013年4月5日時点において、PRISMの標的は11万7,675件存在していた[1)]。

上記各社のうち、グーグルやアップルはPRISMへの関与を否定し、フェイスブックは、要請を慎重に調査し、法の義務の範囲内で情報を提供するとの声明を明らかにしたが、2013年6月8日、国家情報長官のジェームズ・R・クラッパー氏は、PRISMに関する概要報告書を公表した。報告書は、PRISMは秘密のデータ収集またはデータマイニング計画ではなく、「裁判所の監視の下、電子通信サービスプロバイダから、政府が法律上認められた外国諜報情報の収集を容易にするために利用される政府内部のコンピューターシステム」であると記載している[2)]。また、同報告書では、法律上の根拠は1978年外国諜報監視法（FISA）の2008年改正法第702条であると記載され、米国政府は一方的に電子通信サービスプロバイダのサーバーから情報を収集せず、法律上の要件にのっとって収集していること、合衆国市民を意図的に標的とすることは許されていないこと、第702条に基づく諜報情報の収集は立法・行政・司法分野による広範な監督制度に服していることなどが説明されている。その後、グーグル、ツイッター、フェイスブックは、一転してPRISMへの関与を認め、各国政府から受けた開示請求の件数等を公開するに至った[3)]。

PRISM計画を暴露したのは、中央情報局（CIA）の元技術職員であったエドワード・スノーデン氏であり、この人物は、現在はロシアに滞在しているといわれている。同氏の情報提供により、2013年10月24日、NSAはドイツの首相を含む世界の指導者35人の電話を盗聴していたと報じられ、EU首脳会議でもこの問題が取り上げられた。

ところで、米国の通信監視は、PRISM計画が初めてではない。2001年9月11日に発生した同時多発テロ以降、ブッシュ大統領（当時）は、NSAに指示を出し、テロリスト監視計画（TSP）を行っていた。TSPは、2005年12月16日のニューヨーク・タイムズの記事によって暴露されたが[4)]、ブッシュ大統領は、国の指揮官として、武力攻撃を妨害する目的で、令状なくして敵の電子的監視を行うための憲法上の権限を有していることを主張した[5)]。TSPは、現在は打ち切られているが、2007年1月頃まで行われたようである。その後に開始された類似の計画がPRISMである。

一方、日本は、国外からのテロ攻撃を受けた経験はなく、法律上も通信の秘密が厳格に保障されている。しかし、日本でも、政府機関に対する標的型攻撃が複数発生したこと等を受け、2013年10月25日、「特定秘密保護法案」が閣議決定された。同法案は、特に秘匿が必要な安全保障に関する情報（外交・防衛・スパイ活動・テロ）を行政機関の長が「特定秘密」に指定し、「特定秘密」を取り扱える人物を大臣や副大臣、政務官、「適性評価」を受けた公務員らに限定するとともに、当該情報を漏えいした公務員らには、最高で10年の懲役刑を科し、漏えいをそそのかした者にも5年以下の懲役刑を科すこと等を内容としている[6)]。また、その約4カ月前の同年6月10日に情報セキュリティ政策会議が取りまとめた「サイバーセキュリティ戦略」は、行政機関へのサイバー攻撃の手法が複雑・巧妙化していることなどを踏まえ、「各行政機関が緊密に連携してサイバー空間におけるカウンターインテリジェンスに関する情報の収集・分析・共有に係る取組を一層推進するとともに、外国機関との連携を強化するなどして、より強固な情報保全体制を構築する」方針を打ち出した。政府は、内閣情報局を2014年1月に発足させ、米国の国家安全保障会議（NSC）などとの機密情報の共有を強化させる狙いがあると報じられている。

このように、日本においても、国の情報保護に向けた政策が進められており、そのために実施される通信解析や共有、通信遮断等が、通信の秘密との関係でどこまで許されるべきかが一つの問題となる。

2. 2008年FISA改正法第702条[7]

PRISM計画は、2008年FISA改正法第702条を根拠とする。FISAは、ウォーターゲート事件を受け、1978年10月25日成立した法律であり、政府機関が外国諜報情報を得るために実施する電子的監視や物理的捜索等に関して、外国諜報監視裁判所（FISC）の裁判所命令を得るための手続等を定めている[8]。FISCはFISAによって設けられた特別の裁判所であり、合衆国の七つの巡回区から公に任命された11名の連邦地方裁判所裁判官によって構成される。

FISAは、同時多発テロを受け、2001年米国愛国者法、後述する2007年合衆国保護法及び2008年FISA改正法等により改正され、現在の規定となった。

FISAの電子的監視に関する規定では、連邦政府の捜査機関において、外国勢力及び外国勢力のエージェントが行う外国諜報情報を収集するための要件等を定めている。

連邦政府の職員が電子的監視を行う際は、FISCの裁判所命令を申請しなければならない。FISCの裁判官は、連邦政府の行政官により申請され、その申請を司法長官が承認したこと、監視対象者が外国勢力またはそのエージェントであること、及び、電子的監視を行う施設または場所が、外国勢力またはそのエージェントに利用され、または利用されようとしていることを信じるに足りる相当な理由があること、「最小化手続」[9]を満たしている等の判断を下した場合には、申請されたとおりに、または修正を加えて、電子的監視を承認する「一方的命令」（ex parte order）を発しなければならない。「一方的命令」は、FISCの裁判所命令が、監視対象者に告知されないことを意味しており、FISCは「秘密法廷」（secret court）といわれている[10]。

連邦議会は、2007年8月5日、合衆国保護法[11]を成立させた。PRISM計画開始の約1カ月前である。この法律は時限立法であり、2008年2月16日に期間満了により廃止された。その後、2007年合衆国保護法の内容を受け継ぐ形で制定されたのが、2008年7月10日に制定されたFISA改正法[12]である。

2008年FISA改正法は、個別の裁判所命令を得ることなく、国外に居る合衆国人以外の者を標的にするための手続（第702条）[13]、国外に居る合衆国人を標的にする際における個別の裁判所命令を得るための要件及び手続（第703条、第704条）[14]を定める。FISAの定める「電子的監視」は、合衆国人を対象に、国内で受発信される有線・無線通信内容の法執行目的による取得等を意味する。これに対して、2008年FISA改正法は、対象が国外であり、合衆国人以外を含める点で異なっ

図表1　2008年FISA改正法第702条に基づく外国諜報情報取得の制限

取得時に国内に居ることが分かっている人物を故意に標的にしてはならない。	国外に居ると合理的に信じられる合衆国人を故意に標的にしてはならない。
当該取得の目的が、国内に居ると合理的に信じられる特定かつ既知の人物を標的とすることにある場合に、国外に居ると合理的に信じられる人物を故意に標的にしてはならない。	発信者及び意図された全受信者が、取得時に国内に居ることが分かっている通信に関して、その通信を故意に取得してはならない。
	憲法修正第4条に即した態様で行わなければならない。

ている。「合衆国人」(United States Person)には、合衆国の市民、適法に永住権を認められた外国人、合衆国市民若しくは適法に永住権を認められた外国人を相当数の構成員とする権利能力なき社団、または合衆国で設立された法人が含まれる。ただし、外国勢力である法人や社団は含まれない。

2008年FISA改正法第702条は、司法長官と国家情報長官の共同許可により、最長1年の間、国外に居ると合理的に信じられる人物を標的とした、外国諜報情報の取得を認めている。共同許可は、司法長官と国家情報長官の共同認証を承認する裁判所命令、または、緊急事態が存在する旨の両長官の判断のいずれかに基づくことが必要である。本稿では、前者について触れることとする。

まず、外国諜報(ちょうほう)情報を取得するには、図表1のような制限が存在する。

裁判所命令を得る手続は次のとおりである。

司法長官は、国家情報長官と協議の上、国外に居ると合理的に信じられる人物を標的に限定して取得し、かつ、発信者と意図された全受信者が取得時に国内に居ると分かっている通信を故意に取得しないようにするための「標的設定手続」を採用しなければならない。同様に、司法長官は、国家情報長官と協議の上、情報取得に関する最小化手続を採用しなければならない。標的設定手続と最小化手続は、FISCによる司法審査を受けなければならない。

司法長官と国家情報長官は、共同許可に先だち、FISCに対し、書面による認証及びそれを裏付ける宣誓供述書を、封をした状態で提出しなければならない。この認証において証明すべき事柄は図表2のとおりである。同表の証明事項では、取得の対象人物を特定するように義務付けられていない点が注目される。また、電子通信サービスプロバイダから、またはその支援を受けて情報を取得することから、通信傍受のみならず、蓄積された通信や他のデータへのアクセスも含まれると理解されている[15]。

FISCは、認証や標的設定手続・最小化手続が、法定要件を満たし、憲法修正第4条に即していれば、該当する通信の取得の実施に先んじて、それらを承認する命令を発しなければならない。

2008年FISA改正法は、2012年12月31日に期限を迎える予定であったが、オバマ大統領は、同年12月30日、2012年FISA改正法再授権法に署名し、同法の期間を2017年12月31日まで延長した[16]。

3. 日本における通信の秘密[17]

通信の秘密は、憲法第21条2項後段の「通信の秘密

図表2　認証時の証明事項

標的設定手続が存在しており、それがFISCから既に承認され、承認を得るため既に提出され、または認証とともに今後提出されること。	上記手続及びガイドラインが、憲法修正第4条の要件を遵守すること。
取得に関して、電子的監視又は物理的監視の規定に基づく最小化手続が用いられることになっており、FISCから既に承認され、承認を得るため既に提出され、または認証とともに今後提出されるものであること。	取得の重要な目的が外国諜報情報の入手にあること。
取得の制限を遵守し、裁判所命令の申請を確実に行うためのガイドラインを採択すること。	取得は、電子通信サービスプロバイダから、またはその支援を受けて、外国諜報情報を取得すること。
	外国諜報情報の制限を遵守すること。

は、これを侵してはならない」との規定を受け、電気通信事業法、有線電気通信法、電波法でそれぞれ保障されている。

通信の秘密を保護する趣旨は、思想表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護することにある。ただし、通信の秘密は法人にも保護されることから、プライバシー権のみでは通信の秘密の趣旨を裏付けることはできない[18)]。

保護される「通信」は、特定者間の実質的に秘密とされるべき通信をその対象とすると解されており[19)]、音声電話だけでなく通信、電報も含まれる。また、通信内容はもちろん、通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、受発信場所、通信回数等も含まれる。

代表的な規定として、電気通信事業法第4条を見ると、次のように定められており、違反者は刑事罰に処せられる（同法第179条）。

「第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

2　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」

「電気通信事業者の取扱中に係る」とは、発信者が通信を発した時点から受信者がその通信を受ける時点までの間、電気通信事業者の管理支配下にある状態のものを指し、それ以外の全ての通信の秘密は、電波法または有線電気通信法の保護の対象となる。

通信の秘密を「侵す」行為は、①知得（通信当事者以外の第三者が積極的意思で通信の秘密を知り得る状態に置くこと）、②漏示（他人の知り得る状態に置くこと）、③窃用（発信者又は受信者の意思に反して利用すること）である。これらのうち、いずれか一つの行為が行われれば通信の秘密を侵害する。

義務の名宛人は、業務従事者への加重規定を除き、全ての者である。

4. 通信の秘密の正当化：捜査機関の通信傍受等

通信の秘密の保護は、憲法に基づく精神的自由の一つとして、強く保障される。しかし、その保護は絶対無制約ではなく、公共の福祉の観点から、例えば、拘留中の者が発受する通信物の検閲・差押、裁判所及び捜査機関による通信書類等の差押・提出命令、後述する犯罪捜査のための通信傍受、いわゆるプロバイダ責任制限法に基づく発信者情報開示等の場合等には制約される[20)]。

ところで、ここ数年にわたり、政府機関へのサイバー攻撃が問題となっているが、国の情報を守るという目的は、通常の犯罪捜査を超える重要性を持つともいえる。しかし、いかなる要件下であれば通信の秘密の侵害を正当化できるかという点は、必ずしも明確とはいえない[21)]。

サイバー攻撃には、例えば、コンピュータをウイルスに感染させれば不正指令電磁的記録供用罪、IDやパスワードを悪用したり、プログラムの不備を突くなどしてアクセス権限のないコンピュータを利用できる状態に置けば不正アクセス罪、業務用ホームページの無断改ざんやDOS攻撃、ウイルスを感染させたコンピュータの機能を阻害する行為には電子計算機損壊等業務妨害罪がそれぞれ適用され得る。

これらのサイバー攻撃は国境を越えて行われることから、日本の刑事法の場所的適用範囲や通信傍受手続等も考えておかなければならない。本稿では、紙幅の関係上ごく簡単に触れることとする。

まず、日本法に基づく犯罪については、構成要件の一部をなす行為や結果が日本で発生すれば、国内犯と

して処罰される。仮に、構成要件の全てが日本で発生しなかった場合には、国外犯処罰規定の適用が問題となる。刑法各則の罪は、サイバー犯罪条約に基づき、直接に国外犯を処罰することが可能とされており[22]、不正アクセス罪にも国外犯処罰規定が設けられた。日本の刑事罰規定が適用される場合には、捜査機関は、通信傍受手続または電磁的記録の媒体の差押手続等に入ることになる。これについては、1999年8月12日に成立した「犯罪捜査のための通信傍受に関する法律」（通信傍受法）に基づく場合のほか、2011年6月17日に成立した「情報処理の高度化等に対処するための刑法等の一部を改正する法律」により刑事訴訟法が改正され、リモート・アクセス等の諸規定が整備された[23]。

しかし、実際にサイバー攻撃が海外から行われた場合には、無関係な第三者のコンピュータを経由することなどから、攻撃源の特定は容易ではない。また、仮に犯人を特定したとしても、その人物を処断するためには、日本に引き渡してもらう必要があるため、日本法に基づき処罰することも難しいといわざるを得ない。

5. 通信の秘密の正当化：違法性阻却事由

犯罪捜査目的以外の場合に、例えば電気通信事業者において、国家機関に向けられたサイバー攻撃への対処を目的とする通信監視、保護される通信の取得・提供等が認められるか否かは、正当行為、正当防衛や緊急避難との関係で問題となる。

刑法第35条は、「法令又は正当な業務による行為は、罰しない」と定める。法令行為には、前記のとおり、裁判官の令状に基づき通信履歴を提出する場合や、プロバイダ責任制限法に基づく発信者情報を開示する場合などが該当する。

正当業務行為の「業務」とは、社会生活上の地位に基づいて反復・継続される行為をいう。総務省が2010年5月26日に公表した「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会 第二次提言」は、CGM（Consumer Generated Media）事業者によるミニメールの内容確認の是非との関連でこの問題を検討している。そこでは、正当業務に該当するものには、「通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、ISPがルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為に加え、ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）」が挙げられている（14頁以下）。ただし、この提言は、一般的な正当業務性ではなく、「国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、誰もが自由に通信を支障なく利用できる環境を確保する観点から、そうした通信役務の提供にとっての正当性の有無により判断」すると限定的に解し、網羅的・機械的に行う「ミニメール」の内容確認には正当業務性は認められないと結論付けた。この考えに基づくと、サイバー攻撃に対応するための通信監視等の場合、通信役務の安定的運営を具体的・現実的に阻害する事態の生じない限りは、正当業務性を満たすことは困難となる。

その他の正当行為は、通信当事者の双方から承諾を得る場合[24]に認められるが、国家機関へのサイバー攻撃の場面では想定しにくい。

次に、刑法第36条1項は「急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない」と定める。これについては、仮に侵害者との関係で正当防衛が成立するとしても、無関係な通信が不可避的に含まれることにより、第三者の法益を侵害した場合には、緊急避難の問題となる[25]。結局、違法性阻却は、実質的には緊急避難の成否によることとなる。

刑法第37条1項本文は、「自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない」と定める。緊急避難の要件は、危難が現に存在しているか、間近に迫っている状態であること（現在の危難の存在）、避難行為から生じた害が避けようとした害の程度を超えなかったこと（法益の権衡）、当該避難行為をする以外には他に方法がなく、かかる行為に出たことが条理上肯定し得ること（補充性）が必要とされる。緊急避難の場合は、侵害が不正である必要はなく、侵害者以外の者に向けられた法益侵害行為を正当化するものであることから、法益の権衡と補充性の要件が加重される。

安心ネットづくり促進協議会児童ポルノ対策作業部会の2010年3月30日付「法的問題検討サブワーキング報告書」は、正当防衛と緊急避難に関して、次のように説明している。

「電気通信事業者による通信の秘密の侵害が正当防衛ないし緊急避難と解され得る典型的な事例としては、通信施設に対する攻撃に対応したり人の生命身体に対する危険を避けたりするために通信の秘密を侵すことが必要な場合等が挙げられる。

前者の例としては、大量通信に起因する電気通信事業者の設備障害の発生を回避する目的で、DOS攻撃などのサイバー攻撃、ワームの伝染及び迷惑メールの大量送信及び壊れたパケット等の大量通信に対して、遮断その他の措置を採る場合が挙げられる。

後者の例としては、インターネット上における、人命保護の観点から緊急に対応する必要がある自殺予告事案につき、ISPが、警察に対して、書き込んだ者や電子メールを送信した者の氏名・住所その他当該者を特定するに足りる情報を開示する場合が挙げられる。」（14頁）

緊急避難に関して、刑法学の分野では、実際に正当化されることはほとんどないといわれている。総務省の前記第二次提言も、現在の危難が認められるのは、生命または身体に対する重大な危険に比肩するものに限られると述べている。

しかし、安心ネットづくり促進協議会の掲げた上記の例に照らして考えると、国の情報保護のために緊急に必要が認められる場合には、攻撃者を特定するために、パケットの経路等の通信記録を取得・解析したり、特定の通信を遮断することを認める余地は存在すると考えられる。緊急避難の考えを採用する方針は、総務省が2013年7月8日に公表した「人命救助等におけるGPS位置情報の取扱いに関するとりまとめ」の中でも言及されている。

問題は、国の情報の安全という法益を保護するための通信監視などが、現在の危難、法益の権衡、補充性を満たすか否かである。

まず、DOS攻撃などのサイバー攻撃、ワームの伝染及び迷惑メールの大量送信及び壊れたパケット等の大量通信が行われ、または行われようとしている事実が発生すれば、「現在の危難」が存在するといえる。この点、サイバー攻撃を感知するには、データの異常値を発見することが端緒となるが、それだけでは攻撃の有無を判別することは不可能と考えられ、どの段階から現在性が顕在化したかをリアルタイムで法的に評価するのは困難である。そのため、通信監視が結果的に不正な攻撃を防いだ場合に、現在性の要件を満たしたか否かを事後的に判断することとなる。しかし、サイバー攻撃の予防には事前措置が必須であることから、必要最小限の範囲で、現在性の有無を検知するための通信監視を事前に容認するための法的措置を検討する必要があると考えられる。なお、通信傍受法は、傍受すべき通信に該当するかどうか明らかでないものについて、それに該当するか否かを判断するため、最小限

度の範囲に限り傍受できるとの規定を置くなど、無関係な情報を排除するような工夫がなされている。こうした制度を参考にすることも考えられる。

次に、通信の秘密と国の情報の安全の間には、法益の権衡が認められ得ると考えられる。最後は補充性であるが、第一次的にはサイバー攻撃者を取り締まることが、通信の秘密に対する侵害性の少ない手段といえる。しかし、サイバー攻撃は、いったん発生してしまうと、攻撃前の状態に戻すことは不可能であり、事後的な通報は無意味である。上記のとおり、攻撃への対策を行うのであれば、事前に検知を行い排除することを目的とした監視の仕組みを導入せざるを得ない。また、サイバー犯罪の攻撃者を特定することは容易ではなく、取り締まりに期待することは問題の先送りを意味する。他方、通信記録の取得、解析や通信の遮断行為には、不可避的に無関係な通信を含まざるを得ないことから、補充性を満たすためには、保護すべき情報を機密性の高いものに限定すること、攻撃に無関係な通信を侵害しないようにするための技術的措置を講じることが、最低限必要であると考えられる。保護すべき情報は、制定が予定される「特定秘密保護法」の「特定秘密」に相当するものなどが考えられ、係る秘密の含まれたサーバーを監視対象にするという方法もあり得る。

6.おわりに

米国では、2001年9月11日の同時多発テロ以降、テロの脅威が現実のものとなり、通信の秘密やプライバシーといった個人の利益を犠牲にしても、国の安全を優先すべきという価値判断が、米国社会の共通認識となっている[26)]。

2008年FISA改正法は、個別の裁判所命令を要求しておらず、令状主義自体を骨抜きにする内容である。そして、裁判所命令を得る場合でも、FISCの命令は極めて緩やかに運用されている。1979年から2012年までのFISCに対する裁判所命令の申請件数は、合計3万3,949件、許可件数は3万3,942件であった。申請が年末に行われ、許可が年明けに出されることがあるため、各年の申請件数と許可件数は必ずしも一致しないが、申請却下はごくわずかにとどまる[27)]。

オバマ政権は、2013年8月9日、監視に対する国民の不安を和らげるため、司法審査への信頼改善や監視に関する情報公開を進めることなどを方針に掲げ、年内に最終報告書を提出する予定であることを明らかにした[28)]。監視計画自体を見直す方針ではないようである。

これに対し、日本は、テロへの脅威は現実的ではなく、国家安全目的による通信の利用と、通信の秘密が尖鋭に対立しているわけではない。しかし、厳格に保護される通信の秘密であっても、不可欠な公共の利益を実現するために適切に設定された必要最小限の制約は許される[29)]。そして、国の情報の安全という不可欠な公共の利益のために、通信の秘密の侵害を正当化する方法には、前記のとおり、刑事手続によるものと、緊急避難の理論を用いるものがある。

しかし、令状申請による場合には、米国と同様、令状主義の形骸化が問題である。

毎年の捜索差押許可状や検証許可状の件数について、2012年度の司法統計では、発付件数は23万6,289件、却下件数は104件であった。2011年度の司法統計では、発付件数は合計22万6,041件、却下件数は183件であった。また、2012年中の通信傍受の実施状況等では、令状申請件数は32件、発令された件数も32件であった。2011年は、令状申請件数が27件、発付件数が25件であった[30)]。このように、令状を申請すればほとんどの確率で発付されており、令状主義は事実上機能していないといわざるを得ない。

残る手段は緊急避難であるが、前記のとおり、現在

の危難や補充性に課題が存在する。

通信の秘密は厳格に過ぎるという批判を耳にすることがある。しかし、米国のような事実上無制限の監視は許されるべきではなく、また、通信の秘密の例外を解釈で押し広げることで、従来の解釈・運用と矛盾を来すことも法的安定性の観点からは望ましくない。国家安全の大義名分の下で、事実上無制限の侵害行為が容認されることのないよう、保護すべき情報の範囲、技術的な制限手段の在り方を含め、立法措置を含めた適切な運用ルールの制定とそのための全体的な合意形成が求められる。

Kaori Ishii
石井 夏生利
筑波大学 図書館情報メディア系 准教授、博士（法学）。専門はプライバシー権、個人情報保護法
内閣官房「社会保障・税に関わる番号制度　個人情報保護ワーキンググループ」委員、総務省情報通信政策研究所特別上級研究員、総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」「スマートフォンを経由した利用者情報の取扱いに関するWG」委員、同「スマートフォン時代における安心・安全な利用環境の在り方に関するWG」委員、行政書士試験委員等。著書は、『インターネットの法律問題ー理論と実務ー』新日本法規（共著）（2013）、『プライバシー・個人情報保護の新課題』商事法務（共著）（2010）、『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』勁草書房（単著）（2008）など。

注

1) *NSA slides explain the PRISM data-collection program*, The Washington Post, Jun. 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last visited Aug. 28, 2013).

2) Director of Nat'l Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Jun. 8, 2013), http://www.dni.gov/files/documents/Facts on the Collection of Intelligence Pursuant to Section 702.pdf.

3) 日本経済新聞2013年8月27日朝刊11頁「ネットとプライバシー（1）　米政府、どう情報収集　企業から自動吸い上げ」、IT mediaニュース2013年8月28日「Facebook、各国政府からの個人情報要請状況を公開」（http://www.itmedia.co.jp/news/articles/1308/28/news039.html）。

4) James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N. Y. Times, Dec. 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html (last visited Aug. 28, 2013).

5) U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

6) NHK NEWS WEB 2013年10月25日「特定秘密保護法案を閣議決定」（http://www3.nhk.or.jp/news/html/20131025/k10015544181000.html）。

7) FISA全般については、平野美恵子ほか「米国愛国者法（反テロ法）（上）」外国の立法第214号

注

(2002年11月)1－46頁、同「米国愛国者法(反テロ法)(下)」外国の立法第215号(2003年2月)1－86頁、岡本篤尚『《9・11》の衝撃とアメリカの「対テロ戦争」法制―予防と監視―』(法律文化社、2009年)、金井淳「「愛国者法」の改正と通信の傍受」ジュリスト第1307号(2006年3月)101頁、同「国外諜報監視法(FISA)の改正」ジュリスト第1345号(2007年11月)51頁参照。

8) Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § § 1801–1885c (2012).

9) 電子的監視を行う情報の収集、保有、提供等を必要最低限とすること等を内容とする手続きをいう。

10)岡本・前掲『《9・11》の衝撃とアメリカの「対テロ戦争」法制』180頁。

11)Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (repealed 2008).

12)Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § § 1881–1881g (2012).

13)50 U.S.C. § 1881a.

14)50 U.S.C. § § 1881b, 1881c.

15)Edward C. Liu, ***Reauthorization of the FISA Amendments Act***, CRS REPORT FOR CONGRESS, R42725, Apr. 8, 2013, at 5-6.

16)なお、TSPやPRISMに対する修正第4条違反等を主張する訴訟は、訴えの利益がないとして退けられている。*See* ACLU v. NSA, 128 S.Ct. 1334 (2008); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

17)通信の秘密に関する解説は、違法性阻却事由を含め、小向太郎『情報法入門　デジタル・ネットワークの法律』(NTT出版、第2版、2011年) 71－81頁参照。

18)多賀谷一照ほか編『電気通信事業法逐条解説』(電気通信振興会、2008年) 37頁。

19)岡崎俊一「通信の秘密の保護とその課題」(2012年8月改訂) 多賀谷一照、松本恒雄編『情報ネットワークの法律実務』(第一法規、1999年) 3303－3319頁、3308頁。

20)詳細は、岡崎・前掲「通信の秘密の保護とその課題」3311－3312頁。

21)正当化理由を含め、通信の秘密に関する憲法学的観点からの問題提起を行ったものとして、宍戸常寿「通信の秘密について」早稲田大学グローバルCOEプログラム『季刊　企業と法創造』通巻第35号「特集・憲法と経済秩序IV」(2013年2月) 14－29頁。

22)インターネットと刑法に関しては、宇賀克也・長谷部恭男『情報法』(有斐閣、2012年) 247－269頁、267頁、高橋和之ほか『インターネットと法』(有斐閣、第4版、2010年) 241－247頁。

23)安冨潔『刑事訴訟法』(三省堂、第2版、2013年) 210－220頁、池田修・前田雅英『刑事訴訟法講義』(東京大学出版会、第4版、2012年) 180－191頁。

24)多賀谷・前掲『電気通信事業法逐条解説』36－41頁。

25)浅田和茂・井田良『新基本法コンメンタール　刑法』(日本評論社、2012年) 102頁参照。

26)位置情報の取得に関して、連邦最高裁は、令状の範囲外で自動車を監視した行為を修正第4条違反とする判決を下した。United States v. Jones, 132 S.Ct. 945 (2012).

27)Electronic Privacy Information Center, ***Foreign Intelligence Surveillance Act Court Orders 1979-2012***, http://epic.org/privacy/wiretap/stats/fisa_stats.html#footnote12 (last visited Aug. 28, 2013). 申請が拒否されたのは11件である。

28)CNET Japan2013年8月10日「米大統領、NSAの改革に向けた4つの方針を発表」(http://japan.cnet.com/news/business/35035812/).

29)宇賀・長谷部・前掲『情報法』68頁。

30)法務省ないしは厚生労働省が毎年発表している「通信傍受の実施状況等」を参照。

「International Communication Association（ICA） Annual Conferences」参加報告

米谷 南海
慶應義塾大学 大学院 政策・メディア研究科 後期博士課程

**2013年6月18～21日、ロンドンにて、
コミュニケーション研究分野で最大規模の国際学会の一つであるICAが開催された。
環境の変化に伴う研究手法の課題と可能性などが活発に議論された。**

◆2013年次のICA大会概要

今回、筆者は公益財団法人KDDI財団による海外学会等参加助成を受け、ロンドンで開催されたICA（International Communication Association）に参加する機会を得た。ICAは1963年にアメリカの研究者を中心に発足したが、現在では65カ国から約3,500人の参加者が集うコミュニケーション研究分野で最大規模の国際学会の一つであり、2003年にはNGOとして国連に公認・登録されている。

2013年度のICA年次大会は、“Challenging Communication Research”というメインテーマの下、“Communication and Technology”、“Communication History”、“Communication Law and Policy”、“Ethnicity and Race in Communication”、“Game Studies”、“Global Communication and Social Change”、“Health Communication”、“Journalism Studies”、“Political Communication”、“Public Relations”等、27のユニットに基づいた分科会やワークショップが設置され、2013年6月18～21日にかけて開催された。なお、6月14～17日にはPre-conferenceが、22～24日にはPost-conferenceが、それぞれロンドン各地の会場で開催された。

メインテーマにあるように、ICA2013では、コミュニケーション研究の各分野における研究手法の課題と可能性が議論された。ニューメディアやソーシャルネットワークの台頭といったコミュニケーション環境の変化にどのように対応し、適切な方法論をもって研究を進めていくかが大きな課題となっている。

◆新しいネットワーク構造と今後の研究課題

全体セッションである“The Network Tradition in Communication Research and Scholarship”では、従来のネットワーク理論が今後直面するであろう課題、また技術進歩がネットワーク理論に与える影響というテーマでパネルディスカッションが行われた。例えば伝統的マスメディアが家庭内など限定的な場所で用いられ、人々の価値観を統一させる機能があったのに対して、ニューメディアは様々な場所で使用可能であり、かつ個人が多様な意見をそれぞれに表明することができる。そのような特徴を踏まえ、今後のコミュニケーション研究においては、(1)ニューメディアが形成す

全体セッションの様子


分科会の様子

るネットワークの範囲や重層に着目すること、(2)学際的な分析アプローチが必要であること、(3)分析に用いるデータの量だけでなく収集範囲を広げるべきであることなどが、論者から指摘された。

また、分科会やワークショップにおいても各国におけるコミュニケーション環境の変化事例が数多く紹介され、それに対応するような研究方法論に関する活発な議論が交わされた。その中でも印象に残ったものとして、以下三つのワークショップ及び分科会を挙げておきたい。

第一に、“New Media and Citizenship in Asia: Researching the Practices, Functions, and Effects of the New Mediain Asian Politics”では、アジア地域におけるニューメディアの利用状況やその社会経済的影響が報告された。特に台湾や韓国の選挙におけるTwitterの影響や、YouTubeを用いてスラム街市民の声を国外に届けるインドのプロジェクトに関する報告は、SNSの戦略的活用事例として非常に興味深かった。第二に、“Post-Broadband Access: Comparative Assessments and Prospects”では、人々にとってインターネットアクセスが当たり前のように可能になる時代を「ポスト・ブロードバンド時代」と呼び、その時代に懸念されるプライバシー問題、料金に関する問題、アクセス格差などについて議論が交わされた。従来のブロードバンド普及に関する研究はアクセス格差をアクセスの可不可で論じていたが、今後はブロードバンドの質やユーザーが利用できるサービスの多様性に検討課題が移行していくことが予想される。第三に、“Beyond the Qualitative/Quantitative Dichotomy: Q Methodology as an Innovative Approach to Audience Research”ではQ方法論とインタビュー調査とを組み合わせるアプローチ方法や異文化間の比較研究にQ方法論を活用する方法が報告された。再現性の低さや比較研究の困難さといった伝統的な定性分析手法が抱える課題を、Q方法論によって克服する方法論が報告された。

ICA2013への参加を通じて、今後のコミュニケーション研究では、新しい情報通信サービスやプラットフォームの登場により、従来とは異なるネットワーク構造が形成されている点を意識して研究を進めていく必要があることを痛感した。このような貴重な機会を与えていただいた公益財団法人KDDI財団に心よりお礼申し上げたい。

Nami Yonetani
米谷 南海
慶應義塾大学 大学院 政策・メディア研究科 後期博士課程
2009年慶應義塾大学総合政策学部卒業、2011年慶應義塾大学大学院社会学研究科修了(修士)。専門は、メディア産業論及び情報通信政策論。研究業績に、"The Role of Cable TV Operators as a Facility Based Competitor in the Local Broadband Market. A Case Study from Three Competitive Areas in Japan" Pacific Telecommunications Council 2013 O.S. Braunstein Student Paper Prize Award 受賞など。

彼らの流儀はどうなっている？

執筆：高橋麻理子　絵：大坪紀久子

オスクジャクは羽の目玉模様を競い合い、メスに求愛すると考えられてきた。
しかし、彼らはさらに進化を遂げていたのかもしれない。

もてるクジャクは声で勝負

ダーウィンの悩み

150年ほど前、チャールズ・ダーウィンは友人への手紙に、「オスクジャクの尾羽を見るたび私は気分が悪くなる」と書いたという。なぜオスだけが美しい目玉模様の羽を持つのだろうか？　あの美しい羽は、生存にもオス同士の戦いにも役立ちそうにない。

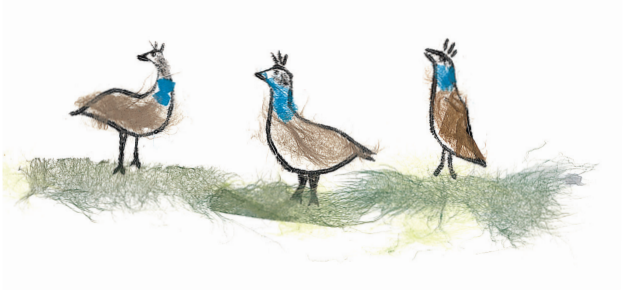
そこでダーウィンは、美しい羽を持つオスほどメスから好まれ、多くの子を残したのではないか、と考えた。

イギリスの研究者が放し飼いのインドクジャクを観察し、羽の目玉模様の数が多いオスほど多くのメスから繁殖相手に選ばれたことを報告したのは、22年前。ダーウィンの悩みは解決されたかに見えた。

しかし、日本や他国の追試では、メスの好みとオスの目玉模様の数に必ずしもいつも関連が見られたわけではなかった。ア

Mariko Takahashi　東京大学 大学院 総合文化研究科 附属進化認知科学研究センター 特任研究員

1975年生まれ。国際基督教大学教養学部理学科卒業、
東京大学大学院総合文化研究科広域科学専攻博士課程単位取得退学。
キジ科の鳥の繁殖生態や求愛ディスプレイの進化を調べている。



イトラッカーを使った研究によって、メスがオスの目玉模様の大半に注意を向けていないこともわかってきた。

今、再び、ダーウィンの悩みに挑戦する時である。

けたたましい鳴き声

インドクジャクには、明らかに、もてるオスともてないオスがいる。目玉模様の数でないなら、メスは何を手掛かりにオスを選んでいるのだろうか？

様々なオスの特徴を調べた結果、私は、“鳴き声”ではないかと考えている。数キロ先まで届く繁殖オスのけたたましい鳴き声は、目玉模様のけばけばしさと比べても遜色（そんしょく）ない。

小鳥のように美しい声ではないけれど、「人間の好みの基準で他の種の好みを判断してはならない」とはダーウィンも書いている。

何より、オスの鳴き声の特徴（例えば鳴き声の繰り返し回数）には、羽の目玉模様の数と比べてはるかに大きな個体差がある。そして実際に、インドや日本の調査地では、「ケオーン」や「カー」という鳴き声を繰り返し鳴いたオスほど、メスから多く選ばれていた。

インドクジャクと最も近縁なマクジャクにも目を向けてみよう。近縁といっても、2種のクジャクが分かれたのは、およそ500万年前。ヒトとチンパンジーが分かれた頃の大昔である。それにもかかわらず、この2種のオスは、目玉模様の羽も、それを使ったダンスもそっくりなのだ。つまり、驚くべきことに、あの美しい羽とダンスは500万年もの間、ほとんど変わらずに維持されてきたようである。一方、求愛の鳴き声は2種のオスで全く異なり、インドクジャクのオスの方がけたたましい。鳴き声の性差も、インドクジャクの方がはっきりと大きい。

美しい羽は流行おくれ

ここからは私の妄想だ。かつて“祖先クジャク”のメスは、より美しい羽を持つオスを選んで繁殖したのだろう。ダーウィンが想像したとおりに。その後、オスとメスの間で、より刺激的な求愛を巡るせめぎ合いが続き、インドクジャクのオスは、美しい羽とダンスという“流行の過ぎてしまった最低条件”を維持しつつ、大きな鳴き声という新しいアピール手段を得たのかもしれない。

ダーウィンも、「最も新しい手段で着飾ったオスが、他のオスとの競争で有利になっただろう」と書いている。もしこれが本当だとすれば…、今から数百万年後、インドクジャク（の子孫）のオスたちは、美しい羽を広げて、踊って、鳴いて、さらに、私達には未知の全く新しい求愛レパートリーを、メスに披露しているのだろうか？

やさしいICT用語解説 ❾

4K·8K

次世代放送サービスとされている「4K·8K」。
総務省は、4K·8Kテレビ放送の実用化スケジュールを具体的に提示している。
どのように、画像は変わるのだろうか。

◆デジタル画像の高密度化

4K·8Kとは、デジタル映像の解像度に関する俗称である。4K·8KのKは1000の単位のことで、画面の水平方向の画素数を指す。デジタル映像は色と明るさを表示する点(画素)の集合で表現され、その画素の数が水平方向に約4000の規格が4K、約8000の規格が8Kである(図表参照)。

現行の「地上デジタルテレビ」放送の画素数は、1440×1080(水平方向×垂直方向、以下同じ)で、「フルハイビジョン」と呼ばれるBSデジタルテレビ放送では1920×1080(2K)である。これが「4Kテレビ」では3840×2160、「8Kテレビ」では7680×4320となり、それぞれ解像度(総画素数)が現行フルハイビジョンの4倍、16倍となる。他方、「デジタルシネマ」の分野でもカメラや編集機材、劇場が4K規格に対応するようになってきており、映画製作会社が加盟する団体Digital Cinema Initiatives(DCI)が定めている4Kの主要規格は4096×2160とテレビの4K規格とは異なっている。ただし、カメラや編集機材の多くは映画規格、テレビ規格のどちらでも使用可能となっている。以下では、生活に密着するテレビ放送について述べる。

4K·8Kテレビの技術開発は、日本ではNHK放送技術研究所が1995年からハイビジョンを超える「超高精細映像システム」として取り組んできており、8Kについては「スーパーハイビジョン」と呼んでいる。世界的には、国際電気通信連合(ITU)が、「4K Ultra High Definition Television(4K UHDTV)」、「8K Ultra High Definition Television(8K UHDTV)」として4K·8Kテレビの国際標準規格を策定している。ITUでは、4K·8Kテレビに対する映像の縦横比(アスペクト比)、1秒間に表示する画面の枚数(フレーム数)、映像の表示方式などのほか、映像信号の圧縮伸張技術についても国際標準化機構/国際電気標準会議(ISO/IEC)と共同で国際標準規格を定めている。

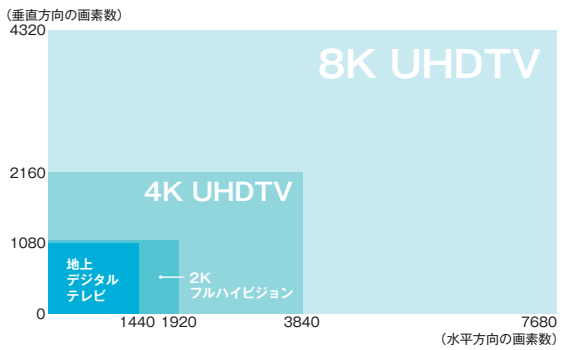
◆求められる技術開発

このようなテレビの高解像度化が進展している背景には、表示装置となる液晶パネルの高度化や低価格化、映像処理技術の進化とともに、消費者の「大画面」志向がある。50型を超える大画面市場は、低迷するテレビ市場において唯一台数ベースでも金額ベースでも伸びているとの調査結果が公表されている。ただ、50型を超える大画面になると、フルハイビジョン規格の解像度では画素が見えやすくなり画質に物足りなさを感じるようになってしまう。このため、解像度を上げることで大画面かつ高画質による没入感を実現し、消費者の購買意欲に結び付けようという動きとなっている。

現状では、4Kの解像度を持つコンテンツは市場には十分に出回っていないため、2Kフルハイビジョン用のコンテンツを4Kのテレビで見る場合が多いが、2Kのコンテンツの画素間の色の変化や映像の動きの変化を滑らかに見せる技術的な工夫が施されており、4Kテレビでの映像は2Kテレビよりもきれいに見えるといわれている。

また、4K·8Kのテレビ放送を実用化するためにはカメラやビデオなどの撮影機材やテレビ受像機の他にも、テレビ信号を中継したり、放送したり、ケーブルテレ

図表 解像度の比較



ビ回線を使って配信する技術の開発も必要になる。

4K･8Kテレビの信号量は、解像度が高くなればなるほど増える（フレーム数や画素、色の精細度が増すともっと増える）こととなり、4Kテレビではハイビジョンテレビ信号（標準的な映像信号量1.5Gbps、以下同じ）の約6.7倍（10.0Gbps）、8Kでは26.5倍（39.8Gbps）という膨大な信号量を処理、伝送する必要がある*)。これらの映像信号を、画質を損なうことなく送受するためには、ハイビジョンの伝送で使われている信号圧縮伸張技術よりも、より圧縮伸張率の高い技術を開発する必要があり、NHKやKDDIなどで開発が進められている。

KDDIでは、2013年2月、8Kのスーパーハイビジョン信号を80Mbpsにまで圧縮する技術を開発し、CATV回線で伝送することに成功している。映像信号の圧縮伸張技術については、ITUとISO／IECが2013年1月に国際標準技術としてH.265／HEVC（High Efficiency Video Coding、）を承認しており、同じ画質であればBSデジタル放送で使われているH.262／MPEG-2（1995年策定）比でおよそ4倍、地上デジタル放送で使われている圧縮方式H.264／MPEG-4 AVC（2003年策定）比で約2倍の圧縮率を実現している。

◆実用化のタイムスケジュール

韓国では2013年7月から、韓国ケーブルテレビ放送協会が世界に先駆けて4Kのテレビ実験放送を始めているが、我が国では、2013年2月、総務省の「放送サービスの高度化に関する検討会」で、今後の4K･8Kテレビ放送の具体的なスケジュールを提示している。それによると

2014年　可能な限り早期に、関心を持つ視聴者が4Kを体験できる環境を整備
2016年　可能な限り早期に、関心を持つ視聴者が8Kを体験できる環境を整備
2020年　希望する視聴者が、テレビによって4K･8Kの放送を視聴可能な環境を実現

となっている。この検討会開催までは2020年の実験放送、2025年が実用化試験放送とされていたので、4K･8Kテレビ放送のサービス開始は5年以上前倒しされており、テレビ技術・産業の国際競争は既に始まっている。2013年5月には、NHKやソニーなど、放送、通信、家電メーカー21社・団体で構成する次世代テレビ開発のための「次世代放送推進フォーラム」が設立され、オールジャパンで世界市場への進出を目指している。

放送局の設備、電波の送受信から家庭内の受像機まで、テレビ放送は入り口から出口までが一つの規格で統一されて初めて機能する巨大なシステムである。東京オリンピック（1964年）とカラーテレビ、シドニーオリンピック（2000年）や日韓共催ワールドカップサッカー（2002年）とBSデジタル放送など、新しい規格は視聴者の興味が高まるスポーツイベントに合わせて普及が図られてきた。これからも、スポーツイベントを目標に実用化に向けて放送実験や各種のルール作りなどが進められる。その意味でも2020年の東京オリンピック招致成功は絶好の追い風となっている。

*) 現在は、10bit/pixel（画素）、60fps（フレーム数）、4：2：2（色）フォーマットでの利用が一般的と推測されている。

臨場感と解像度

臨場感は画面を見込む角度「視角」によって決まる。より広い視角で画像を見る、つまり目で見える範囲いっぱいになるほど画面に近づけば、臨場感は高まる。テーマパークやイベントで体験できる大画面映像を使ったアトラクションで、スリルや浮遊感、身体が動いているような感覚を覚えるのは、この視覚による臨場感の利用である。

一方で、画面に近づいていくと画素、つまり画像を構成する色の点が見えるようになってしまう。画素が見えにくくなる画面からの距離「視距離」（画面からの距離を画面の高さで割った値で、単位としてHが使われる）は、地上デジタルテレビ放送などで採用されているハイビジョン方式では3Hといわれている。では、どこまで近づけば臨場感を高める上で有効なのか。NHK放送技術研究所の研究では、人が感じる臨場感は0.75H、視覚80°～100°で飽和するとされている。この0.75Hとなる画面の大きさに対して、視力1.0の人が画素を見分けられないようにするためには、水平画素数を約8000にすればよいという研究結果が出た。スーパーハイビジョンの画素数8Kは、このようにして導き出されたという。

それでも地球は回っている。
……ガリレオ・ガリレイ

ガリレオの言い訳

髙橋秀実

1633年、地動説を唱えていたガリレオ・ガリレイはローマ教皇庁の異端審問所で有罪の判決を受けた。本の発禁処分と蟄居（ちっきょ）せよという判決。そこで彼は「それでも地球は回っている」とつぶやいた――。

という有名なエピソードがあるが、どうやらそれは後世の作り話らしい。彼は素直に判決に従ったばかりか、「何を書いたか覚えていない」「読み返してみたら別人が書いたかのようで、これでは地動説を支持していると思われてもしかたがない」「間違いを認めます」などと弁明していたそうなのだ。

とぼけたのか。

あるいは権力に屈したのか。真相はよくわからないので、審問の対象になった『天文対話』（岩波文庫　昭和34年）をあらためて読んでみたのだが、有罪にした教皇庁の気持ちがなんとなくわかるような気がした。

なにしろ回りくどい。そもそもこの本はガリレオ本人が地動説を訴えているのではなく、3人の登場人物による対話形式。天動説を盲信する男、中立の紳士、そしてガリレオらしき男。天動説の男を4日間にわたって論破していくのだが、その方法がいやらしい。人格を中傷したり、実験したのかと問いただして、あなたこそ実験したのかと切り返されると、「実験しなくてもそうならなければならないからです」と開き直る。そして中立の男が「結論は出た」と賛同しても、「私は結論していないし、結論しようともしていない。根拠と返答、反論と解決を述べただけ」などと蒸し返したりする。実はすでに教皇庁は地動説を仮説として認めていたらしく、判決はこの意地悪な物言いに対して下されたかのようなのだ。中でも印象的だったのはガリレオらしき男の次の発言。

「地球の自然的本能が二四時間で中心の周りを回ることであったならば、そのあらゆる部分の内在的で自然的な傾向もま

article：**Hidemine Takahashi**
ノンフィクション作家。1961年生まれ。東京外国語大学モンゴル語学科卒業。
著書に『素晴らしきラジオ体操』『からくり民主主義』『やせれば美人』『趣味は何ですか？』『結論はまた来週』『「弱くても勝てます」開成高校野球部のセオリー』など。
『ご先祖様はどちら様』で第10回小林秀雄賞受賞。最新刊に『男は邪魔！「性差」をめぐる探究』（光文社新書）。

た、じっとしていることではなく同じ進行のあとを追うことであるはずだ」

地球は常に回っている。回ることが「本能」で、一緒に回っている私たち人間にも「あとを追う」という傾向があるはずだという指摘。天動説に追従することへの皮肉でもあるようだが、それは同時にコペルニクスの地動説のあと追いをするガリレオの言い訳ではないだろうか。

「それでも地球は回っている」

ガリレオがそう言ったかどうか定かではないが、これは人間は何かのあとを追いかけることしかできない、あるいは同じようなところを回っているだけなのだという箴言（しんげん）なのかもしれない。

※参考文献『ガリレオ―伝説を排した実像』ジョルジュ・ミノワ著　白水社　2011年

背景

16世紀半ば、コペルニクスは地動説を唱え、ケプラーやガリレオ・ガリレイ（1564～1642年）がこれに続いた。ガリレオは1616年と1633年にローマの異端審問所により有罪となった。ローマ教皇庁が、ガリレオ裁判は誤りだったと認めたのは1922年である。

編集後記

今号の特集は「インターネット時代における通信の秘密」としました。法律を専門とする先生方に様々な視点で論じていただきました。いかがでしたでしょうか？

Nextcom誌では学識経験者の先生方で構成する監修委員会を設置し、読者の方々にご満足いただくための改善点などにつきご指導をいただくとともに、著書出版助成やNextcom情報通信論文賞の受賞者をご審査いただいています。

来年3月発刊予定の次号では、上記受賞者に関するご報告をさせていただく予定です。

また、次号の特集は、東日本大震災から3年となることを踏まえ、「災害と情報通信Ⅱ（仮称）」とする予定です。（しのはら）

Nextcom（ネクストコム）Vol.16 2013 Winter
平成25年12月1日発行

監修委員会（五十音順）
委員長　舟田 正之（立教大学 名誉教授）
副委員長　菅谷 実（慶應義塾大学 メディア・コミュニケーション研究所 教授）
委員　依田 高典（京都大学 大学院 経済学研究科 教授）
川濵 昇（京都大学 大学院 法学研究科 教授）
辻 正次（兵庫県立大学 大学院 応用情報科学研究科 教授）
林 敏彦（大阪大学 名誉教授）
山下 東子（大東文化大学 経済学部 教授）

発行　株式会社KDDI総研
〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエアタワー
TEL：03-6678-6179　FAX：03-6678-0339
URL：www.kddi-ri.jp

編集協力　株式会社ダイヤモンド社
株式会社メルプランニング
有限会社エクサピーコ（デザイン）
印刷　瞬報社写真印刷株式会社

本誌は、我が国の情報通信制度・政策に対する理解を深めるとともに、時代や環境の変化に即したこれからの情報通信制度・政策についての議論を高めることを意図しています。
ご寄稿いただいた論文や発言等は、当社の見解を示すものではありません。

●本誌は当社ホームページでもご覧いただけます。
http://www.kddi-ri.jp/nextcom/index.html

●宛先変更などは、株式会社KDDI総研Nextcom（ネクストコム）編集部にご連絡をお願いします。（Eメール：nextcom@kddi-ri.jp）