第３章

＜警察政策フォーラム＞
ＩＣＴ社会の自由と安全～通信の秘密を考える

＜警察政策フォーラム＞
「ＩＣＴ社会の自由と安全～通信の秘密を考える」

警察政策研究センター

警察政策研究センターは、平成25年３月14日、市民生活の自由と安全研究会、（公財）公共政策調査会、（一財）保安通信協会及び（一財）警察大学校学友会との共催並びに慶応義塾大学法学部及び警察政策学会の後援により、慶応義塾大学三田キャンパス（東京都港区）において、警察政策フォーラム「ＩＣＴ社会の自由と安全～通信の秘密を考える」を開催した。

近年、スマートフォンやソーシャルメディア等の情報通信技術の発達はめざましく、それに伴い、組織犯罪、テロ等の各種犯罪において通信が果たす役割は飛躍的に増加している。このため、こうした犯罪の予防・検挙に当たっては、通信に対するアプローチが欠かせない。その一方で、日本国憲法第21条第２項において「通信の秘密」が規定されていることから、これを保障しつつ新たな通信形態をも念頭に入れて市民の安全を守るためにはどのような施策が望ましいのかを検討することが重要となる。

本フォーラムは、上記の点を踏まえ、昨今の情報通信技術と警察活動との関係、通信に関する憲法上の問題点等について優れた知見を有する内外の研究者・実務者による報告を基調として議論を深めることにより、今後我が国において実施すべき施策について検討することを目的として開催されたものである。

本フォーラムでは、大沢秀介慶応義塾大学法学部教授による開会挨拶の後、葛西まゆこ東北学院大学法学部准教授によるイントロダクション（「憲法学から見た通信の秘密」）が行われ、さらに、有識者４名による基調講演が行われた。講演者及び講演タイトルは、次のとおりである。

○　石井徹哉氏（千葉大学大学院専門法務研究科教授）
　「刑事法から見た通信の秘密」
○　四方光氏（警察大学校刑事教養部長（当時）、現慶応義塾大学総合政策学部教授）
　「サイバー犯罪捜査における事後追跡可能性と通信の秘密」
○　ラルフ・ポッシャー氏（フライブルク大学法学部教授）
　「より成熟した安全法に向けて」
○　林紘一郎氏（情報セキュリティ大学院大学教授）
　「通信の秘密：個人の権利か、事業者の義務か」

また、これらの基調講演の後のパネルディスカッション（討論）では、横内泉警察政策研究センター所長（当時、現宮城県警察本部長）がコーディネーターを務め、上記の基調講演者のほか、大沢秀介氏、小山剛氏（慶應義塾大学法学部教授）、板橋功氏（（公財）公共政策調査会第一研究室長）により、ＩＣＴ社会の自由と安全について活発な議論が行われ、盛会のうちに終了した。

なお、本フォーラムには、大学研究者、企業関係者、報道機関、関係機関、警察関係者等、約210名が出席した。

【開会挨拶】

慶応義塾大学法学部教授　大沢秀介

ただいまご紹介いただきました慶應義塾大学の大沢でございます。本日はお忙しい中、多数の皆様にお越しいただきましてありがとうございました。深く御礼申し上げます。

先ほどご紹介がありましたように、我々の市民生活の自由と安全研究会では、警察政策研究センターの方々とともに、2001年の9.11事件を契機として、公益財団法人公共政策調査会、一般財団法人保安通信協会、及び警察大学校学友会の財政的援助をいただきながら、10数年間、市民生活の自由と安全に関わるテーマを学者と実務家の共同研究という形で行ってまいりました。その活動は毎月の定例会に加えて、今回のようなフォーラムを慶応義塾大学法学部及び警察政策学会のご後援をいただく形で3年に一度開催をし、それらの研究活動を踏まえた成果を出版という形で社会に問うという形で行ってまいりました。

現在の研究会のテーマは、情報に関わる諸問題に対して憲法、さらに広く法的な対応を考えるということにあります。今回の警察政策フォーラムのタイトルである「ICT社会の自由と安全～通信の秘密を考える」は、そのテーマと強く共鳴するものと思っております。また今回のテーマは、広く情報技術を社会の中でいかに共有していくかということに関わる、現在、我が国で喫緊の課題となっているものでもあります。

そこで今回のフォーラムでは、実務家として警察大学校の四方刑事教養部長、刑事法の観点から石井千葉大学法科大学院教授、ドイツ法の観点からフライブルク大学のポッシャー教授、そして長年この問題に携わり具体的な提案を示してこられた情報セキュリティ大学院の林教授という、今回のテーマを考える上で最も適任の諸先生方にご報告をいただくことにしております。

それらのご報告を踏まえた上で、後ほど司会の横内所長からご紹介いただくことになるかと思いますが、慶応大学の小山教授、公共政策調査会の板橋室長、そして私がコメンテーターとして先生方の御報告について述べさせていただき、その後今日、お集まりいただいた皆様方からのご意見・ご質問等を併せて、今日のフォーラムで示された課題について具体的な方向に向かった議論をできる限りすることができたらと思っております。

先ほどご紹介がありましたように本日のフォーラムは17時半までという、かなりの長丁場になるかと思いますが、皆さんとともに有意義な時間を過ごしていきたいと思っております。

どうか、よろしくご協力・ご参加いただければ幸いです。簡単ですが、これで私の開会の挨拶とさせていただきます。

【イントロダクション】「憲法学から見た通信の秘密」

東北学院大学法学部准教授　葛西　まゆこ

０　はじめに

私からは、「憲法学から見た通信の秘密」と題し、本日のフォーラムのイントロダクションとして、今までの日本の憲法学における議論や判例動向をまとめてお伝えする。

１　通信の秘密に関する諸規定

まず、日本の法体系において、通信の秘密がどのように規定されているかという点を簡単にご説明申し上げる。

憲法 21 条 2 項は、「検閲は、これをしてはならない」「通信の秘密は、これを侵してはならない」としており、日本国憲法は明文で通信の秘密を保障している。

また、いわゆるコモン・キャリア、すなわち通信事業の事業者が守るべき通信の秘密についても、各種法律によってカバーされており、電気通信事業法３条、４条、６条などがそれに当たる。

なお、本日はフォーラムのテーマに照らし、法律の中でも特に電気通信事業法に焦点を当てることをあらかじめお断りしておく。

２　「通信の秘密」、「検閲」とは何を意味するのか

次に、憲法上あるいは電気通信事業法上、求められている通信の秘密とは何を意味すると捉えられてきたのかという点について、ご説明申し上げる。

(1)　憲法 21 条 2 項にいう「通信の秘密」の内容[1]

まず憲法上の話からだが、憲法 21 条 2 項にいう「通信の秘密」とは、郵便、電話、コンピュータ通信等、およそ通信によるコミュニケーションに関する秘密すべてを指し、例えばメールの内容などのコミュニケーションの内容だけではなく、誰にいつメールをしたのかなどの、コミュニケーションをとったかどうかという存在自体に関する事柄も含むと言われている。

この「通信の秘密」は憲法上、プライバシー権の保護の一環として一般に捉えられてきた。なぜなら、主に外部に発信することを前提とする「表現の自由」とは異なり、「通信の秘密」は内的コミュニケーション過程の保護を通じて、個人間の私的接触を可能にしようとするところが、本来の意義であると憲法学の伝統的理解では考えられているからである。

そのため「通信の秘密」は、非公開でコミュニケーションを行う自由である、通信の自由を論理的前提としている。ネット上の掲示板への書き込み、ホームページの解説など、広く公開を前提とするような公然性を有する通信は、「通信の秘密」の「通信」には含まれず、「表現の自由」の問題になると言われている。その場合でも、権利を侵害された者に発信者情報の開示請求などを認めるプロバイダ法など、通信特有の問題はある。

憲法上の「通信の秘密」とは、以下の３点の内容を保障していると言われている。

---

[1] 以下の説明は、憲法学において通説的見解とされる、佐藤幸治『日本国憲法論』（成文堂、2011 年）320－322 頁に従って、整理したものである。

①公権力により個別的通信の内容及び通信の存在に関し調査の対象とはされないこと。
②通信業務事業者により職務上知り得た通信に関する情報を漏洩されないこと。
③通信の秘密の論理的前提である通信の自由に関係して、通信業務提供者から公正な通信業務の提供を受けることができること。

ただ、この保障内容にも限界はあると言われており、現行法上もさまざまな制約が認められている。例えば刑事手続上の制約としては、郵便物などの押収について定めた刑事訴訟法100条が挙げられる。また、従来からよく議論されてきたものとしては、「通信傍受が認められるのか」という論点があるが、この点は次の判例のところで取り上げることとする。

(2)　電気通信事業法における「通信の秘密」[2]

次に、電気通信事業法における「通信の秘密」とは、どのように捉えられてきたのかという点についてご説明する。

電気通信事業法3条の「電気通信事業者の取扱中」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をいい、電気通信事業者の管理支配下にある状態のものを指す。また「取扱中」に関わる通信の範囲は、伝達行為が終了した後の情報も保護の対象となり、通信終了後にも電気通信事業者が保管している通信内容に関する記録、通信記録なども保護の対象になるとされている。

電気通信事業法においては4条、179条により「通信の秘密」の保護が罰則規定をもって担保されている。ここでいう「秘密」とは一般に知られていない事実であって、他人に知られていないことにつき本人が相当の利益を有すると認められる事実をいうとされる。本人が秘密と考える主観的な秘密が直ちに法的に保護に値するとは言えず、一般人が通常秘密にしようとする蓋然性がある客観的秘密であることが必要だとされている。

原則としては、内的なコミュニケーションである通信については、本人の意思を尊重すべく、電話や電子メールなどの特定者間の通信はひとまず秘密性が推定される。これに対して電子掲示板やホームページに掲載された情報など、不特定の者に対して表示することを目的とした通信の内容は、4条の「対象外」と考えられている。

4条の「通信の秘密」の範囲は、通信内容はもちろんのこと、通信の日時、場所、回数、当事者の氏名、住所、電話番号など、通信の意味内容が推し量れるような事項すべてを含むと考えられている。

「通信の秘密」を侵すというのは、①通信当事者以外の第三者が積極的意思を持って知得しようとすること、②第三者にとどまっている秘密をその者が漏洩すること、及び窃用することも、それぞれ独立して秘密を侵すことに該当するとされている。

(3)「検閲」について

最後に、「検閲」についても多少ご説明させていただく。

憲法上も、電気通信事業法上も、「検閲」という文言がある。日本国憲法上禁止されている「検

---

[2] 以下の説明は、多賀谷一照ほか編著『電気通信事業法逐条解説』（電気通信振興会、2008年）34－41頁に沿ってまとめたものである。

閲」とは何か、という点については、税関検査判決（最大判昭和59・12・12民集38巻12号1308頁）という最高裁の判例が定義を示している。その定義とは、「行政権が主体となって、思想内容等の表現物を対象として、その全部又は一部の発表の禁止を目的として、対象とされる一定の表現物につき網羅的一般的に、発表前にその内容を審査した上、不適当と認めるものの発表を禁止することを、その特質として備えるもの」というものである。ここで注意すべき点は、この判例が言う「検閲」の定義は、かなり狭い射程のものであって、現在まで、最高裁が「＊＊は憲法21条2項が禁ずる『検閲』に該当し、違憲である」という判断を示したことはないということである。

これに対して、電気通信事業法3条の「通信の検閲の禁止」は21条の検閲の禁止とは異なり、事前審査に限定されておらず、より広い概念を意味するのではないかと一般に指摘されている。電気通信事業法3条の「通信の検閲の禁止」は、国家による通信内容の検査や内容を変えることを禁ずる趣旨のものである。

3　「通信の秘密」に関する判例

ここまで、学説上、「通信の秘密」の位置づけや内容についてどのような議論がされてきたのかという点を述べてきた。

次に、これまで問題となってきた裁判例を振り返りたい。「通信の秘密」の範囲に関連するものとしては、郵便で争われたものと電話による通話の聴取が争われたものがあるが、本日は郵便のものについては省略する。

(1)　大阪高判昭和42・12・25判時514号82頁

(1)は、日本電信電話公社（当時）の職員が不必要に他人の通話を聴取したとして懲戒免職された事案である。ここでは、公衆電気通信法5条の「通信の秘密」の射程についても判示された。なお、公衆電気通信法というのは、1984（昭和59）年の電気通信事業法の成立に伴い廃止され法律であり、この5条の規定は現在の電気通信事業法4条に引き継がれており、同じ内容のものと捉えて差し支えはない[3]。

判決は括弧書きではあるが、以下のような判示を行っている。「（ここに「通信の秘密」とは単に通話内容だけでなく誰と誰が通話したかという事実をも指し、またこれを「侵す」ということは通信の秘密を他人に漏らすことだけでなく、必要もないのに他人の通話を聞くことも含まれるものと解すべきである）」。(1)において、「通信の秘密」の範囲は、単に通信の内容という本丸のみに限定されないという点において、先に説明した憲法学説と違いはない。「通信の秘密」の範囲は内容のみならず、場所や回数も含むということである。

(2)　東京地判平成14・4・30裁判所HP

この事案では、電気通信事業者に勤める者が、持ち出し禁止のものを持ち出したという違反行為

---

[3] 念のため、当時の5条の条文の内容は、以下のとおりである。公衆電気通信法5条　①　公社又は会社の取扱中に係る通信の秘密は、侵してはならない。②　公衆電気通信業務に従事する者は、在職中公社又は会社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。

が争われており、電気通信事業法違反の公訴事実のうち、D株式会社関係のものについて無罪を言い渡し、C株式会社関係のものについて未遂罪の成立を認めた事案である。(2)では個々の通信とは無関係の加入者の住所等の基本情報の持ち出しは通信と無関係なので、「通信の秘密」の侵害には当たらないということが示された。その根拠としては、以下に挙げたようなことが述べられている。

ア　D会社関係の電気通信事業法違反の公訴事実について

ここでは「基本情報照会」と題する文書7通及び「料金基本情報」と題する文書1通の合計8通の文書を社外に持ち出した行為が争われた。

・「『基本情報照会』のデータは、特定の加入電話につき、契約者の氏名、電話番号、電話の設置場所、連絡先などの情報を、また、「料金基本情報」のデータは、特定の加入電話につき、電話料金の請求書の送付先や支払状況などに関する情報をそれぞれ記録しているところ、これらはいずれも、個々の通信とは無関係なものとして保管されている情報であり、「通信の秘密」には当たらない。したがって、これらの情報を不正に出力しても電気通信事業法104条違反の罪は成立せず、被告人両名はこの公訴事実について無罪である。［波線は引用者］」

イ　C会社関係の電気通信事業法違反の公訴事実について

ここではC株式会社の移動通信制御装置から、携帯電話合計3台に関する通話中か否かの通話中情報や位置情報を記録したデータ3件をそれぞれ出力し、これらを印字した「加入者データ読出・結果出力画面」と題する文書3通を社外に持ち出した行為が争われた。

・「『加入者データ読出・結果出力画面』のデータは、特定の携帯電話（電話番号）につき、通話中か否かの通話中情報や位置情報や設定されている留守番電話サービス用暗証番号などを記録している。このうちの、例えば当該携帯電話（電話番号）につき設定されている留守番電話サービス用暗証番号については、個々の通信とは無関係なものとして保管されている情報であり、『通信の秘密』には当たらない。これに対し、例えば、位置情報は、もし現在通話中であれば、個々の通話（通信）の受発信場所を示すことになるから、『通信の秘密』に当たることになる。［波線は引用者］」

「関係証拠によれば、本件において『加入者データ読出・結果出力画面』のデータ3件をそれぞれ出力した際、たまたまいずれの携帯電話も通話中でなかったため、前記データ3件のいずれにもC株式会社の取扱中に係る通信の秘密に当たるものは含まれず、結果として、通信の秘密は侵されなかったのであり、未遂罪が成立するにとどまる。［波線は引用者］」

(2)の事案においては、従来どおり「通信の秘密」の範囲を広く設定しつつも、波線を引いた部分に見られるように、文字通りの通信との関係性を重視しながら判断している。

この判決への評価はここでは差し控えるが、この後の議論でも問題となると思われる刑訴法の197条3項から5項の「通信履歴の保全要請」の問題などを考える際に、この判例は参考になる部分があるように思われる。

(3)　東京高決昭和28・7・17判時9号3頁

(3)では、通信の傍受ではないが、電子装置を使用した室内会話の傍受が争われた。詳しく述べると、日本共産党の幹部がとある法令違反容疑で行方を追われていたときに、警察官が共産党員Ａの借りている部屋の隣の押し入れに管理人の承諾を得て盗聴器を取りつけ、隣の部屋の会話をふすま越しに録音したことが問題となった。

裁判所は以下に挙げたような判示を行っている（波線は引用者）。「右聴取は、右捜査目的を達成するに必要な範囲と限度とにおいて行われた限においては、」たとえ第３者Ａの基本権行使に「軽度の悪影響が与えられたとしても、それは右聴取行為に必然的に伴う結果であつてこれを目して職権を濫用するものであるとすることはできない。」なぜなら、「右の範囲と限度内における聴取は合法的な捜査行為として公共の福祉を図る所以」であり、第３者Ａらは「所論基本権等を右の公共の福祉のために利用すべき責任を有するからである。」

判旨のうち、波線を引いた部分が学説上は批判の対象となっている。この(3)の判断に対して批判を加えない憲法学説は皆無であると言ってよい[4]。

その後、通信の傍受に関しては、通信傍受法が制定されるまでの間、刑事訴訟法上の検証として行うことができるのかどうかという点で争われていた。

(4)　最決平成11・12・16刑集53巻9号1327頁

(4)において、最高裁は多数意見において以下の判示を行い、検証許可状による傍受は一定の条件を満たせば、憲法上許されるとした。多数意見は、「電話傍受は、通信の秘密を侵害し、ひいては、個人のプライバシーを侵害する強制処分であるが、一定の要件の下では、捜査の手段として憲法上全く許されないものではないと解すべき」であり「重大な犯罪に係る被疑事件について、被疑者が罪を犯したと疑うに足りる十分な理由があり、かつ、当該電話により被疑事実に関連する通話の行われる蓋然性があるとともに、電話傍受以外の方法によってはその罪に関する重要かつ必要な証拠を得ることが著しく困難であるなどの事情が存する場合において、電話傍受により侵害される利益の内容、程度を慎重に考慮した上で、なお電話傍受を行うことが犯罪の捜査上真にやむを得ないと認められるときには，法律の定める手続に従ってこれを行うことも憲法上許されると解するのが相当である。」とした。

なお、この最高裁の決定には元原利文判事による反対意見も付されている。元原判事は「電話傍受が本件当時捜査の手段として法律上認められていなかった強制処分であり、本件電話傍受により得られた証拠の証拠能力は否定されるべき」であり、「電話傍受は、憲法21条2項が保障する通信の秘密や、憲法13条に由来するプライバシーの権利に対する重大な制約となる行為であるから、よしんばこれを行うとしても、憲法35条が定める令状主義の規制に服するとともに、憲法31条が求める適正な手続が保障されなければならない」と述べている。

(5)　東京地判平成13・8・31判時1781号112頁

---

4 例えば、最高裁判所判事を経験した伊藤正己教授は、この判決は、「人権侵害に対する考慮を十分しないままに容認した例」であり、「それは適切でない」と述べている。伊藤正己『憲法』（弘文堂、第３版、1995年）328頁。また、佐藤幸治教授も、この判決に対して「これは今日では全く支持しえない見解である」と述べている。佐藤・前掲注（1）323頁。

その後、通信傍受法（平成 11 年 8 月 18 日法律第 137 号）が制定され、その合憲性は(5)において国賠訴訟のかたちで争われている。しかし、国賠法上の違法性は認められていない。(5)においては、(4)を引用した上で以下に挙げたような判示を行っている。

「通信傍受は、憲法 21 条 2 項が保障する通信の秘密を侵害し、ひいては個人のプライバシーを侵害する強制処分であるが、これらの権利といえども、絶対に無制限のものではなく、公共の福祉の観点から、捜査のために必要最小限の範囲における制約を加えることは許されるというべきである。そして、重大な犯罪に係る被疑事件について、被疑者が罪を犯したと疑うに足りる十分な理由があり、かつ、当該通信により被疑事実に関連する通話等が行われる蓋然性があるとともに、傍受以外の方法によってはその罪に関する重要かつ必要な証拠を得ることが著しく困難であるなどの事情が存する場合において、傍受により侵害される利益の内容、程度を慎重に考慮した上で、なお傍受を行うことが犯罪の捜査上真にやむを得ないと認められるときには、法律の定める手続に従ってこれを行うことも憲法上許されると解することが相当であり（最高裁平成 9 年（あ）第 636 号同 11 年 12 月 16 日第 3 小法廷決定・刑集 53 巻 9 号 1327 頁参照）、本件法律の内容が憲法 21 条 2 項その他の憲法の一義的な文言に違反しているということはできない」。

(6)　東京高判平成 22・12・8 東高刑(刑事)61 巻 1～12 号 317 頁

なお、直接の憲法論が展開されたわけではないが、(6)は、通信傍受法制定後、捜査官が詐欺の実行行為グループのアジトの上の階の部屋を借りて、その上の階のベランダから下の階のベランダで携帯電話により通話する男の肉声を録音したことが争われた事案である。

(6)においては、今回の録音は通信傍受法にいう「傍受」には該当せず、いまだ任意捜査の範囲を逸脱したものとは言えないため、刑訴法上も違法ではないとの判断が下されている。

4　おわりに

憲法学者の奥平康弘教授は、憲法 21 条 2 項の「通信の秘密」とは、憲法 38 条 1 項の「黙秘権」と同様に、我慢の規定だと指摘する[5]。詳しく述べると、奥平教授は、市民がプライベートに内密にやりとりする情報であればあるほど、国家機関はその情報を取得したいと思うのは自然なことだが、その私的な領域にダイレクトに入り込むことはやめて、必要な情報は、これに代わる他の手段・方法による入手に努めようとする、そういう我慢の規定だと主張している。

通信傍受法は、まさにその我慢のしどころを規定していると思われる。ただ、メールなどの現代的な通信手段は、その通信が侵害された場合、その侵害を当事者が認識することは極めて困難である。通信が侵害されているのか否か、通信の内容が改変されているのか否か、そもそもその通信を発信している（発信した）のは本当に本人なのかなど、ヴァーチャル・リアリティならではの不安感は、疑いだせばきりがない。この特性から、通信に関する法的枠組みは、心配性の市民によって、疑いの目を持って警戒され続けることにつながってくる。

私からは、イントロダクションとして憲法の視点から大枠の話をさせていただいた。本日のフォーラムでは、この難しい問題をどのように考えるべきなのかという点について、多方面にわたる専門の

---

[5] 奥平康弘「いま市民的自由を語る意味」法律時報 71 巻 12 号（1999 年）8 頁。

先生方から多角的に検討されることであろう。本日お集まりいただいた聴衆の皆様も含めて、ご一緒にこの問題について考えていければと思っている。

【基調講演１】「刑事法から見た通信の秘密」

千葉大学大学院専門法務研究科教授　石井徹哉

0　はじめに

ICT社会は電気通信事業法が問題の焦点になってくるので、電気通信事業法を素材にしながらお話しさせていただく。先ほど葛西先生からお話しいただいたように、その前提としては憲法上の「通信の秘密」の問題がある。必要な範囲において個人的な考え方をお示ししたいと思うが、憲法の学者の方々の基本的な見解とは少し異なっており、成文法である憲法の条文に従った理解をしたほうが望ましいのではないかと考えている。

1　憲法21条2項後段と通信の秘密侵害罪(電気通信事業法)

(1)　憲法における通信の秘密

ア　憲法21条とプライバシー保護の二重構造

憲法21条2項では「通信の秘密」は侵してはならないと規定をしているので、やはり憲法上の保障は「表現の自由」の保障との関連づけで考えるべきであろう。そうすると、そこで禁止されている「通信の秘密」の侵害は、基本的にはコミュニケーション内容の探知からもたらされる表現行為の萎縮が主たる焦点であり、その範囲においては憲法21条の強力な保護のもとにある。

これに対して、後ほど出てくる「通信の秘密」全般の問題は、もう少し緩やかなプライバシーの権利の問題であり、我が国における憲法上の「通信の秘密」の理解は、プライバシーの権利であるとしつつも、21条に置かれていることによって、より厳しい制約を課していこうということになっているのではないか。

電気通信事業法における「通信の秘密」の保護の場合に関しても、通信内容の問題は21条の問題としてより強く保護されるべきかもしれないが、その外的な要素あるいは構成要素、通信内容に関わらないような部分に関しては、より緩やかな保護で足りる部分もあるのではないかということが最終的な結論になると思われるので、以下その話をしていきたいと思う。

イ　刑事法との関わり合い＝刑事手続における侵害の許容性

刑事法において「通信の秘密」を侵害する場合はたくさんあるが、基本的に現行の刑訴法の問題としては、刑訴法100条における郵便物等に関する問題、222条あるいは222条の2によるような、通信履歴の差押え、通信傍受の問題がある。こうした手続法的な問題は、国家権力が「通信の秘密」に関わるところを侵害するわけなので、当然これは憲法上の権利制約の関係で議論されるべきだろう。

(2)　実体刑法における通信の秘密

これに対して、現在の特にインターネットが社会基盤となっているところにおいては、より実体法的な電気通信事業法における「通信の秘密」の侵害が問題になってくると考えられる。

実体法上で見ていくと、現行の刑法典においては通常のプライバシー侵害は割と軽く処罰されて

いることが窺われる。例えば刑法 133 条は、信書の開封に関しては１年以下の懲役にしかなっていない。これに対して電気通信事業法 179 条１項は２年以下の懲役で、法定刑がかなり高く設定されている。

電気通信事業法の侵害あるいは違法性の程度は、単に個人のプライバシーを侵害したものとして規定されているわけではなく、それ以外の部分が電気通信の公共性又は電気通信事業に対する社会的信頼をも侵害するがゆえに、より重く処罰されるのだと考えるのが妥当だと思われる。

２　通信の秘密侵害罪の構成要件

(1)　保護法益

電気通信事業法の「通信の秘密侵害罪の構成要件」の保護法益は、第一義的に「通信の秘密」を保護するわけなので、通信当事者のプライバシーの問題としてその秘密を包括的に保護していこうという部分があると思われる。

同時に信書開封罪よりも重い法定刑を科されている部分は、電気通信事業の公益性・公共性に鑑みたサービス提供の適正性、それに対する信頼をより強く保護することが理由となっているのではないかと考えられる。

したがって、電気通信事業法における通信の秘密侵害罪を犯したときに、それが正当化される場合は、両方の利益を侵害してもより多くの利益が保護されるのかどうかという観点が出てくるだろうと思われる。

(2)　客体：電気通信事業者の取扱中に係る通信の秘密

ここで、電気通信事業法の通信の秘密侵害罪の構成要件の中身を示しておこうと思うが、その詳細については先ほど葛西先生からご紹介いただいたので、構成要件に当たらない場合について説明させていただくこととする。

基本的に、「通信の秘密」という場合には、通信の内容、通信の構成要素をもとに考えられていると理解されている。通信であるということで、まさにコミュニケーションがないといけないわけだが、通信に該当しないものが幾つか出てくることになる。

簡単に言うと、通信を前提とせず探知可能な情報は、「通信の秘密」に該当しないことになる。

一つの例として、某社のストリートビューカーによる SSID/MAC address（注）の収集行為がある。SSID/MAC address は、ビーコン的に電波が出されているので、その意味においては通信確立以前の問題であるから、通信を前提としない探知可能な情報であるといえる。さらに、一般的に SSID 等を電波として流しているので、秘密とはならないと思う。

二つ目の例は位置情報の話と関係する。携帯電話は各基地局のアンテナによって通信するのだが、電話事業者は、どのアンテナのそばに携帯電話があるかによって携帯電話端末の位置情報を把握することができる。これに関しては、単に携帯電話がどこにあるかというだけの話なので、携帯で通話をしていない状態の場合は、通信を前提とせず探知可能な状態であると言えるため、「通信の秘密」を侵害したということにはならない。

ただし、その携帯端末を持っている人がどの辺にいるかはわかるので、プライバシー的な情報になると思われる。捜査機関がこれを捜査の証拠として収集しようという場合において、検証令状は

必要だが、それ以上のものは必要ないということになる。

一般の携帯電話事業者が、アンテナの位置情報に基づいて情報を蓄積していることについても、事業者自体が「通信の秘密」を侵害していることになることは少ない。

電気通信事業法は、電電公社、KDD時代の公衆電気通信法の発展としてつくられたものであり、電信電話といった旧態的な通信を前提にしているような法律構成になっている。ところが、現在の電気通信事業はインターネット通信にシフトしているので、どこまでが秘密のものなのかという話が難しくなっている。構成要件は定義的に説明できるが、どこまでが「通信の秘密」なのか、公開を予定されている情報はどこまで秘密に含まれるのかという点が、明確に確定されるべきではないかと思われる。

（注） SSID（Service Set Identifier）とは、無線LANにおいて通信の相手方を識別するために用いられる固有の番号をいう。無線LANは、有線LANと異なり、電波を使って通信するため、複数のアクセスポイントと交信可能となる「混信」状態が発生するおそれがあることから、無線LANのアクセスポイントと各端末にSSIDを設定しSSIDが一致する端末にしかアクセスできないようにすることにより、これを防止することとしたもの。

MAC address（Media Access Control address）とは、LANカード等のネットワーク機器のハードウェアに割り当てられた、通信の相手方を識別するために用いられる固有の番号をいう。

3 通信の秘密侵害罪の違法阻却事由

構成要件該当性を前提として、違法阻却事由としてどんなものがあるかということが問題になってくる。保護法益はプライバシーと電気通信役務の適正性とそれに対する信頼であるから、そういった利益を侵害して構わない場合はどういう場合だろうか。

(1) 捜査機関による行為

捜査機関等による行為は、基本的に35条によって法令行為として許容されている場合になる。憲法に対する適合性、あるいは刑事訴訟法に対する適合性を検討して、それがOKとなれば可能となる。先ほど申し上げたように、アンテナによる携帯端末の位置情報に関しても、令状要件を満たした形で検証令状等によって探知することができると考える。

(2) 事業者により業務上必要とされる行為が正当化される場合

問題は、事業者等、民間の人たちが許容される場合はあるのか。通信の秘密侵害罪の構成要件に該当するけれども、正当化される場合はあるのか。

ア 刑法35条の正当行為とされる場合

この点に関して判例等はほとんどなく、行政監督庁による実務的な運用しかない。全般的な動向を見ていくと、基本的には通信役務の業務に適するような方向での対応に関しては、正当化を考えていこうという傾向にある。

例えばインターネットにおいては、パケットをルーティングして配信していくわけだが、その

際にはパケットのヘッダ情報を見ながら配信する。インターネット通信の役務を提供するということは、つねに「通信の秘密」の構成要素の部分、IPアドレス等の行く先を見ながらでないと配信できない。この場合、一つは通信業務に不可欠であること、もう一つは自動的・機械的になされるので通信内容が探知される可能性は低いことをもとにして、許容されたと考えられる。

さらに、大量の通信パケットが生じて輻輳等が発生している場合は、その障害を突きとめる限度において、「通信の秘密」の侵害は許容されると考えられる。ただし、いずれの場合も特徴なのは、通信内容を探知するわけではなくて、基本的には通信の構成要素の部分を探知して、それによって「通信の秘密」が侵害されているにすぎないと言える。

もう一つは、そのような行動自体が、通信役務を提供する上で必要不可欠、あるいはやむを得ないものであるということだ。そのようなことから、通信役務の公共性に適する事柄に関して、かつ、通信構成要素に関わる侵害しかない場合について、正当化を肯定していると言える。

イ　通信当事者の同意

通信当事者の同意についての議論がよくなされるが、通信の秘密侵害罪が通信役務の適正性とそれに対する信頼を保護していることを考えると、当事者が同意すれば直ちによいということにはならない。完全に個人の利益を侵害する犯罪であれば、当事者の同意によって正当化されるが、本来は社会的な利益を保護するものなので、単に当事者の同意があるというだけでは難しいだろう。通信事業者による業務の一環であること等、通信事業の公共性との観点を何らかの点で満たさないと違法阻却されないと考えられる。

ウ　児童ポルノのDNSブロッキング

児童ポルノのDNSブロッキングについては、時間も限られているので詳細は割愛させていただくが、一言だけ述べさせていただくと、この問題はまずは削除する、発信サーバを遮断することが重要である。それが十分できないときは、その理由を検討すべきである。もし「通信の秘密」を侵害しないと、徹底した削除あるいはサーバの遮断ができないのであれば、「通信の秘密」の侵害の問題を取り上げて検討すべきではないかと考える。

4　捜査機関による行為

(1)　通信傍受

通信傍受の問題に関しては、先ほど葛西先生から判例のご紹介があった。重要なことは、これらの判例において、犯罪の種類に関して重大な犯罪ということでしか限定していない。ところが、現在の通信傍受法は対象犯罪を絞り込んでいる。最高裁の平成11年決定、東京高裁の平成４年判決のような重大な犯罪をどのように限定していくのか。それが現在の通信傍受法の立法において示されている対象犯罪と整合性を有するかということは、もう少しきちっと議論した上で限定されるべきだろうと考える。

現在法制審議会では、その通信傍受に関して対象犯罪の拡大、あるいは通信傍受を伴う立会要件の合理化などの方向性を検討し、立法を提案されている。平成11年決定のような要件があるので、それとの整合性をもう少しきちっと見るべきだろうと思われる。現在の通信傍受法は、この判例よ

り厳しい要件を設定しているのではないかという印象を持っている。

(2) 携帯電話の GPS 情報の探知(令状による場合)

続いて、携帯電話の GPS 位置情報の探知だが、これがアンテナによる位置情報と違うのは、最近の携帯電話は GPS のアンテナを持っており、それによって位置情報を検知できる。そのため、捜査機関が携帯事業者、電話事業者を通じて、位置情報を探知することができるかどうかという問題になる。

アンテナの位置情報については、検証令状によってなされることができると考えられ、GPS の位置情報も同様の要件でよいだろうという感じが一般に持たれる。しかしながら、総務省の個人情報に関するガイドラインでは、令状に基づいて当該端末について位置情報の探知を開始する場合、当該端末に対してこれから位置情報の探知をする旨の通知をしなければならないという規定がされている。

では、なぜそのような通知を要求するのかということが問題になってくる。通常、捜索差押え令状にしても検証令状にしても、令状を持って捜査を行う場合、裁判所の許可のもとで、個人の権利を令状の要件の範囲において侵害してかまわないとされる。ところが、その端末に対して通知をしなければいけないということは、ノーティスの要件が追加されるわけだが、裁判所の令状だけでは不十分なことについての説明が十分にできないのではないかと思われる。

平成 11 年の通信傍受による決定を参照しても、そのような措置は不要だと考えられたと思われる。この場合、通知を要求しなければいけないということは、「通信の秘密」という問題を盾にとり、「通信の秘密」が憲法 21 条に規定されていることを盾にして、形式的に、保障を絶対化しているきらいがあるのではないかと思われる。

この場合は、「表現の自由」と直ちに関わらないところ、無関係に近いところで通常の個人のプライバシーにしかすぎない問題なので、令状によって直ちに実施して構わないのではないかと思われ、通知要件を附加することは、「通信の秘密」の憲法上の保障を過度に絶対化しているところに問題がある。また、刑事手続の要件を法令にあたらない総務省のガイドラインによって規定してよいのかという点にも疑問が残る。

(3) 通信記録の保全要請と事業者による保全行為

続いて保全要請の問題に移るが、これは昨年の刑訴法改正により、刑訴法 197 条 3 項以下に記載されている。概要としては、捜査機関が特定の犯罪行為について通信事業者に対し、通信記録等の保全を要請するものである。それは保全要請だけであって、保全された、あるいは保全要請された通信記録を捜査機関が取得する場合には改めて令状が必要になる。

そういう意味では通信事業者に保全要請をするだけにすぎず、任意処分として考えられているため、任意捜査の一般規定である刑事訴訟法の 197 条に置かれている。これは、当然、通信事業者の側も保全行為に関しては「通信の秘密」の侵害に該当するようなものはないということが前提になっている。つまり、通常業務に必要な範囲において保存した通信履歴を別分けして保全・保護し、削除しないように置くだけにすぎないということになる。

ところが、これは今後の課題なのかもしれないが、一定の範囲内においては、通信事業者が「通

信の秘密」を侵害しないと、保全要請に応えられない場合があるのではないかと考えられる。これが正しいかどうかはご議論をいただきたいと思うが、携帯電話からインターネットに 3G 回線等を使ってアクセスしている場合、事業者によっては IP アドレスを複数の端末で共用している場合がある。

どの端末によってなされたかを特定する場合、たんにIPアドレスがわかっただけでは不十分で、その IP アドレスを使って、いつ、どこにという形の端末情報に対する部分の区分けをしなければいけなくなってくる。そのとき、果たして同じ IP アドレスを使っていた他の端末の所有者の「通信の秘密」の侵害が避けられるかどうかという問題がある。こういったものについて、今後もう少し検討しなければいけないだろう。

あるいは、これは保全要請に直接関わることかどうかわからないが、被害者として見たときに証拠保全をする際の問題として考えることが必要ではないか。特に大量のパケットを特定の IP アドレスに対して送出して、サービスができないようにする DDoS 攻撃のような場合、どういう形で受けたかという証拠保全のために、通信が確立すれば通信履歴が各サーバに残るが、通信の確立がないので残らない場合がある。

最近のクラウド事業では、ハードは一つだが、たくさんの仮想サーバを供している場合がある。特にネットワークがハード１個の場合、どの仮想サーバに対するものなのか精査しようとすると、当該ハードウェアに対して来たパケット全部についてとめて、その中でより分けしていかないと被害者の証拠保全ができなくなってくる。

この場合においても、通信履歴を適切に保存しようとすると、他人の「通信の秘密」の侵害がなされなければいけない。はたしてこういったものが、任意処分といえるか、あるいは正当化要件に該当するかどうかは甚だ怪しくなってくる。こういった問題についても、今後検討すべきでものではないかと考える。

(4)　伝統的な通信形態とインターネットの進展した現在の通信形態の相違

以上のような問題の最終的な解決は何かと言うのは難しいところはあるが、現在の電気通信事業法は、公衆電気通信事業法から発展した形においてなされている。公衆電気通信事業法の場合は電信電話の時代であり、運営主体は電電公社、国際電信電話株式会社といった公企業が主体となっている。国家機関ではないが、それに準じた扱いで考えることができるので、憲法的な要請も十分に配慮しながら通信全般を保護していくことが要請されていたと言える。

さらに電信電話という伝統的な古い通信形態の場合、通信の外形部分、構成要素の部分を保護しておかないと通信内容は保護できなかったと言える。言いかえれば、通信記録及び通信履歴によって通信当事者及び通信の場所をも容易に特定することが可能であり、また、これらから具体的な通信内容を探知することはできなくとも、その他諸般の事情をあわせ、通信内容の話題や概要を推知することも可能であったと言える。

これに対して現在のインターネットの通信は、かつての電話のような形で通信内容の保護がなされる必要があるのかどうか、その点が問題になってくると考える。

一つは、インターネットの仕組み自体がパケットという形で、それが複数の通信経路を自由に通りながら配信できる仕組みになっている。ということは、通信の内容ではなくて構成要素の部分、

周辺の外形的部分に関してみんなが知って構わなくなる。通信内容に関わる部分に関しても、経路の起点起点においては、別に探知するわけではないが、容易に探知できる状態になっている。

私がこの問題を始めたのは1998年か1999年なので15年ほどになるが、そのとき仲間うちで話したことは、電子メールははがきと同じで、どこかの人がサーバを介して見ようと思ったら見られる。隠したければ暗号化するしかないであろう、ということであった。おそらくインターネット全般、通信の内容はそういうものにすぎない。

はがきのようなインターネット通信であれば、例えば、メールサーバに蔵置されている電子メールについて、刑訴法の100条の信書の差押えと同じような捜査方法も十分にあり得る。それより厳しい電話と同じような保護をしていくことが果たして適切なのかどうか、これは疑問だと思っている。

インターネットの場合、通信の構成要素、外形部分の問題と、どこで切るかは精査しなければならないが、通信内容の問題は厳密に切り離して、内容部分はコミュニケーション内容の問題であるから強く保護しなければならないが、外的な構成要素の部分については通常のプライバシーの保護と考えてもいいのではないか。

もう少し言うと、インターネットはバーチャルネットワーク、バーチャルリアリティと言われるが、バーチャルは仮想ではあるけれども、まさにリアリティ、現実であって、現実社会の延長線であり、我々は手足の代わりに通信を介して行っているにすぎない。インターネットの通信履歴は、通常、人がどの地下鉄に乗ってどの駅で降りたかというのと同じ扱いで考えてもいいのではないか。もう少し立法的に言えば、インターネット時代に即した形で、「通信の秘密」を考えるべきときが来ていると思われる。

【基調講演２】「サイバー犯罪捜査における事後追跡可能性と通信の秘密」

警察大学校刑事教養部長（当時）、現慶応義塾大学総合政策学部教授
四方　光

０　はじめに

私は昨年の 10 月まで警察庁の情報技術犯罪対策課長をさせていただいていた。かつて私が担当させていただいたサイバー犯罪において、我々は犯罪が発生してから犯罪を追っていくのであるが、これができないと大変困ったことになる。この事後追跡可能性という問題と、本日のメインテーマでもある「通信の秘密」の問題について、犯罪の現状等も併せてご説明したいと思う。

内容は３点。サイバー犯罪の現状について、概略、最近の情勢を簡単にご紹介したいと思う。それから事後追跡可能性、これは捜査の死命を制するものだが、どういうところで問題になってくるかということについてご説明する。それらの現状を踏まえ、具体的にどうしていったらいいのかは難しい問題であるが、検討していただかなければいけない課題、方向性について私見を申し上げたいと思う。

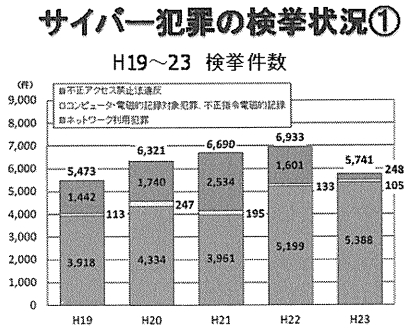
１　サイバー犯罪の現状

(1)　サイバー犯罪の検挙件数①

まず、サイバー犯罪の現状だが、会場の皆様の中には詳しい方もおられるので、既に何度も聞いた話になるかもしれないが、サイバー犯罪はこの数年、基本的に増勢傾向にある。リアルの世界での犯罪は、この 10 年近くずっと減少の一途をたどっている状況だが、サイバー犯罪は検挙件数ベースではあるが基本的に増勢である。

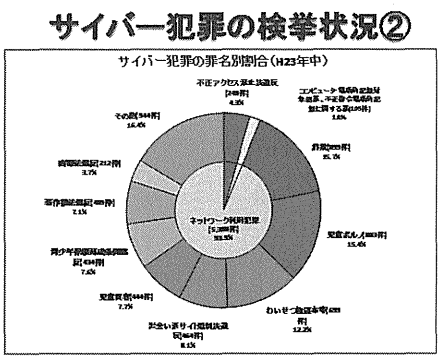
サイバー犯罪は法律上の用語ではないが、警察では次の３種類に区分している。不正アクセス禁止法違反、２番目のカテゴリーとして、刑法典にコンピュータ・電磁気的記録関係の幾つかの犯罪が書かれている。そして、インターネットあるいはネットワークを犯罪の主要な手段として使っているさまざまな犯罪をまとめて、ネットワーク利用犯罪というふうに呼んでいる。

サイバー犯罪は基本的に増勢だが、不正アクセス禁止法違反の検挙は、23 年は非常に減っているではないかと怪訝に思われるかもしれないが、これは検挙のノウハウとの関係でこういうことが起こっている。平成 22 年までは、インターネットオークションに対して ID・パスワードを不正取得して、不正アクセスをして詐欺を働くというパターンが多かった。それについては、警察の検挙ノウハウを使った検挙活動とオークション事業者のご努力もあり、大きく減っている。当然、不正アクセス自体は暗数の部分は相当あるはずだが、得意技としていた事象がなくなり、検挙件数が減っている。



(2)　サイバー犯罪の検挙状況②

先ほど、ネットワーク利用犯罪にはさまざまなものがあると申し上げたが、その内訳は、詐欺、児童ポルノ、猥褻物頒布、出会い系サイト規制法違反、児童買春、淫行条例違反、著作権法違反、商標法違反等々となっている。ただ、これは検挙ベースなため、著作権法違反や商標法違反については暗数が実態より多い可能性はある。



（事例１）　遠隔操作ウイルスによる威力業務妨害事案

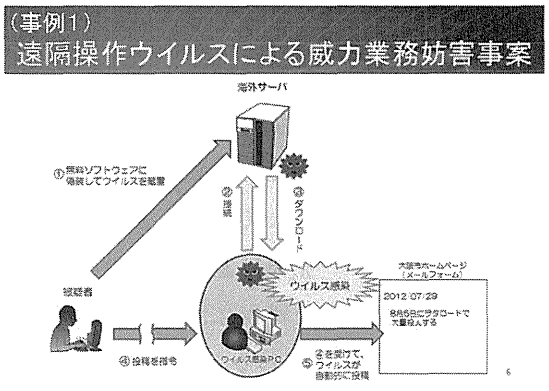
最近話題になった事例について、捜査中のものもあり詳しくは申し上げられないが、幾つかご紹介したいと思う。

昨年の後半から非常に話題になり、ご迷惑もかけた遠隔操作ウイルス事案の基本的な構造だが、一時期犯人とされてしまった方々が海外サーバに増設された掲示板などにアクセスして、そこでウイルスに感染してしまうというものだ。

ウイルスを使ってパソコンを乗っ取るという現象なわけだが、これは前からほかの犯罪でもしばしば見られていた。ただ、この事案の特徴的なところは、パソコンを乗っ取っておいて、その乗っ取られた人が犯人であるかのように工夫を凝らして、殺人予告等々を行うという構造になっている点である。

(3)　遠隔操作ウイルス事案の特徴

さらに特徴を言うと、現象事案としてあらわれたのは、大量殺人等を示唆する掲示板上の書き込みであり、先般の検挙罪名ではハイジャック防止法等に当たるものであった。リアルな世界の人の生命・身体の安全に直結する可能性があることを本当にしようという人間だとしたら大変なことだということで、警察の捜査は相応の態勢をとって行い、また、予告の対象になった事業者や公的機関等も業務の妨害を受けることになる。



この手の書き込みは昔も現在もいろいろあるが、特に話題になった秋葉原の通り魔事件は実際にやってしまったという事案である。この手の書き込みがしょっちゅうある中で、本当にやってしまうというのはそれほどあるわけではないが、万が一実際にあったらいけないということで、警察ではこの手の書き込みの検挙を一つ一つ丁寧にやっているところである。

2 番目は、一般ユーザーをウイルスに感染させ、パソコンを乗っ取るということをやっている点である。後でまた別の事案でもご紹介するが、これは少し手の込んだサイバー犯罪の常套手段の一つでもある。警察のサイバー犯罪の捜査力が追いついていないのではないかというご指摘をいただいているが、この種の乗っ取りがあることについては警察も前から認識していた。

３番目は、乗っ取った人を犯人に仕立てている点である。このことが不可能ではないということは想像することができたかもしれない。しかし国際的に見てもそれほどあちこちにあって、こういうことに気をつけろという話にはなっていなかったと認識している。結果的にこのようなことになり、誤認逮捕された方々には大変申しわけないが、当時としては、乗っ取った相手を犯人に仕立てるというところまでは想像がつかなかった。

４番目は、既に使われ始めていた技術であるが、高度匿名化技術を使っている点である。警察の追跡がほぼ不可能と言われる、Tor（トーア）という技術を使っている。

今回は恐らくは愉快犯のようなものだった可能性はあるが、技術的には金銭目的等いろいろな犯罪に使い得る手口であり、今後もこの手の犯罪に対処していかなければならないという認識を持っている。

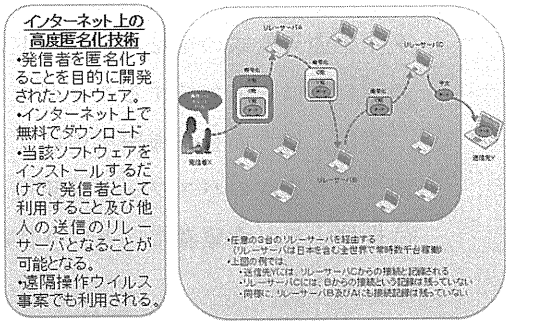
遠隔操作ウイルス事案の特徴

- **掲示板上に大量殺人等を示唆する書き込み**
- **掲示板等における通常のやり取りを通じて、ウイルスに感染させ、他人のPCを乗っ取り**
- **当該他人を犯人に仕立てる**
- **高度匿名化技術等を悪用**
- **愉快犯的な動機のようだが、技術的には他の犯罪にも悪用可能**

(4)　インターネット上の高度匿名化技術

Tor（高度匿名化技術）であるが、ウイルスを載せた掲示板なり乗っ取ったパソコンに犯人が直接に指令を出すと、IPアドレス等の追跡捜査によってわかってしまう。それを防ぐために、世界中で数千と言われている高度匿名化技術に賛同しようという人たちがサーバを提供して、機械的にランダムに三つぐらいとって、そこの経路をたどっていくという仕組みになっている。しかもたどった痕跡を一回一回消していき、暗号化もかかっているということで、最初の被害を受けたPCから１個目はたどれるが、その後が今の技術では全くたどれない、そういう仕組みになっている。

インターネット上の高度匿名化技術



一昨年、警察庁の私的諮問機関である総合セキュリティ対策会議でも、事後追跡可能性の問題の一つとして高度匿名化技術が取り上げられてはいた。しかし、日本国内でも賛同してサーバは立っているらしいが、全世界で行われているのが実態であり、これは一挙には解決できない問題である。

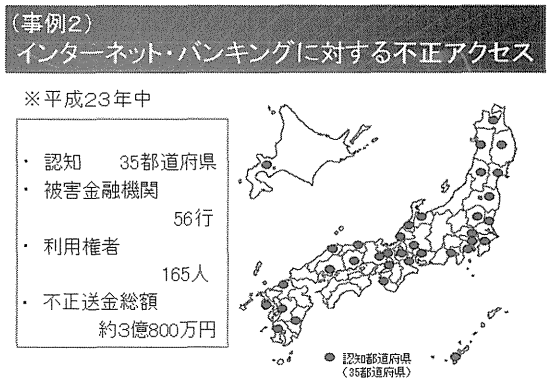
このTorだが、もともとは善意でつくられたという話だ。政治活動の自由が制限されている国において、「通信の秘密」を確保して、匿名による表現の自由を守るために、世界各国の善意の技術者等々が「私のサーバを使っていいですよ」ということで、この仕組みができたということである。

ただ、詳細は承知していないが、外国では既に犯罪に使われ始めている。一昨年、我々が研究したときには、日本国内の犯罪ではそんなに使われていなさそうだが、そのうち使われるかもしれないから考えなければいけないという段階であったのだが、実際に重大な犯罪に使われてしまったということである。

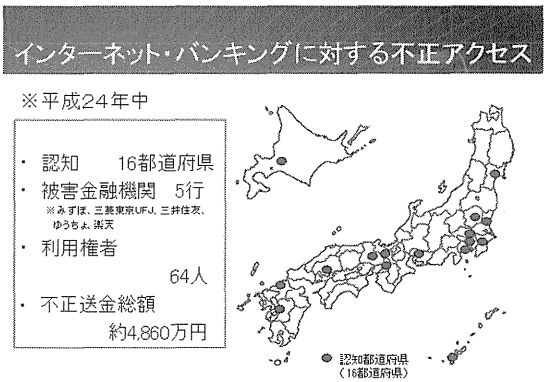
（事例２）インターネット・バンキングに対する不正アクセス

昨年、一昨年にかけて、インターネット・バンキングに対する不正アクセス・不正送金事案が多発した。平成 23 年中、35 都道府県で不正送金の総額が 3 億 800 万円、次の 24 年は少し減ったが 16 都道府県で 5000 万円近く被害があった。

この手口も、一般ユーザーにウイルスを感染させたのではないかと見られている。金融機関のメインコンピューターにクラッキングで直接入り込むのはなかなか難しい。預金者である一般の個人や企業のパソコンにウイルスを感染させて、インターネット・バンキング用の ID・パスワードを盗る。その ID・パスワードを使って預金者になりすまし、別途用意しておいた口座に不正送金をして、コンビニの ATM 等々から預金を引き出すという手口である。

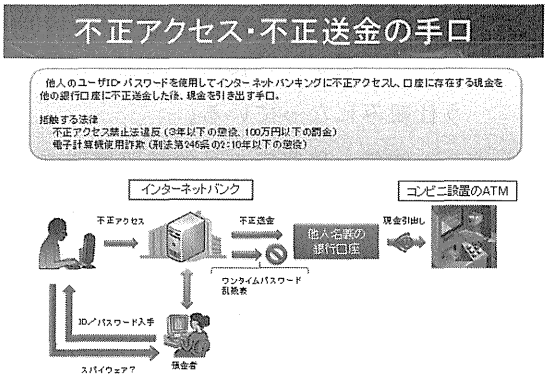


この手口に対して大手銀行は、ワンタイムパスワードといって１分ごとに暗証番号が変わる第２の暗証番号を使ったり、乱数表でその都度打ち込んだりということがあるかと思う。このタイプの可変式の第２パスワードがあると、この手口には一応対抗することができる。



実は、地方の金融機関を中心に多くの金融機関では可変式のパスワードが採用されておらず固定式だけ、あるいは可変式を任意のサービスでは提供するが希望者だけという仕組みになっているところがある。そこで、こういう被害があるということだ。

少し脱線するが、乱数表やワンタイムパスワードでブロックされるということで、もう少し手の込んだ不正アクセス・不正送金が出てきている。例えば、乱数表の記載をそのまま打ち込ませてしまうフィッシングも出ており、それによってブロックを越えてしまうという手口も起こっている。

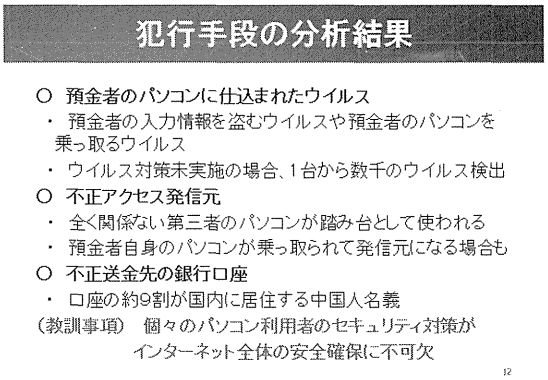


(5)　犯行手段の分析結果

この種のウイルスはウイルス対策ソフトが有効だが、ウイルス対策ソフトを使わないとどうなるか。この捜査を行っていく中で我々も驚いたのだが、24 時間接続していてウイルス対策は何もしていなくて踏み台にされた方のパソコンを見ると、1 台から数千のウイルスが見つかった。パソコンがよく動いていたなと思うような事例もある。不正アクセスの発信元については、ウイルスによってパソコンを乗っ取り、そこを踏み台にするということも起こっている。

我々が痛感したのは、電子商取引等々をされている事業者のサーバのセキュリティの向上も大切

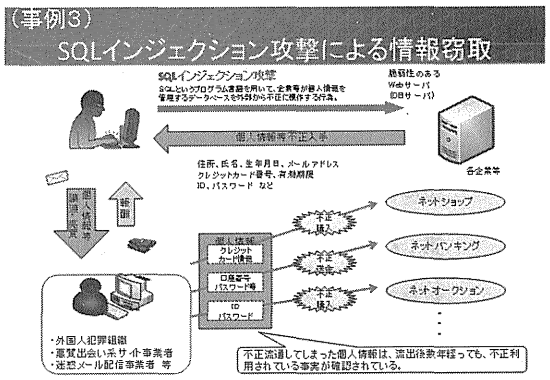
だが、個々の利用者のパソコンのセキュリティを考えていかなければいけない時代になったということだ。

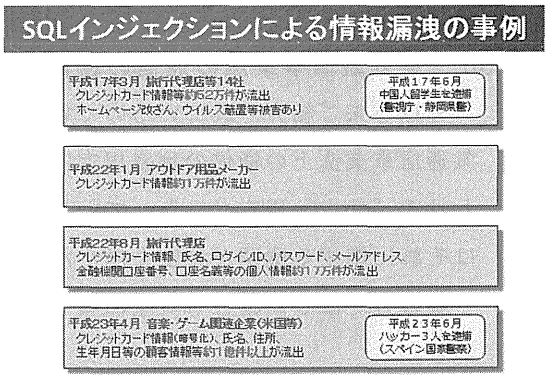


（事例３）SQL インジェクション攻撃による情報窃取

事例３の SQL インジェクション攻撃による窃取は、技術的には比較的簡単な技術と言われている。事業者のサーバの不正アクセスに対する弱点を見つけて、そこから入ってクレジットカード番号等々を盗むというものだ。この弱点を見つけるプログラムがあるらしく、機械的に弱点のあるサーバを見つけていき、そこからクレジットカード番号を盗っていくということが横行しているようだ。

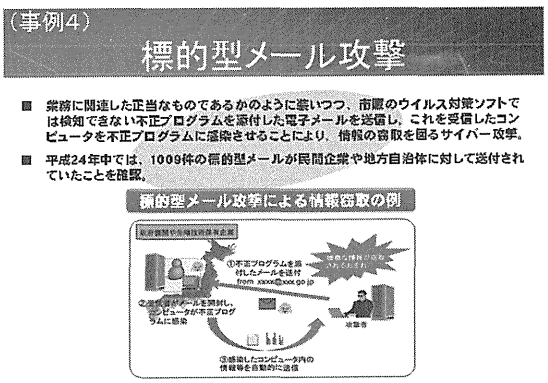
最近のクレジットカード番号による電子商取引は相当な数があり、大手だけではなくて中小の事業者も被害に遭った場合は相当数の番号が盗られている。SQL インジェクションやウイルスによる窃取等を考えると、固定式の番号だと、いつ盗られてもおかしくないような時代になってきている。

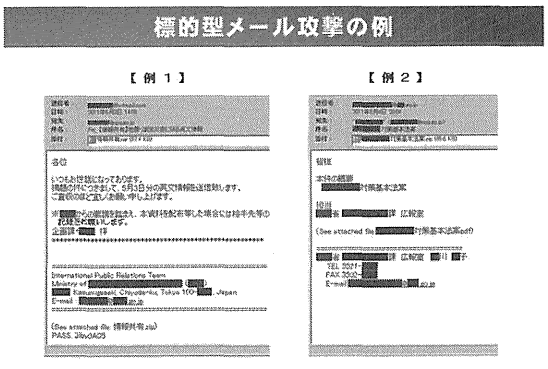




（事例４）　標的型メール攻撃

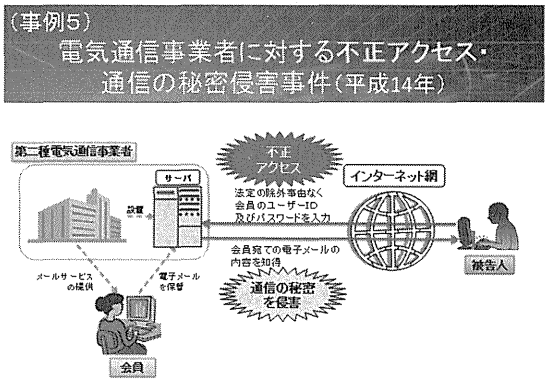
一昨年ぐらいからサイバー攻撃で話題になっているのが、標的型メール攻撃というものだ。知り合いのふりをしてメールを開かせてウイルスに感染させ、パソコンを乗っ取っていくという手口だ。迷惑メールのように誰か知らない人から来たというのではなく、近しい人、会ったことのある人からメールが来て、そこからウイルスに感染させていく。ウイルスによって乗っ取っていき、個人に貸与されたパソコンから組織全体のメインサーバへ侵入していくというものだ。





（事例５）　電気通信事業者に対する不正アクセス・通信の秘密侵害事件（平成 14 年）

事例５は少し古い事件で、これまでにご紹介したものに比べると大きく話題になったわけではないが、今回のテーマに関連すると思われるのでご紹介する。



メールサーバを持っている通信事業者は、大手以外にも同種の事業を行っているプロバイダはたくさんある。そこに不正アクセスをして、サーバ全体を乗っ取るというより、ある特定会員の ID・パスワードを盗って、当該会員の電子メールの内容を見たというものだ。多数の顧客・ユーザーの電子メールの中身を見たという話ではない。しかし、ID・パスワードが電子メールのものであった場合、当該ユーザーの電子メールの内容は通信事業者の扱っているところから盗ることができるという事案である。

(6)　電気通信事業法の通信の秘密規定

先ほど来ご紹介されているので省略するが、電気通信事業法上の通信の秘密規定に関しては、いわゆる「何人も規定」になっている。国、あるいはそれに準ずる機関が秘密を侵すだけではなくて、一般の方が侵した場合も対象になるという規定である。

電気通信事業法の通信の秘密規定

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。

第179条　電気通信事業者の取扱中に係る通信（第百六十四条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

19

2　サイバー犯罪捜査における事後追跡可能性の重要性

サイバー犯罪の特徴については、過去の研究者の方々の分析も参考にして五つの点を挙げるのだが、本日は匿名性、事後追跡の困難性について述べたいと思う。

サイバー犯罪の特徴

- **匿名性、事後追跡の困難性**
- **瞬時性、大量性、空間的無限定性**
- **分散性**
- **「情報性」**
- **専門性、技術性、「進化性」**

19

(1) サイバー犯罪捜査における事後追跡可能性

これは、サイバー犯罪が起こった後、犯罪捜査をどのように行っていくかという典型的なパターンを描いている。被害者のサーバなりコンピュータのログを見て、どこから通信が来たかをさかのぼっていくという捜査をして、攻撃者なり犯人のところにどのようにたどり着くかという理念図である。

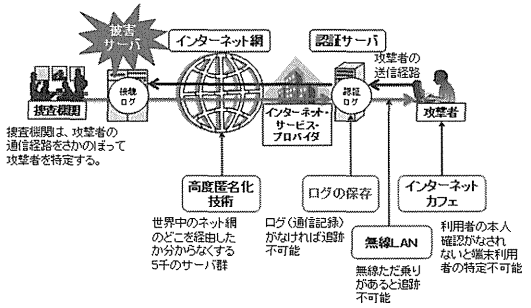
そこには幾つものハードルがあって、その一つとして高度匿名化技術（Tor）がある。Tor ほど手の込んだものでなくても、海外には犯罪者を顧客にしているプロキシサーバという、追跡をしにく

くしている中継サーバを使う場合もある。

次の段階が、今日のテーマの一つにもなる、通信プロバイダの段階でログを保存していなければ、次をたどることができなくなるという問題がある。

さらに、通信プロバイダに入っていく途中で無線LANのただ乗りがある。最近は少なくなったと思っているが、かつて無線LANのセキュリティが弱かった時代には、一般家庭や企業の近所までパソコンを持っていき、そこからただ乗りで入っていく。実際にIPアドレスの捜査で、この家庭の誰かがやっているのではないかということで張り込みをかけても、それらしい人がいない。周辺をたどっていくと隣の駐車場の車の中でパソコンをぱちぱちやっている者がいて、それが被疑者だったという事例もある。

サイバー犯罪捜査における事後追跡可能性



もう一つ、これは基本的に通信回路と機械とを結んでいく捜査のため、最後の端末のところでは誰が使っていたかという、リアルの世界の捜査が必要となる。インターネットカフェの中には本人確認をしていないところもあって、どこの端末から来たかというところまではわかるが、誰が使ったかはわからないということもたまに生じる。

(2)　サイバー犯罪条約におけるログの保存条項と諸外国の対応

次に、ログの保存の問題を中心に述べたいと思う。ログの保存については、各国ともログが欲しいということで、サイバー犯罪条約の中にログの保存に関連する条文があり、大まかに言うと二つの方式で対応している。

一つは、アメリカあるいは日本の改正刑事訴訟法の場合のように、犯罪の嫌疑が生じた後で、捜査機関がプロバイダにお願いしてログを保存してもらうというタイプである。もう一つはEU指令。EU加盟国全部ではないが、通信が行われた後6カ月から2年の間ログの保存義務を課す法律をつくるようにという対応の仕方がある。

改正刑事訴訟法の規定については既に紹介されているので省略する。

サイバー犯罪条約におけるログの保存条項と諸外国の対応

サイバー犯罪条約第16条
（蔵置されたコンピュータ・データの迅速な保全）

→ アメリカ・日本（改正刑事訴訟法）の対応
犯罪の嫌疑が生じた時点以後のログの保全要請

→ ヨーロッパの対応（EU指令）
通信実施後6ヶ月－2年間の一律のログ保存義務
（cf ドイツにおける保存規定の違憲判決）

22

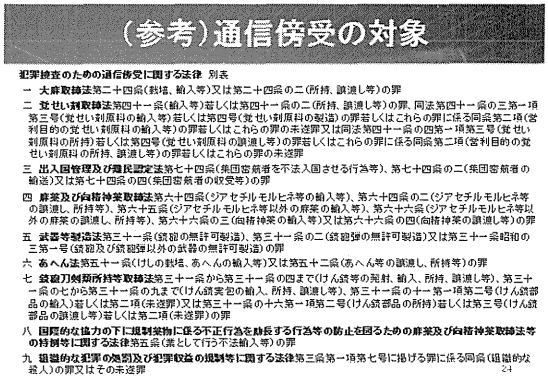
改正刑事訴訟法のログ保存要請規定

刑事訴訟法第197条
3 検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。
4 前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。
5 第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。

23

（参考）　通信傍受の対象

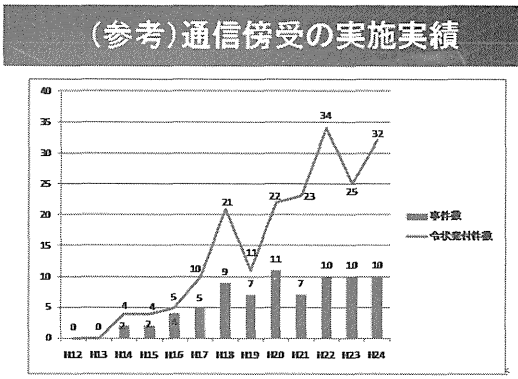
ログの保存がなされないと、犯罪が起こってから後ろをたどるという典型的な捜査はできなくなる。ではどうするかという大きな問題がある。一つは。まさしく通信がされているその場で押さえる。リアルの世界でいくと邀撃捜査のようなものになるが、そこで通信傍受が話題になってくる。

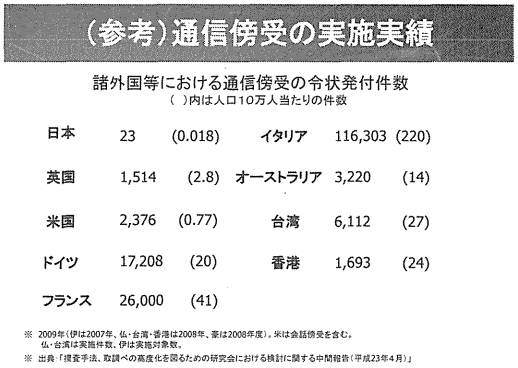


通信傍受については、大きく分けると「薬物関係」「銃器」「集団密航」「組織的な殺人」の４類型と理解されている。

（参考）　通信傍受の実施実績

次に通信傍受の実施実績である。私の知る限り、今まで日本国内ではサイバー犯罪関係の通信傍受はされていないはずなので、これはリアルの世界の犯罪だと思っていただいていい。国内での実施実績は徐々に上がってはいるが、諸外国と比べると桁がかなり違うことをご覧いただきたい。このような状況について、仄聞するところによると、法制審議会などでご議論いただいているようである。本日のテーマの一つでもあるので、ご参考に各国との比較をさせていただいた。

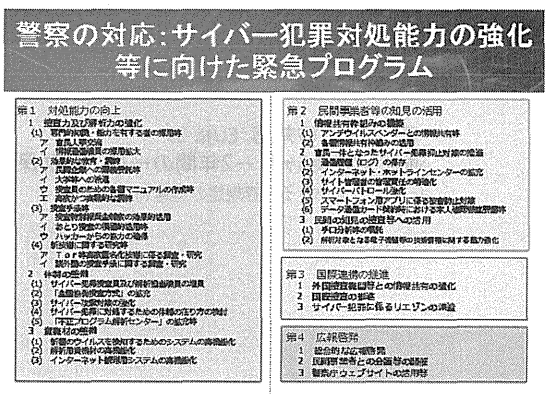




3　今後の課題

(1)　警察の対応：サイバー犯罪対処能力の強化等に向けた緊急プログラム

今後の課題だが、現行法令のもと、できることを一生懸命やろうということで、昨年の暮れ近く、警察庁では「緊急プログラム」というものをつくった。まず第１は、捜査機関の対処能力を向上させなければいけない。専門家をよりたくさん育成し、トップレベルの捜査力を上げていくとともに、裾野を拡大し、また機材を整備していく。



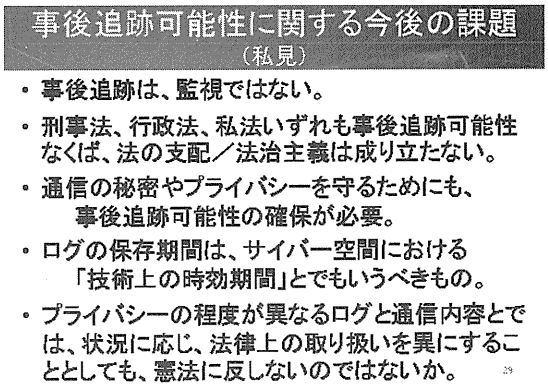
第２に、民間事業者との協力関係の更なる強化だ。昨年の春に私は担当課長として不正アクセス

禁止法の改正をやらせていただいたが、その過程において、従来と比べるといろいろな事業者の方々と意見交換をする機会が随分と増えた。その意味ではよかったが、今後のことを考えると、もっと緊密な情報交換や協力体制が必要だ。

それから、国際連携もあるだろう。また、国民の皆様方あるいは事業者の方々への啓発ということを柱にしたプログラムがある。

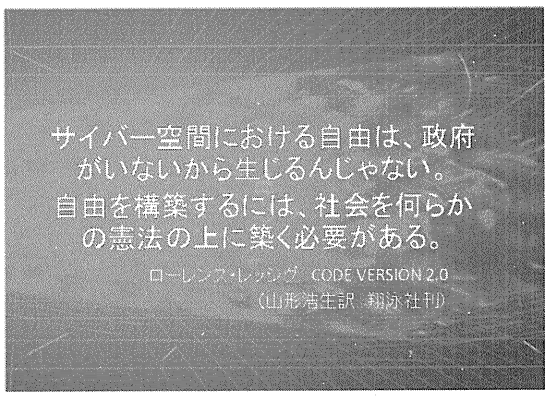
(2)　事後追跡可能性に関する今後の課題（私見）

これは現行法制上でやれることを全部やろうという話だが、今後の法制の在り方を考えると、私の個人的な考え方ではあるが、次のようなことを、通信ログの保存の問題を中心に先生方に考えていただきたい。



一つは、警察がサイバー犯罪の捜査を強化すると言うと、監視社会の到来だと言われる人もある。しかし、基本的に事後追跡は、犯罪が起こってからさかのぼるので、常時人々の活動を監視するということとは質的にだいぶ違っているということである。

そもそも憲法のもとで各種の法体系全体が、捜査機関でも行政機関でもそうだが、法の実施なり施行をして紛議があったら裁判所に持っていくということをする。事後追跡可能性がなければ、法を実効たらしめる枠組みが全部機能しなくなるのではないか。実際に、Tor などが犯罪に使われる、あるいはログがなくて捜査ができないということをしばしば体験すると、そのように非常に強く感じるのである。



先ほど事例５で申し上げたが、国家対私人ではないが、電気通信事業法上の「通信の秘密」という意味では、「通信の秘密」を侵害するような犯罪がサイバー犯罪として行われている。あるいは、プライバシーを侵害するような犯罪がサイバー犯罪として行われている。それを防御する、あるいは検挙していくことも、事後追跡可能性がないとできないのである。

ログの保存期間は、一種の技術上の地平線というか時効期間のようなものだ。先ほど石井先生からもお話があったが、ログの記録は解釈上、「通信の秘密」の一つかそうでないかという議論もあるとは思うが、少なくとも通信内容とは違う。立法論での法律上の取り扱いが違ってもおかしくないのではないかと、個人的には思っている。

サイバー空間における自由は、政府がいないから生じるんじゃない。
自由を構築するには、社会を何らかの憲法の上に築く必要がある。
ローレンス・レッシグ

サイバー上の監視社会を気にされている、アメリカの憲法学者ローレンス・レッシグの有名な本がある。先ほどのログの保存の問題ではないが、自由をしっかり守っていくためには憲法の上にネット社会を築く。その憲法の上に築くためには、事後追跡可能性のようなものが必要なのではないか。このことが、私の申し上げたかったことである。

【基調講演３】「より成熟した安全法に向けて」

フライブルク大学法学部教授　ラルフ・ポッシャー　Ralf Poscher,
＜編集＞警察政策研究センター教授　稲垣吉博

自由主義社会において、安全法制は特有なアンビバレンス（両面価値）によって特徴づけられている。つまり、安全法制は自由と法益の保護に貢献するものでありながら、それが強化されすぎたり濫用されたりすると、逆に自由や法益を脅かしかねない。過度の監視や国民の基本権への介入が、そもそも守るべき価値や生活形態を圧殺してしまう可能性がある。

治安当局による国民の完全監視や恣意的な介入という権限は、花開くべき自由を芽のうちに萎れさせ、操作的に利用可能な支配知（注：権力者のみに与えられ、その権力志向に役立つ知識）をつくり出しかねず、そうした支配知は個々人の自由のみならず、民主的国家の集団的な自律性をも破壊する可能性を持っている。

私が、今日のこの短い講演の中で「より成熟した」安全法制のコンセプトとして紹介したいと考えているのは、そのようなアンビバレンスを自覚した安全法制、つまり自らの中に含むマイナス面をきちんと自覚し、それを崇高な目的を掲げて隠したりするのではなく、自らのアンビバレンスを真摯に受け止めるような安全法制ということである。

権力分析の中でミシェル・フーコーは、権力の戦略に対し、常に対抗権力や対抗戦略も発展してゆく点を指摘した。より成熟した安全法制というものは、対抗戦略の発展を漫然と社会のイニシアティブに委ねたりはしない。社会では、対抗戦略はしばしばアウトサイダー性、違反行為、それどころか犯罪行為とも結びつけられているからである。より成熟した安全法制は、自らの意図せざる結果に対してあらわれる対抗戦略をも共に考慮し、安全法制自体の中にそれを組み入れる試みをするものである。

ご報告したいのは、より成熟した安全法制という難問にきちんと向き合おうとしているように思える、ドイツの安全法制のさまざまな傾向についてである。

ドイツでも紆余曲折の経緯があったが、幾つかの事例をご紹介したいと思う。日本は 1995 年に東京の地下鉄サリン事件を体験したが、ドイツでは最近、大規模なテロ攻撃は起きていない。しかしそのドイツでも、安全法制をめぐる政策では当初、過激な反応に陥る傾向があった。

それは無理もないことかもしれない。初期には大規模な措置を通じて実行力を誇示したいという願望もしばしば混じっており、実際にその一部は政治的行為を象徴するものでもあったからだ。初期の段階において、意図せぬ結果に対する対抗戦略についても同時に考えろというのは、無理な要求だったかもしれない。

そこで過剰反応を抑制する後づけの機関が必要となった。それは、意図せざる結果について指摘し、熟慮のプロセスを始動させ、そのための基準を定めることができなければならない。ドイツでの安全法制上の議論において、この役割は連邦憲法裁判所によって担われることになった。

さらに立法府においてもこの難題に取り組み、一方では判例に対する反応において、また他方では自らの理念やコンセプトを用いて、より成熟した安全法制の発展に影響を及ぼしてきた。

今日のフォーラムでは特に通信の監視がテーマとなっているので、まず通信の様式が激しく変化しているにもかかわらず、なぜ安全法制上のアンビバレンスが存在し続けているのか、そしてなぜ「プライ

バシーの終焉」（注：ネットワーク化された社会にプライバシーは存在しないという考え方）などと言われるこの時代にもかかわらず、緊張関係が一向に解消されないのかの2点についてご説明したいと思う。

その後で、成熟した安全法制が正真正銘の難題である理由について、簡単に述べたいと思う。その後になるが、講演の主眼である憲法解釈学上の発展のなかに見られる戦略について述べることとする。この戦略は、安全法制の難題にこたえるためのもので、以下に申し上げる三つの要素に基づいている。

1 新たな監視ツール

まず一つ目が、新たな監視ツールである。国際テロリズム及び組織犯罪との闘いの中で、ドイツでも情報技術の分野において、警察の捜査手段は格段の進歩を遂げている。一例を挙げると、大盗聴（注：広場や駅などの公共の場ではなく個人宅等私的領域まで拡大して行われる傍受のことをいう）、オンライン捜索、通信の傍受、通信データの保全、衛星による GPS 位置測定、携帯電話の位置測定を用いて人物の位置確定ができる IMSI キャッチャー、車両登録標識の自動捕捉、ビデオ監視、そして、従来からあるスクリーン捜査・ラスター捜査といったツールである。

こうしたさまざまなテクニカルツールにより、これまで予想だにされず、ましてや知る由もなかった規模での監視措置が国家には可能になった。もしもすべてのツールが投入されるならば、治安当局には国民の生活活動がほとんど丸見えとなる。

オンライン監視などと比べれば、まだ全く無害に思われるメールボックスへのアクセスは、一見すると古き良き時代の郵便物押収と同等のように見える。しかし、完全に新たな質を持つに至っている。関係者の通信内容全体へのアクセス、しかもすべての送受信メール、コンタクト、ネットワークを含み、生涯の全期間にわたるアクセスとなると、これは全く別の質を持つものになる。

このことが明確になったのは、遅くとも、アメリカの CIA 長官であったペトレイアス将軍の事件（注：女性問題で辞職を余儀なくされた事件）のころからと考えることができる。この事件は、さまざまなコンタクトを追跡していくと、米軍指導部の中枢にまで入り込んでしまう危険があったため、追跡を途中でやめてしまったというものである。

2 情報の自己決定と自律性

二つ目の要素は、情報面での自己決定と自律性である。情報の追跡が可能ということは、よく言うプライバシーの終焉を支持する人ならば、場合によっては許容できるのかもしれない。ただ、終焉したと考えるのは現実的ではないと思う。とりわけデータ保護を通じて確保されるプライバシーは、厳格な解釈での自由の概念と極めて緊密に結びついている。基本法が保護する自由とは、単なる選択者（chooser）の選択の自由だけではない。基本権保持者の自律性を意味するものである。つまり、自らの歴史に鑑み、自らの人生設計を背景に、自ら下した決定を、自ら理由づける人物としての自律性。これが、基本法が保護する自由となる。

しかし、個人データへの無制限のアクセスによって、他人に対するイメージが操作され、ゆがめられ、さらに不透明となり、固定化されてしまいがちである。そのような他人のイメージは、人としての自律性として理解される自由のさまざまな条件を侵害してしまう。

それらは効果的な自己表現を困難なもの、それどころか不可能なものにしてしまい、さらには人生

設計の可能性を制限してしまう。流布した人格についてのデマのせいで特定の職業分野でチャンスを失ってしまった人は、場合によっては、自らの人生設計を修正することになってしまうだろう。そうなると、デマがなければ可能であった人生設計に基づいた行動の可能性を考えることはないだろうし、人としての自律性を結局は失ってしまうことになる。

過度な監視は、それ自体、法律違反に対する正当な処罰であっても、さまざまなデメリットと結びついている。それゆえ、自己検閲（注：周囲に対する不安から自身の思想・行動・作品などを自ら統制すること）が行われるのである。それらのデメリットから守るために、情報上の自己決定権（注：自己に関して誰が何を知り、何を利用するかについて認識し、それを自ら決定する権利）がある。

当然、情報上の自己決定権は、法律違反に対する懲罰から免れるものではない。しかし過度の監視は、結果として、自律性という厳格な意味での自由を制限する、さまざまな形の自己制限をもたらしてしまう。要するに、人間の尊厳という構想において、外的に自由であるだけではなく、内的に自律的な人間と定められている私たちの自律性は、合法的なアプローチによっても脅かされかねないのである。

ただし、自律性は程度の問題となる。というのも、人生設計のための行動の余地は、そのときの時代や社会の歴史的偶然性によって、絶えず制限されているからだ。このように、自律性は相対的であるため、行動の余地のありさまは変化し、小さくなったり大きくなったり、時代によって変化する。現在はプライバシーの終焉と予言されるようになって、個人データの自由な取り扱いが可能になってきた。そのため、この動向は行動の余地の変化の中で解釈されていかなければいけない。

しかし、情報面の自己決定の喪失という問題を、我々の自律性の喪失の危険、ひいては自律的存在としての我々の自己理解の喪失の危険と切り離して考えることはできない。この自律的存在は憲法によって守られているだけでなく、ルネサンス以来再三脅かされてきた西洋文明の基盤でもある。

プライバシーと自律性の構造的関係並びに自律性という意味で厳格に解釈される自由の意味合いに鑑みると、私は「プライバシーの終焉」というテーゼに次の言葉を対置したいと思う。たとえプライバシーが我々にとって不利でしかなくとも、プライバシーは消滅することはないということだ。

３　憲法にとっての難題

国内の安全を守るための国家による監視措置のアンビバレンスは、コミュニケーション文化が変化しているにもかかわらず存続している。したがって、法秩序は今後も二つの側面を考慮しなくてはならない。

一つは、安全当局が新たなツールを用いて対処しなければならない、新たな脅威状況に対する考慮である。例えば、国際テロリズムや組織犯罪集団が最新のデジタル技術を駆使して活動している場合、安全当局も同じ土俵でそれらに対処できなくてはならない。もう一つは、意図せぬプライバシー侵害に対する考慮である。もしそれがひどくなれば、国民の自律性とともに、高度な意味での国民の自由だけでなく、民主主義の根幹までもが脅かされてしまう。

こうした状況の中での憲法の課題は、有無を言わさず「ノー」と言うことではない。むしろ、憲法の課題は安全政策のための基準を策定するということにある。この基準は、行動の必要性を認めつつも、基本法の裁量余地や、治安機関に対する法治国家的かつ民主的な統御を保障してくれるものなのだ。

しかし、このような憲法の課題は、決して簡単なものではない。憲法の伝統的な介入の基準、そして統御の基準は、とりわけ脅威の極端な規模によって、その真価が問われることとなる。

例えば、具体的な危険を前にしたときの古典的な法治国家的介入の閾値などに見られる。国際テロリズムに由来するような脅威に対しては、従来の警察法が定めるように、それらの脅威が日常的な危険のように具体的なものとなるまでは、警察が動いてはならないというのではまずい。しかるべき具体的な危険の発生を未然に防ぐため、そしてそれを適時に発見し、効果的に阻止するために、安全当局は既に危険の前段階で用いられている偵察ツールを必要としている。

「具体的な危険」という基準に代えて、どのような発動基準を定めるべきだろうか。抽象的な危険、危険状況、危険の推定などで果たして十分なのだろうか。具体的な危険の前段階というのは、大変幅広いものである。どのようにして発動基準を憲法の中から導き出すべきだろうか。

基本法解釈学の中心的な支柱である比例原則（注：達成されるべき目的（例：安全の保持）とそのために採られる手段（例：権利の制限）の間の均衡を要求する原則）も、法治国家の侵食という大きな渦の中に巻き込まれている。既に具体的なものとなっている危険の阻止や、既に行われた犯罪行為の追及とは異なり、危険の予防においては比例原則によって、ほとんど太刀打ちできないような大きなダイナミズムが展開される。

できる限り効果的な予防のためには、できるだけ多くの情報があるということはただ単に適切だというだけでない。効果を高めるためには不可欠になる。そして、9.11 の同時多発テロや、マドリッド、ロンドンで起きたテロ、あるいはもっとひどい襲撃を防ぐために情報の単なる収集、保存、あるいは処理をすることが、どうして不適切だと言えるだろうか。

予防という考え方のダイナミズムは、比例原則の裏をかいて、その効果を失わせてしまうように思われるが、そのようなダイナミズムは既に、比例性だけではなく、その操作可能性（注：効果的な予防を図るために必ずしも比例原則によらない場合が認められるということ）をも憲法上の基準へと高めるべきという要請につながっている。それによると、予防措置が違憲となるのは、それが比例性を欠く場合のみならず、常に比例的である場合にも生じ得るということになる。

憲法と憲法の解釈にとって、このような崩壊の兆候に対して、解釈論上適切な構造を開発することは決してつまらない使命などではない。その構造は、一方では新たな脅威状況に考慮するものであり、しかし他方では、法治国家としての境界の設定や、統御、構造化といった要求を放棄しないものなのだ。

4 連邦憲法裁判所の反応

さて、連邦憲法裁判所は、このような難問に対して、これまで 10 数件の大変印象に残る判決で、ほぼすべての新しい安全法制上のツールに反応してきた。例えば、テロリズム撲滅のための連邦刑事局の新たな権限に関するさらなる訴訟手続が現在も進行中だ。

裁判所はこれまでの決定において、憲法上の枠組みを開発した。これには、考えられる限り最大の危険をも阻止し防止するための措置も順応しなければならない。裁判所によって発展されてきた解釈論上の枠組みの基本構造は、主に三つの要素から成り立っている。手続法上の保障、相対的な介入制限、そして絶対的な実質的介入制限。これらは、決して安全法制上の観点を越えてはならないものである。

(1)　手続法上の保障

では、まず手続上の保障から見ていくとする。まず裁判所は、文献上の多くの見解と完全に一致する形であったが、実体的基準の撤廃を手続法上の要件で相殺する形で反応した。安全当局による基本権侵害が特に甚大な事例について、裁判所は裁判官留保（注：捜査機関が個人の法益侵害に当たる特定の措置を行うに当たっては、裁判官の命令又は許可を必要とするという原則）を要求し、秘密裡に行われる措置の場合は、報告義務を求めた。プライベートな人生設計の核となる領域を保護するため、実施措置に関しては部分的に詳細な基準を設け、立法府が導入した議会の報告義務を憲法上正当であるとした。

まさに、安全当局に対する民主的なコントロールを保障することも、隠匿され秘密裡に行われる介入が多い状況では、構造上の理由から容易なことではない。隠匿された措置は、しばしば当人の事実上の法保護の可能性に対しても影響を及ぼす。つまり、自分の知らないところで行われている措置に対して裁判で争うことはできない。しかし、当事者が起こす司法手続は、結果としてその公開性を通じて、個々人の法的保護だけでなく、秘密裡の措置の場合には、隠れてしまっている安全当局に対する公的な統御をも可能にする。

立法府が民主的な統御の欠如を補うため、ここで部分的に新しい道を歩み始めたということは、強調されてしかるべきことだ。

例えば刑事訴訟法第100b条第5項及び第6項がある。それによると、各州及び連邦検察局は、暦年ごとにボンにある連邦司法局に対して、それぞれの管轄エリアで指令された通信の監視について報告しなければならない。そして、この報告をもとに、連邦司法局は連邦全体で指令された措置の一覧を作成し、それをインターネット上で公表する。

同様に諜報機関も、テロ撲滅法によって認められた権限の行使について、議会に報告しなければならない。そして、それが評価されることになる。その評価に関しても、厳しい基準が設けられている。いずれにしても事実上これらの報告、そして評価の結果はオープンであり、メディアにも浸透することとなる。

こうした報告は、さまざまな効果をもたらすこととなった。世間一般でこの報告を見ることにより、現実的な評価をすることになった。実際、最初の報告書を見た人の多くが、テロ撲滅法に基づいて行われた措置の数が意外に少ないことに驚いた。批判的な人々は監視の数がとても多いのではないかと危惧していたが、彼らが描いていたシナリオの規模を大きく下回るという結果が出てきた。したがって、このような透明性を設けることは、現実的にむしろ安心につながる評価をもたらすこととなったのである。

それでも、こうした報告書は通時的及び共時的な比較を許容するものになっている。このようにして当該の措置が著しく増加していたり、あるいは州によって差異があったり、ほかの州に比べてこの州では権限の扱いが寛容だった場合、政治的な正当化が求められることになる。

実際、連邦司法局による盗聴に関する統計が公表されたことにより、個々の連邦州の間で大きな相違があることが浮き彫りになった。当然、この相違はたちまちメディアが注目し、メディアに取り上げられることになり、ドイツ南部にある州では、通話監視の件数が何倍も多かったことがわかった。例えばバイエルン州の通話監視の件数は、北部にあるハンブルク州よりも10倍も多かったことがわ

かった。

そうなると当然、内務大臣たちは釈明をしなければならない。そして、非常に厳しい局面に立たされることとなった。各大臣は、自分たちの州がほかより危険であるということ、あるいはそうした措置をしたからこそ安全なのだということ、そのどちらも証明することができなかった。

憲法改正に取り組む立法府は、議会の監視委員会の権限をも強化した。この委員会は、基本法で憲法上きちんとした形で盛り込まれており、連邦の諜報活動に対する議会の監視、コントロールに関する法律によって新たに詳細が定められている。

このように、秘密裡に行われる措置の政治的な監視が行われているが、アメリカではこのような措置が、裁判所によっても、政治的にも監視されていない。つまり、諜報機関以外は、一体どのような措置が行われているのかがわからない。どのような決定がどのように行われて、どのような盗聴が行われているのか、誰も知らないというのがアメリカの現状である。

ドイツにおいては立法措置の中で、議会が警察機関によって行われる措置に関しての報告を受け、また監視できるという措置が行われている。当事者はそうした措置が行われていることを知らないため、そもそも法的措置に訴えることができないということは先ほどお伝えしたが、少なくとも議会内での監視が行われているということが重要である。

もし、さらにその範囲を拡張するのであれば、制度改革も併せて行う必要がある。議会による監視が、法律上または事実上排除されている司法による監視を補う確実な手段に思えようとも、さらにその役割を拡充するためには、制度改革も併せて行う必要がある。

(2) 相対的な実質的介入制限

以上は手続上の話だが、このほかに、連邦憲法裁判所は手続法による埋め合わせの価値を評価するだけにとどまらず、安全政策上の措置における相対的及び絶対的な実質的介入制限を規定した。

解釈論上、恐らく最もセンセーショナルで革新的だったのは、オンライン捜索の判決において、個人情報システムの不可侵性に対する権利を認めたことであり、連邦憲法裁判所は、これにより全く新しい憲法上の実質的な基準をつくりだしたのである。

連邦憲法裁判所は、情報自己決定権のほかに、一般的人格権をさらに明確に打ち出して、それを特別な手続法的、実質的保護の対象とした。この新しい基本権は、治安当局がデータを集めるだけではなく、個人情報システムを操作することによって生じる危険性をも想定している。ここまでする必要があるかどうかについては、意見が分かれているところである。

しかし、オンライン書店アマゾンが著作権上の観点から顧客のタブレット端末にアクセスして、そこに保存されている書籍データを消去する決定を下したことからもわかるように、電子化の増加に伴って、情報自己決定権に対する従来の侵害レベルを超えた操作が可能になってきている。消去対象となった最初の本がジョージ・オーウェルの『1984』だったことは、皮肉にも警鐘を鳴らしているようである。

相対的な介入制限は、このほかに基本権侵害のレベルに応じて、裁判所が定めているさまざまな発動基準からも設けられている。憲法裁判所は、具体的な危険という法治国家的な発動基準を普遍的なものとして固持してはいないものの、特に介入の度合いの強い措置、あるいは特に影響の幅広い基本権侵害については、引き続きこの発動基準を要求している。このような措置は、相手を萎縮させてし

まう可能性を秘めており、基本権を行使する意欲を損なわせてしまう可能性があるからだ。

介入の度合いの強い措置の例としては、オンライン捜索に対する決定がある。影響度の広い例としては、通信データの保全及び車両登録標識の自動捕捉に対する決定がある。

ラスター捜査（注：コンピュータを利用して大量の個人データから容疑者を絞り込む捜査方法）に関する判決においても、憲法裁判所は具体的な危険という要件を固守した。危険状況が全般的な影響を持つものではあるが、特定の集団に限定されない場合は、9.11 のような同時多発テロのような事態が起こった後でも、なお、特定の特性で全国民をラスター捜査することは正当化されない。

求められているのは、むしろ実際の根拠に基づいて、蓋然性について具体的な判断を下すことだ。しかしこの根拠は、ラスター捜査ツールの不合理性を論証するほど詳細なものである必要はない。損害の時間、場所、人物に関する具体的な根拠、あるいは妨害者に関する具体的な証拠があれば十分なのだ。

(3)　絶対的な実質的介入制限

憲法裁判所は、いかなる個別事案においても、立法府であっても越えてはならない絶対的な限界を設定している。その根拠としているのは人間の尊厳の保障である。最もセンセーショナルだった決定は、恐らく航空安全法に関する判決であろう。9.11 のテロ攻撃のときのように、旅客機を空飛ぶ爆弾として利用する意図がある場合であっても、それを追撃してはならないという判断が下されたのである。裁判所にとって、人間の尊厳の保障とは、犠牲となる乗客たちの人生の長さと、地上で巻き込まれて被害を受ける可能性のある人々の人生の長さを比較することはあり得ないということだ。

しかし、この航空安全法のケースにおいて、撃墜することが乗客の人間としての尊厳を侵害することになるのかという問題とは関係なく、この判決が明らかにしたことは、いかなる深刻な緊急事態においても、人間の尊厳を侵害することは基本法で認められていないということだ。航空安全法に基づき、たとえそれが時限爆弾のように、非常に切迫したシナリオであっても、人間の尊厳に対する侵害が明白な事例は正当化されることは決してない。

刑事裁判所も、人間の尊厳の保護は絶対的であると固持している。例えば誘拐犯に対して、誘拐された子供の居場所を聞き出そうとして、拷問をちらつかせて脅迫した警察所長は、強要罪で有罪判決を受けた。欧州人権裁判所も、尊厳保護の絶対性を支持している。それどころか、ドイツに対して、その警察署長への処罰が軽すぎるとして非難したぐらいだった。連邦憲法裁判所は、音声と映像による住居の監視、すなわち大盗聴についての判決の中で、基本法第１条第１項（注：人間の尊厳の不可侵性についての規定）に基づき、私的領域における絶対に保護しなければならない核心領域を定め、国家的措置に対するさらなる制限とした。

憲法裁判所としては、とりわけ通信の監視にとっても重要な基準を、人間の尊厳の保障から導き出さざるを得なかったわけだ。刑事訴訟法の規定は基本法の改正に伴うものであったが、基本法に関わる憲法の改正限界は、人間の尊厳の保障にしかないからである。

「私的領域の核心的部分において人格を発揮することとは、感覚や感情といった内面的事象、思索、見解、体験を、国の機関に監視されているという不安を感じることなく、非常に個人的な方法で表現することである。感情の表出、無意識的な体験の表明、性的な表現形態も保護の対象になる」。これが私的領域の核心的部分である。

私的なくくりにおさまらない内容については、核心的領域には属さない。憲法裁判所は、日記の保護に関する判決の中で、内面的な感情や印象だけにとどまらず具体的な犯罪行為を示す記述を、核心領域の保護の対象外とした。

このようにして定めた私的領域の核心的領域に対する国家の介入は、連邦憲法裁判所によれば、基本的に許されないというのではなく、常に許されないということだ。住所、パソコン、通信に対するあらゆる形態の監視がこれに該当する。この核心的領域は、いかなる形態の侵害に対しても常に保護されている。

憲法裁判所は、核心的領域に該当する限り、ほかの利益を斟酌する余地はないと明言している。「この保護は斟酌により、比例原則によって相対化してはならない。重大な犯罪は常に存在するものであり、刑法適用の実効性のほうが、被告の人間の尊厳を守ることより重要だと感じる人が多い場合もあるだろう。しかし、国家がそのような評価をすることは禁じられている」。

核心的領域の絶対的保護という考え方から、裁判所は、核心的領域に踏み込むことが想定される監視措置に対して、一連の基準を策定している。

措置によって核心的領域が侵害されることが想定される場合、監視は直ちに中止しなければならない。例えば、信頼できる人物を使って個人宅で会話を盗聴している場合で、具体的な犯罪行為に関わっていることを示すものが何もない場合などである。

監視が適用外とされていない限り、原則的に監視は許されている。しかし、その場合でも適切な措置を講じることによって、最大限の慎重さを維持しなければならない。そのため、個人宅を監視する場合には、自動監視はやめて、核心的領域に踏み込みそうになったら、いつでも監視を中断できるようしておくことが必要になる可能性がある。何時間も連続的に自動で監視装置を稼働させるのではなく、担当者がしっかりと状況を見ながら捜査することが必要だということである。

最大限の慎重さにもかかわらず、ある措置によって絶対的保護の対象である私的領域の核心的領域の実態が捕捉されてしまった場合、記録は直ちに廃棄されなければならない。当該情報は、いかなる形であれ利用することはできない。加えて、消去義務と利用禁止が確実に遵守されるよう、収集したデータの利用可能性、取り扱いについては、第三者機関が決めるようにしておく必要がある。

正しく理解されていれば、核心的領域のデータが一緒に収集されてしまうような状況においても、人間の尊厳の保護を実現することは可能である。そもそも核心的領域のデータを収集する段階で、既に人間の尊厳の保障に対する侵害があったということにはならない。

しかし、核心的領域への介入が実際には不可避である場合、人間の尊厳を尊重するために意図せぬ介入をできる限り回避することが求められる。それでも介入が回避できなかった場合には、当該データの閲覧を直ちに中止し、データを即座に破棄し、絶対に使用しないことが求められる。さらに、関係者の尊厳を尊重する観点から、特に利用禁止については、確実に実行されているか第三者機関がチェックするよう求められている。通常、これは裁判所が行う。

介入措置によって意図せぬ結果が想定される場合、そのような事態を回避すべく尽力する。それでも回避できなかったときには、関係者への影響を可能な限り小さくとどめるべく尽力することによって、関係者へ配慮することができる。私的領域の核心的領域に踏み込んでデータ収集を行う場合には、当該データが一切利用されないようにすることが、これに該当する。

５　結び

より成熟した安全法制というのが私の立てたテーゼであるが、それは安全法制そのものが持つアンビバレンスを常に自覚しているものである。そのような安全法制をつくっていくことは簡単ではない。特に憲法にとっては難しいことだ。脅威の規模があまりにも大きすぎて、憲法では対応しきれなくなってきているようにも見える。解釈学及び法政策上の想像力と断固とした決意が要求される課題だが、それがあれば、解決の糸口はあると思われる。

ドイツの安全法制は、そのような解決策を模索すべく確実に歩みを進めている。もちろん、ドイツのやり方が唯一の方法ではないし、またドイツの安全法制においても、克服すべき課題はたくさんある。また、文化的背景に左右されることも多い。文化が異なれば、脅威への対応の仕方も異なってくる。特に民主主義の伝統が強い国々は、法制面からというよりも、政治的プロセスに重点を置いて、最新の安全ツールの意図せぬ効果をチェックすべく取り組んでいる。

とはいえドイツの事例から、安全法制が抱えるアンビバレンスという問題に取り組むことが有益であることをご理解いただければ、幸いである。今、多くのことが危険にさらされている。私たちの安全だけではなく、現代の自由な社会の生活も危険にさらされているのである。

【基調講演４】「通信の秘密：個人の権利か、事業者の義務か」

情報セキュリティ大学院大学教授　林　紘一郎

0　はじめに

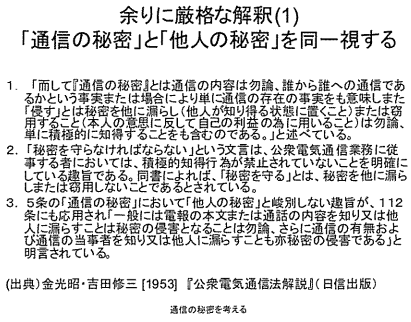
私の話は、テーマとしては「通信の秘密：個人の権利か、事業者の義務か」となっているが、要は懺悔録のようなものである。NTT に 33 年も勤めながら、この問題についてはあまり考えたことがなく、従来の解釈を所与のこととしてやってきた。その後、この慶応義塾大学で職を得て、またその機会に『情報メディア法』という書物を書き博士号をいただいたのだが、その書物を書くときも、今ほど問題意識を持っていなかった。

しかし、2004 年から情報セキュリティ大学院大学の設立に参画し、セキュリティの面からいろいろなことを研究すると、これは大変深い問題だということが、よわい 70 にして惑わずではなく、70 にしてやっとわかったというようなことである。その反省を込めて若干お話し申し上げたい。

1　余りに厳格な解釈(1)

まず、実務経験者としてケースから始めたいと思う。三つ取り上げる。あまりに厳格な解釈がかえって事態を混乱させている例である。

一つは、通信の秘密と他人の秘密を区分けしないということだ。電気通信事業法 4 条 1 項には「通信の秘密は、侵してはならない」とあり、4 条 2 項には「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」となっている。文言が明らかに違う以上、その外延も違うのではないかと思うが、そのような解釈は、少なくとも公衆電気通信法が制定された 1953 年以降はとられてこなかった。



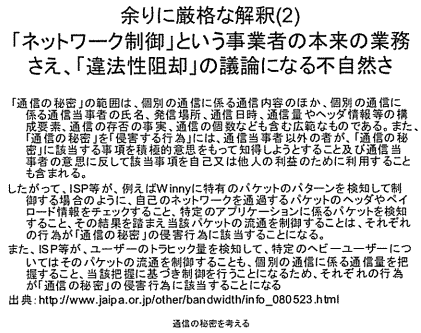
さらに 1963 年、この 10 年後だが、吉展ちゃん事件が起きて、電電公社が郵政省を通じて内閣法制局に見解をただした文書がある。そのときは明らかに、質問者も回答者も、4 条 1 項と 2 項を書き分けて質問し、書き分けて答えをいただいている。しかし NTT の社内通達である「電文 1100 号」を出すときに、この二つは区別しないことを明確にしたという経緯がある。

これはちょっと待ってほしい。それ以前の郵便では、郵便の信書の中身を見たらどうなるか、表書きを見たらどうなるか、そういう議論をしていたが、それを忘れてしまったのではないか。

2　余りに厳格な解釈(2)

2 点目は、余りに厳格な解釈をすることによって、通信事業者が困っているということである。ご案内のとおり、インターネットには膨大な情報が流れる。映像を中心にして大変量が多いと、他の方の通信を圧迫することがある。東日本大震災のときに、仙台方面に電話をかけようと思うと、混んでいてとてもかからない。そのときに通信事業者はどうするか。50%規制、極端なことを言えば 80%規制や 90%規制をかけて、一定の量の通信しかさばかないということを、自らの職責としてやっている。

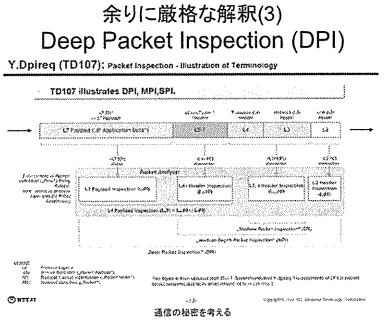
しかし、インターネットのトラフィック制御については、通信の秘密の侵害ではないかという疑いが出て、総務省で検討した結果、形式論理的には通信の秘密の侵害であるが、特定のケースについては、違法性が阻却される正当業務であるから許されるという構成をとっている。いってみれば、医者が今から外科手術をするにあたって、形式的には傷害罪を犯すかもしれないが、患者の依頼を受けて、これが唯一最高の治療方法であるがゆえに、違法性は阻却されるということを考えながら仕事をやっているようなものであり、そんなことでいいのかという感じがするわけである。



３　余りに厳格な解釈(3)

３点目として、現在最も話題になっているのがDeep Packet Inspectionである。これは、やっている方々がどうやっているかはなかなかわからないが、標準化も進んでいて、ここにあるような標準が大体決まりそうである。

ペイロード（Payload）という部分があって、手紙で言うと封書の中に書いてある事柄になる。ヘッダー（Header）と言われている部分は、手紙で言うと宛先や発信者のアドレスになる。Deep Packet Inspectionというのは、ペイロードのほうにまで入り込んでインスペクトするという仕組みであり、これは明らかに通信の秘密を侵している。それ以外に、Medium InspectionやShallow Inspectionがあり、先ほどの解釈では、すべてのインスペクションが形式的には通信の秘密を侵すことになるということを言っているわけである。それは本当にそうなのかという疑問が生ずる。



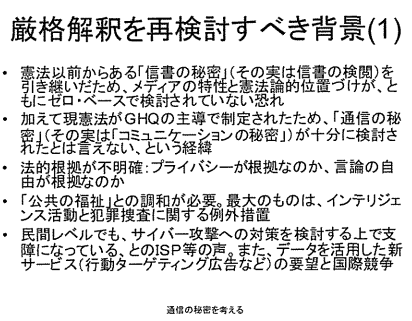
４　厳格解釈を再検討すべき背景(1)

次に、厳格的な解釈を検討すべきと私が考える背景を３点ばかり説明し、それを簡単にまとめてみる。

まず１点目は、現行憲法以前からある信書の秘密。この歴史を調べていくと、信書の秘密と言うのがおこがましいぐらい、これは信書の検閲のことであって、秘密を守るようになったのは随分後になってからだ。現行憲法は、その歴史を引き継いでいるので、メディアの特性と憲法論的位置づけという議論を初めからやって、この規定になったとはとても考えにくい。

現行憲法だけに注目した場合にも、押しつけられたと言われているGHQ案を見ると、原案は“secrecy of any means of communications”であり、会話も含めたあらゆる形態の通信の秘密を守るということであったが、最終案ではこの“any means of”が削除され“secrecy of communications”になっている。アメリカ法に詳しい方なら、当然これは会話等も含むとお考えになると思うが、日本側は通信、特に電気通信という、非常に狭い意味の秘密の保持と受け止めたのである。

２点目として、憲法学者の方にはぜひご検討いただきたいのは、プライバシーが根拠なのか、言論の自由が根拠なのかということだ。現在の通説はプライバシー説になっているが、私のように法人の通信をたくさん扱ってきた者からすると、法人についてもプライバシーはあるのかと思ってしまうので、どちらといえば言論の自由と考えたほうがいいのではないかと思うが、いかがなものだろうか。



それから第３に、通信の秘密が絶対のものではなく、「公共の福祉」との調和があり得るということは、裁判所も認めているところである。その本来の最大のものはインテリジェンス活動であろうかと思うが、これについては日本法に規定はない。つまり日本法は、憲法が停止するという状態も想定していないし、外国と情報戦をやるときにはどうしたらいいかということも想定していない。唯一あるのは、犯罪捜査に関する例外措置であるが、例外措置は例外措置としていかにあるべきかを厳格に検討すべきであって、個人の権利と公共的利益の調和をどうやって克服するかということなしには、かえってなし崩し的になってしまうおそれもなしとしない。

昨今は、四方さんのお話もあったサイバー攻撃が民間企業にも向かってきているが、そういうものを分析しようとすると、パケットインスペクションが必要になる。具体的にこうしてほしいという話は伺っていないが、潜在的にはそういう可能性はある。

併せて事業者の間では、パーソナルデータを活用して行動ターゲティング広告等につなげたいという要望もある。これは国際競争になっていて、ご案内のようにアマゾンなどは、私がある本を買うと、次にはこんなものが出たといった広告が飛んでくるわけである。我が国では、そういうことをやるにも、通信の秘密との調整を考えなければならない。この問題は、通信寄りのビジネスをやっている人にとっては、要検討事項になっている状態である。

５　厳格解釈を再検討すべき背景(2)

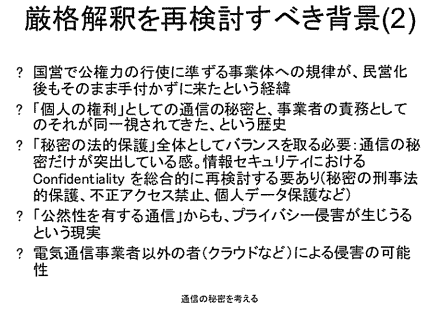
さらにその背景を探ってみると、民営化のときにもっと検討すべきではなかったかということである。私も、85年の自由化と民営化については、官庁で言う総務課長のようなポストにあったので、このプロセスにはコミットしてきた。たくさんの法律を検討しなければいけない中で、通信の秘密の条項を検討した形跡が全くない。自分たちが独占でやってきた時代の倫理は、いかに事業者がたくさん出てきても、同じように守ってもらいたいという考えは、理想としてはよかったかもしれない。しかし、それがそのまま法制化されていいかどうかは考えてみる必要があったが、そのような検討は全くなされなかった。

よく考えてみると、個人の権利としての通信の秘密、これは主として憲法論的視点になるかと思うが、それと事業者の責務としての通信の秘密、この両者が混同あるいは同一視されてきた歴史があるのではないかと思う。これはやむを得ないことであって、唯一の国内キャリアしかなければ、通信の秘密が個人の権利であろうが事業者の義務であろうが、どちらから見ても同じことになる。

しかし現在インターネットで起きていることは、多数の事業者が登場し、それも旧来の分類によれば、第１種電気通信事業者というかなりの初期投資を伴うビジネス、投資してもらった回線を借りる

形で簡単にビジネスが行える旧第２種電気通信事業、その両者の登録あるいは認定等を全く受けずに、「私は情報処理をやっているんです」と言ってやっている事業者、さらに加えて最後のパターンは、日本でビジネスを行っていて「私は日本法の適用なんか知らない」と言っている外国出自の事業者も含めて、たくさんの事業者がいる。そのときに、通信の秘密を、秘密の保護法制全体の中で特に重視しなければいけない理由はどこにあるのかは、もう一度考えてみる必要がある。

何も刑法がすべてをあらわしているとは言えないが、刑法の秘密の保護の章は、信書開封罪のほかは、医者や弁護士の Confidential information をどう扱うかということしか書いておらず、秘密の保護一般についての規定を欠いている。電気通信というビジネスに携わった途端に、法定刑の上限も含めて他の秘密の保護よりも厳しい扱いになる、そういうことが本当に必要なのか。私は、企業の倫理としては必要だという教育を受けたし、後輩にもそのように伝えてきたし、それが電気通信ビジネス全体に広がってほしいとは思う。しかし、それが法制度としてバランスのとれたものかどうかということは、考える必要があると思っている。



この点について自信を持っては言えないのだが、どうやらイギリスはプライバシーという訴訟原因はなくて、Confidentiality で裁いているようだ。Confidentiality という、Confide する側と Confidant の間の信頼関係という契約法的な裁き方をしているということだ。そのようなことも含めて、秘密はどのように保護するのがいいのかというのが問題ではないかと思う。

さらには、例えばブログや SNS に気楽にあることを書いてしまったら、その個人がいろいろな手段で複合的に同定され、「あんなことを言っているのは林だ」と次に書かれてしまう、といったようなことはあり得るわけだ。

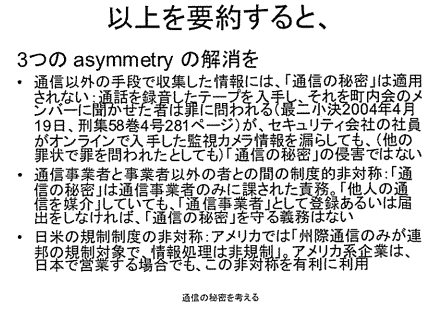
これは、いわゆる「公然性を有する通信」の問題で、電気通信事業法が直接的に適用されるかどうか不明確な点がある。だが、通信の秘密から派生した事象と、事象だけを見ればさほど違わないようなことが起こり得る。それは、通信の秘密なのか、プライバシーの侵害という他の問題なのかという論議がある。

さらに、事業者はすべからくクラウドのほうに行っているが、クラウドビジネスについては事業法がない。どなたがクラウド事業者かというのは、クラウド事業者だと名乗っている人がクラウド事業者だということになり、その方々に「通信の秘密」の観点から、どのような期待をするかというのは難しい問題になるであろう。

以上を要約すると、

途中でまとめてみると、バランスを欠いている三つの局面があると思っている。

一つは、通信と通信以外の境目である。今は、通話を録音したテープを何らかの方法で入手して、それを町内会のメンバーに聞かせた者は通信の秘密の侵害になるという最高裁の



判決があるぐらい、通信の秘密は厳格になっている。しかし、例えばオンラインセキュリティをやっている会社が、セキュリティ上の情報あるいは監視カメラの情報等を他に漏らしても、他の罪状で罪になることはあり得るが、通信の秘密の侵害ではない。

これは、どちらがいいと言っているのではない。通信の秘密を拡大したほうがいいのかもしれないが、要はアンバランスであるということだ。これは、石井先生がおっしゃった位置情報の問題や、公然性を有する通信等、いろいろ広がっていく可能性があると思う。

2 番目は、事業者同士の関係である。通信事業者と通信事業者以外の者の間で、制度的非対称になっているということだ。他人の通信を実行上媒介していても、それが通信事業者として登録あるいは届出をしていないと電気通信事業法の適用はないので、通信の秘密を侵すことについて責任を問われることはない。

3 点目は、いま業界ではむしろこれが一番注目されているのだが、日米の制度的非対称である。アメリカはご案内のとおり、憲法で定められたものだけが連邦の権限であるので、FCC（Federal Communications Commission）は州際通信（インターステート・コミュニケーション）しか規制権限がない。1970 年ごろから、コンピュータ通信は規制の対象か否かという長い論争あり、今に至るもこれは非規制ということになっている。

その非規制の文化で育ったアマゾンやグーグル等の会社が、向こうでやっているビジネスの感覚のままで日本に来て、Deep Packet Inspection であれ何であれ、それは情報処理の一種だということでやっている。そして、そのことについて日本の政府は実効性あるアクションを取れないでいる。アクションを取る勇気を持たないから悪いという見方もあるが、根本のこの制度の差を十分に念頭に置いた上で対処しなければいけない。そこで、これらの三つを解消する方法はいかにということになるわけである。

私は慶應義塾大学で法学博士号をいただいているので、法学者になりきらねばならないのだが、その前にうぬぼれて経済学のほうでも博士号をいただいていて、経済学者としてやっていけるとばかり思っていたのが挫折したという人間である。そのため、すぐに制度デザインをしてしまう悪い癖がある。法学の方は立法論はなるべく控えめになさると思うが、そこは私の出自からいってお許しいただきたい。

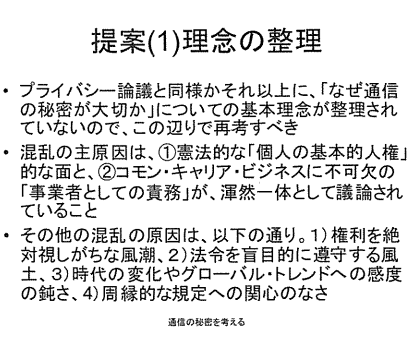
6　提案(1)理念の整理

提案として 2 点ばかり書いている。一つは、理念を整理していただきたい。プライバシー論議は混迷を深めていて、プライバシーはもう死んだという説もあるが、日本ではプライバシーは大事だという意見のほうがまだまだ強い。私はそれをプライバシーシンドロームと呼んでいる。それと同様に、なぜ通信の秘密が大切かという基本理念が整理されていないのではないかと思う。それを再考するのが、第一義ではないか。

混乱の主たる原因は、憲法的な個人の基本的人権の面と、それとは別のコモン・キャリアビジネスに不可欠な事業者としての責務。それらが渾然一体として論議されていて、分かれていないことにあるのではないか。

ちなみに私はクラウドの法律問題という共同研究の中で、クラウドビジネスは電気通信と同様パブリックユーティリティ性を有するがゆえに、何らかの規制は必要ではないかと書いて袋だたきに遭っている人間である。少したたかれすぎたので今は考えを改めて、ここまではいいのではないかということを少しお話しする。

例えばクロネコヤマトに荷物を預けて、クロネコヤマトがそれを開けて見ていたら許せないと皆さんは考えておられるだろう。クラウドはそういうことを大っぴらにやっているに等しいわけで、それは情報を扱う産業の規範として正しいのかということを問いたいわけである。つまり、通信の秘密の厳格性は減ずるが、その外延はもっと広いかもしれないということも同時に考えるべきではないかということだ。



以上のほかに、概念が混乱している原因は幾つもある。一つは、権利を絶対視しがちな風潮ではないか。ほかに飛び火して戦場を拡大するのは避けたほうがいいかもしれないが、自己情報コントロール権はそれの一種ではないかと思っている。

２番目としては、法令を盲目的に遵守する風土がある。コンプライアンスは、法令遵守と線を結ばないと○×式では合格しないというのが日本である。失敗学の畑村先生に教えていただいたが、コンプライアンスを辞書で引くと、幾つかの定義の後の最後の方に「ばね」と書いてある。ばねのように伸縮して相手に合わせるのがコンプライアンスのもとだそうだが、それと法令遵守はかなり隔たりがあるような気がしている。

３番目は、時代の変化やグローバルトレンドへの感度が鈍いことである。アメリカ企業にやられっ放しというのは、相手がえげつないことをやりすぎているのは事実だが、こちらもそれに対抗する方法を講じなければ市場では勝てない。

４番目は、周縁的な規定への関心のなさである。こちらの先生方がこういう問題に関心を持ってくださっているのは大変うれしいが、私がやってきたビジネスのような事柄について、メジャーな学者はあまり関心を示してくれない。多分、通信の秘密は一生懸命やっている、日本国は世界一盗聴が少ない国だからパフォーマンスはいいので、あまり学問的関心を惹かなかったのだと思う。しかし、今は時代がそうではないという感じがしている。

7　提案(2)三層構造（できるだけ早期に）

提案の第２として、では具体的にどうしたらいいか。まず、３層構造に分けて物を考えることを提案したい。我々は何でもレイヤ構造でやるので下のほうから先に行くのだが、一番下位のレイヤは通信の内容、DPIの標準によればペイロードの部分を通信の秘密として、憲法的価値あるいは個人の権利として保護することはいいと思う。信書開封罪が刑法に書いてあるなら、通信の秘密侵害罪も刑法でもいいぐらいに思っている。

それに対して他人の秘密と言われてきた部分は、狭義の通信の秘密を除く、通信の附帯情報である。皆様は想像できないかもしれないが、昔、我々が入社したころは手動式で交換していた。私も訓練の過程では、相手の局の女性の交換手になぜ男性が出たのかと言われる中で交換業務やっていた。そのときには、話し手が東北弁を使ったということもわかるわけで、そういうものが他人の秘密だということになっていた。

それと似たようなことで、今はパケットにいろいろな情報が書かれている。それらも含めて、事業者の義務として事業法に一部強行法規をおき、ほかは約款でやるということではどうかと思っている。犯罪抑止に対しては、一般の個人に対する刑事罰ではなくて、法人に対する課徴金のような、少し違

った方法が有効ではないだろうか。

最後に加入者情報だが、これはプライバシー侵害につながりやすい個人データであるが、基本は契約によるが、消費者保護の観点から一部を強行法規化する。特に現在、民法の改正で検討されている約款の不当条項は必要だという説を、私はとっている。

提案(2) 三層構造（出来るだけ早期に）

情報の分類	該当する情報の例	保護法式
加入者情報	プライバシー侵害につながり易い個人データ	原則は契約によるが、消費者保護の観点から一部を強行法規化する
他人の秘密	(狭義の)通信の秘密を除く、通信の付帯情報	事業者の義務として事業法に一部の強行法規をおき（個人に対する刑事罰ではなく法人に対する）課徴金制度を導入する
通信の秘密	通信の内容(ペイロード)	憲法的価値(個人の権利)を保護するため制定法（できれば刑法）による

通信の秘密を考える

8　提案(3)その根拠

繰り返しになるが、「通信の秘密」は、他の秘密とバランスをとって守る必要があるのではないか。かつて私は秘密の法的保護について拙い論文を書いて今は書き直さなければいけないと思っているが、セキュリティをやっているとだんだん明確になってきたことがある。

それは、次の３点である。①情報は拡散しやすいもので、守りにくい。それを何とか守るには、二つの方法がある。②一つは、プロパティのような財産化して守るということで、知財がその具体的方法になる。③もう一方は秘密として守るという方法だ。

この二分法があまり発達しないうちに、知財の学者が、営業秘密は知財だと言ってしまったので誤解が生じているが、あれは秘密だと私は思う。つまり、個人の秘密としてのプライバシーと、会社の秘密としての営業秘密と、社会あるいは国家の秘密と３種類ぐらいあって、それをどう守るかという秘密保護法制を検討すべきであると思う。

提案(3) その根拠

- (狭義の)「通信の秘密」は、他の秘密（営業秘密や国家機密）と同様、情報主体（当該情報の帰属主体）が秘匿したい情報であるが、（他の二者と違い）その支配・管理が通信事業者に委ねられているので、通信事業者にまで情報主体の権利が及ぶこととすべきである（個人の権利）
- 他方、狭義の通信の秘密以外の事項は、運輸関係の公益事業におけると同様、コモン・キャリアの職務遂行上不可欠の「業務情報」であり、今後クラウド化がさらに進展することも踏まえて、事業運営上の秘密（事業者の責務）として、契約や約款を補う強行法規として規定すべきである
- さらに、SNSなどの新しい通信手段の発達や検索技術の進歩と共に、「紐付け可能な(linkable)情報」の保護が問題になっているが、これらは「個人データ」保護の一般論として論ずべきである

通信の秘密を考える

それが行われたとしても、通信の秘密については自分が守るということはほとんどできないわけである。通信事業者に支配管理権が委ねられているので、その特殊性に鑑みて、通信の秘密を特に保護する規定を置くことは可であろうと思っている。つまり通信の秘密は、上述した三種の「客体としての秘密」を守るための「流通過程の保護」だと考えれば良い。

他方、通信の秘密以外の事項は、先ほどクロネコヤマトの例を挙げたが、コモン・キャリアと言われている職務には不可欠な業務情報だ。特に宛先などは、それがなければ仕事が成り立たない。そういうものは、今後クラウド化が進むとすると、クラウドの部分も含めた約款規制の検討をしたほうがいいのではないかと思っている。

さらに、SNS などの新しい通信手段の発達や検索技術の進歩とともに、「リンカブル（linkable）な情報」ということが話題になっている。これについては、個人データ保護の一般論として論ずべきであって、通信の秘密からだけのアプローチでは不十分ではないかと思っている。

9　提案(4)新法の制改定（中期的）

それではどうするか。大胆に言ってしまえば、刑法の改正において 133 条の 2 を加える。情報サービス基本法を定めて、許認可の有無にかかわらず、事業として情報の伝達処理、提供を行う者に対する一般的規定を設ける。その際、他人の秘密、顧客の情報に関する最低限の守秘義務を法定し、罰則として課徴金を設ける。

そのようなことをやった上で、旧来あった電気通信事業法・放送法等を抜本的に見直すのが正解で

はないだろうかというのが、私の立場である。

だいぶ時間が進んだので、クラウドについては途中で述べたので割愛する。

提案(4) 新法の制改定（中期的）

- 刑法の改正（133条の2として、信書開封に対応する通信の秘密侵害罪を定める）
- 情報サービス基本法を定め、「(許認可の有無にかかわらず）事業として情報の伝達・処理・提供を行なう者」に対する一般的規定を設ける。その際、他人の秘密・顧客の秘密に関する最低限の守秘義務を法定し、罰則として課徴金を設ける
- 上記に合わせて、電気通信事業法・放送法等を抜本的に改正する

通信の秘密を考える

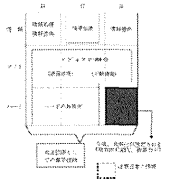
10　（広義の）「通信」を再考する

最後に、この図（下図「広義の『通信』を再考する」参照）は私の博士論文以来の伝統の図であるが、ごく簡単に説明する。データプロセッシングというコンピュータ通信を使ったビジネス（Ｄで表す）、コモン・キャリア的なコミュニケーションのビジネス（Ｃ）、ブロードキャスティングのビジネス（Ｂ）がある。今までこれは、それぞれハード、ソフト、誰の情報かという三つの局面において共通点のない産業だったので、縦割りの規制に服してきた。つまり、ＢとＣとＤはそれぞれ独立の産業であった。

しかしコンピュータとコミュニケーションの高度化（いわゆるC&C）と共に、これらはほとんど全部コンピュータ処理可能となり、ソフト屋が制御し、誰の情報かというだけが違ってきたので、産業秩序はレイヤ別に分離するのが望ましい。竹中懇談会でこの話が出たことはご存じだと思うが、あれの大もとはこの図である。それでもって、だんだん産業融合（B&C&D）のほうへ進んでいると思う。

（広義の）「通信」を再考する

1. 通信と放送と情報処理の融合
2. レイヤ別分離を前提にした融合法制



3. メディア産業とコンテンツ責任

Conduit ＼ Content	事業規制あり	事業規制なし
事業規制あり	Broadcasting	Common Carrier
事業規制なし	Internet?	Press

（出典）総著 [1984]『インフォミュニケーションの時代』中公新書、総著[2005]『情報メディア法』東大出版会

通信の秘密を考える

さらに問題は何かということがわかってきたのは、事業を始めるに当たって、パイプのようなものが必要な事業がある。そのときに、それが規制されているか、規制されていないか。ここで規制があるかないかは、事業法があるかないかとほとんど同じレベルだと考えてほしい。

一方、これが運んでいるコンテンツについても、規制があるかないかというマトリクスをつくると、今までメディアに関する産業は三つに分かれていた。一つは、新聞・出版のように、そういう規制が全くないもの。もう一つの極は、放送のように電波の割り当てを受けて、許認可があって、しかも運ぶ内容については、番組調和原則とかが課せられているビジネス。

コモン・キャリアは、事業規制としては参入退出の規制はあるが、この人たちは中身を見てはいけないというビジネスなので、その限りにおいては規制がないというか、見てはいけないという規制があると言うべきか、そういうことだった。

しかし、インターネットが出てきてこの三つの産業とも融合に向かっている。このときに、このような今までどおりの枠組みは有効なのかということが問われていると私は思っている。

そのような枠組みの中で通信の秘密を一度見直す機会があればと思い、昨年、今日も来てくださっている田川義博さんという昔から論文を幾つも一緒に書いている方と、「心地よいDPIと程よい通信の秘密」という論文を書いた。これがだいぶ話題になったので、ここにもお呼びいただいたという名誉あることになったのだと思うが、何がしか皆さんのご参考になればありがたい。

【パネルディスカッション（討論）】

横内　これからの進め方だが、それぞれバックグラウンドの違う皆様に「通信の秘密」について御発表いただいたが、大変広範な論点に話がわたっており、限られた時間でそれら全てに触れるのは難しいと思うので、大きく二つに論点を絞りたい。

一つ目が警察活動と通信の秘密。特に具体的な通信傍受、これは司法傍受（捜査のための傍受）だけでなく、インテリジェンス活動として行政傍受も含めてである。それから、携帯電話のＧＰＳ機能を用いた位置探査。それから、通信履歴（ログ）の保存の問題。まずはこういった各論について、いずれも今日のお話にあったとおり課題なり問題点があるので、これについてまず議論したい。

その後に、大きな二つ目として、「通信の秘密」の範囲。これは林先生からそれをメインにお話があった。それ以外の方からも保護の範囲の話、在り方についてあったので、これを大きな二つ目にして、その前の各論の話を踏まえて、保護範囲の在り方についての議論を進めるという形で進めてまいりたい。

最初に、このパネルから参加されたお三方からそれぞれ質問、コメントをいただきたい。後ほど議論するテーマに関わるものはそちらのほうで質問していただくということで、それ以外の全体的なものについて最初にコメントをいただきたいと思う。

大沢　慶應大学の大沢です。よろしくお願いいたします。最初に一つ先生方のお話をお聞きして疑問に思いましたことは、「通信の秘密」に関する憲法学の理解と今日のパネリストの方々の「通信の秘密」に関する理解がかなり異なるということです。

憲法学の方では、通信の秘密に関する通説的な見解というのは、プライバシーの権利との関連でとらえていくというものです。そして、そこでいうプライバシーの権利とは、自己情報コントロール権というものであると考えられております。

自己情報コントロール権という概念自体が出てきた状況は、そもそもデータバンクという社会を背景にしております。ただ、その後、データバンク社会とは異なり、情報や技術が社会において幅広く共有されるという事態が広がり、いまはIT社会からICT社会に進化ないし変化するというように進展してきております。そのけか、このような事態の進展に対応してさまざまな問題が指摘されてきました。グーグルのようなトランスナショナルな問題、あるいは対国家、対個人、さらに今日の最後にお話があったように対民間業者との関係において、さまざまな複雑な問題が出てきているわけです。

それぞれ関係を理解するためには国際的な流れ、あるいは時代的な背景・変化を知る必要があります。例えば、警察と情報の関係でいえば、捜査における情報収集に関して、監視カメラのような場合には、令状の有無、監視主体が警察なのか民間なのかが問題となります。アメリカでは最近、行政当局がGPSを用いるという問題などが見られますが、そういう状況をどのように考えるか。さらに具体的には法律における規定がどのようになっているのか、あるいは監視の方法の適切さ・程度の強弱、また先ほどらいは報告の中にでてきている常時監視か否かなど、さまざまな要素を踏まえた形で個別に検討する傾向が強いかと思っております。

そのようなことを踏まえて、今日の個別のご報告についてお聞きしたいと思います。

最初に、石井先生のご報告についてお聞きしたいと思います。石井先生のご報告については、まず通信の秘密の理解についてどう考えていらっしゃるのかが問題になるかと思います。

石井先生は、通信の秘密についてプライバシーの権利と表現の自由の二重構造ととらえておられます。

そして、通信の秘密に属する場合においても、通信履歴の保全のような通信の構成要素の場合には表現の自由にかかわるものではなくて、プライバシーの問題であると考えていらっしゃると思います。

お聞きしたいのは、そのような場合の権利に対する制約の正当化についてです。この点に関連して三つほど質問があります。

一つは、憲法の通説的見解との関係です。通説は、先ほど言ったようにプライバシーと見る立場が強いわけです。また、葛西さんのレジュメの5ページにある平成11年の最高裁判決の多数意見も同じような立場を示しています。そうすると、憲法の解釈は、刑訴法あるいは刑法学者の間でどういうふうに理解されているのかということが疑問になります。これが最初の質問です。

つぎに、プライバシーの制約がある場合に合憲性の判断基準について、石井先生のお話ではかなり緩やかなものと考えられますが、そのような考え方でよろしいのかどうかが少し疑問に思いました。この点を石井先生はどのようにお考えか、お聞きできればと思います。

最後に、プライバシーの利益と電気通信役務の公共性が対立する場合についてどうお考えなのかということをお聞かせ願えればと思います。

次に四方先生のご報告についてですが、先ほどのパワポのプレゼンでは、今日のテーマである電気通信事業者に対する不正アクセス・通信の秘密侵害事件の動向について、件数としてはかなり少ないような印象を受けました。サイバー犯罪全体との関係で、今後この種の事件の動向についてどういうふうになるとお考えかということについて、ご教授いただければと思います。

それから、サイバー犯罪について SQL インジェクションの情報漏洩の事例などを見ると国際的な広がりを持っているように思われます。その点、国際的な協調の現状あるいは在り方についても教えていただければと思います。

ポッシャー教授のご報告については、私は非常に説得されているところがあります。ただ、連邦憲法裁判所の対応として、裁判所によって示された協議上の枠組みの基本構造として3点指摘されているわけですが、手続法上の安全確保、絶対的な介入制限についてはそうかなと思うのだが、相対的な介入制限の内容について、ここがやはりこれから問題になりそうな気がするので、もう少し補足して説明していただければと思います。

それとの関係で、先生のお話の中にあった個人の情報システムの不可侵性の権利について、連邦憲法裁判所が新たな基本権として認めたということですが、この基本権については理論的に十分な基盤を持っているのか、疑問がないわけではありません。その点、ドイツにおいてどのような議論がなされているかお聞かせ願えればと思います。

林先生のご報告については、社会的な要因というか、現実に民間事業者の方が直面している要求が非常によくわかったように思います。

なお、蛇足ですが、憲法解釈について、憲法学者は頭が硬いようなことを言われた気がしますが、必ずしもそうではないのでその点はご了解いただければと思います。

私の質問は、12ページの「（広義の）「通信」を再考する」のレイヤ構造についてです。放送と通信の関係については、放送法の改正等で既にレイヤ構造になっています。その結果として、規制がしやすくなっているということがあるかと思います。情報処理の場合について、パワポでは三つに分けられていたかと思いますが、それも放送の場合と同じようにレイヤ構造にしてしまって規制を考えていくということなのか、お聞かせ願えればと思います。

横内　お三方通して質問していただこうかと思ったが、たくさんあったので、まずは大沢先生のご質問について、順番に石井先生からお願いする。

石井　まず、刑事法の研究者の間の理解はどうかという点に関しては、私の考えは少数だと思われる。ほとんどの方々は、憲法上の通説の理解を前提にしながら検討されていると思われる。

次の合憲性判断基準との関係とも関連するが、憲法を条文解釈としてきちっとやっていくと、表現の自由は確かに保護しなければいけないというのはあるが、プライバシーの権利は明文では定められていない。せいぜい憲法 13 条の個人の尊重だ。ドイツのような人間の尊厳ではなくて、単なる個人の尊重だし、あるいは幸福追求の権利だ。そういう形で出てくる権利というのは、状況によるが、保護が薄くなってもやむを得ない場合があるのではないかということになる。

具体的には、電話の場合だと通信当事者の入口・出口がそれぞれ決まっていて、その中を会話するという形でフローが流れているにすぎない。しかしインターネットの場合は、通信内容の問題は別に置くと、行動の履歴は、我々が日常生活で例えば今日私が自宅からどの駅に行って、どの線に乗って、どの駅で降りてここに来たという行動履歴に近いような局面は多々ある。そういったものが、従来の電話のプライバシーと同じような通信履歴の保護としていいのかとなると、やはり違ってくるだろうと理解している。

あくまでプライバシーだから保護しなければならないではなく、どういうものがプライバシーになっているかに応じて判断基準が変わってくると考えている。

それから、通信事業の公共性との関係では、電気通信事業法の枠組み、構成を考えると、当事者のプライバシーの問題あるいは電気通信役務にいかに公共性を持たせるのかというところに力点を置かざるを得なくなってくる。そうすると、1 人のプライバシーを侵害したとしても、多数の人の通信が安心して利用できていればいいとか、安全に利用できていればいいだろうとなってくるのではないかと考える。

四方　引き続いて私からご質問にお答えしたいと思う。まず、電気通信事業法上の通信の秘密侵害の事件は少ないので、全体を語る上でのウエイトはどうなのかというご趣旨だと理解した。

これは、事例のご紹介自体かなり古い事例を出しているぐらいであり、検挙の数は私の記憶でもそんなにない。ほとんどないと言ってもいいかもしれない。ただ、暗数がどのぐらいあるかはわからないものであり、基本的にサイバー犯罪の場合、事業者の方々から、また一般のユーザーの場合もそうかもしれないが、警察への申告が基本的にあまり多くないという事情が一つある。

電気通信事業者の方々も、先ほど林先生のお話ではないが、昔だとまさしくエスタブリッシュされた巨大企業で、セキュリティも当然高いところだけだった。しかし今はさまざまな企業があり、なおかつ、電気通信事業法上の届出はされていないが、情報処理として実質的には電気通信事業のようなことをやっておられる事業者もさまざまなレベルである。その場合には電気通信事業法上の違反にはならないので、この外側になるわけだが、ここで議論をされている意味での通信の秘密が侵害されている事案は、潜在的にはそんなに少ないとも思えないところがある。

そういう意味で、先ほど SQL インジェクションやサーバの乗っ取り事案をご紹介したわけだが、そういう他の犯罪の動向を含めたときに心配をしているところの一つである。ただ、言いわけがましくなるが、検挙件数のレベルでは大した数が現在あるわけではない。

それから、国際的な広がりという意味では、ご指摘のとおりだ。いつも検挙できているわけではないので被疑者がどこの国の者か自体いつもわかるというわけではないが、SQL インジェクションの攻撃は

国内からもあれば外国からも相当ありそうだと認識している。

私どももそれなりの努力はしている。しかし今日はあまり報告しなかったが、捜査権というのは国家主権の最たるものであるので、国境を越えて捜査権を行使するというのは、比較的連携のとれている国同士でも時間のかかる捜査になり、なかなか難しいというのはある。ただ、国境を越えての SQL インジェクションはそれなりにたくさんあると認識している。

ポッシャー　二つご質問をいただいた。一つは相対的な介入制限について、もう一つは新たな基本権として認められた個人の情報システムの不可侵性についてである。

相対的な介入制限に関しては二つの要素で捜査できると思うし、実際に法廷が捜査統御している。まずは、どの程度の危険かということだが、抽象的な危険、つまりまだ具体化していない危険と、実際に具体化している危険との間で分けることができる。積極的な介入の場合、かなり多くの人が対象になるだろうというときには、具体的な危険でなければならないとしている。その際には、情報の記録の蓄積をしなければいけない。例えば自動車の登録番号など、事前に情報の記録を保存するということになっている。

しかし、実際にそのデータをどう利用するかに関しては、相当厳しい要件が求められる。それも危険の度合いに応じてということだ。一つには、危険の種類と度合いに応じて決める。

二つ目の要素は、そのときに対象となる法益だ。積極的な介入をする場合にはどのような法益が対象になるか。特別危険な犯罪を防止するためということが重要になる。その際も、保存したデータを使う場合には、これまでの裁判所の決定によると、本当に人の身体、命を守るため、そしてどういうものを守るためかということを立法者がきちんと見きわめていかなければいけない。

この介入の制限は法律の中には明記されていない。言ってみれば、安全機関が自由裁量でそれを決めていいということになっていたからだ。いま申し上げたように、一つは危機の度合い、二つ目は法益の種類、この二つのポイントをもとに判断するということだ。その法益を守ることによって、この介入を正当化できるということだ。

もう一つ、新たな基本権については、今まで１件しか事例がない。このときの判断を下した判事はもう退いているので、その後の話は展開していない。この判事の生徒の中にもこの判例を厳しく批判している人がいる。新基本権は必要ないのではないかという議論もある。

私が思うに、情報に関する自己決定権で十分にすべて説明できている。我々が情報システムにどう依存しているか、その情報システムがどう発展しているかにより、個人の情報システムが量的にも質的にも変化している。

国が情報を集め、そして効果的にそれを利用するということは、国が我々個人の情報システムに侵入し、そのシステムの中で操作することとは別のことなのだという議論、これは意味があると思う。

私たちが本質的な観点、我々の生きている世界がバーチャルな世界の中へどんどん移行する中で、例えば図書館もバーチャルな中にしか存在しなくなり、すべてが電子データになり、我々のバーチャルの図書館の中にある本棚からどんどん国が勝手に本を削除するようになり得るわけだ。

このような操作がバーチャルな空間で可能になり、いろいろなコンタクトをつくってしまう。それも私たちの知らないところで。となると、これまでとは全く違う種類の危機、これまでの情報の自己決定権を脅かす危機とは違う危機が私たちの前にあるのだと考える。情報技術がどんどん進化していき、私たちが個人情報システムにますます依存していく中で、この新たな基本権は今後また新たな展開を見せ

る可能性は十分にあると考えている。

林　まず最初に、大沢先生に私が何やら憲法学者は頭が硬いというメッセージをお伝えしたかのように伝わったかもしれないが、まことに申しわけない。私も日々格闘している。特に自己情報から始まって、データ保護とプライバシー保護をごちゃごちゃにする議論の中に巻き込まれていたもので、ついついそんなことを申し上げて失礼した。

（図表）

通信手段の変遷と通信の秘密

主たる通信手段	郵便	電報	電話（手動交換）	電話（自動式回線交換）	インターネット（パケット交換）
「通信の秘密」の例	手紙・封書において伝えたい内容	電文そのもの	通話内容	同左	同左
「他人の秘密」の例	発信人・宛先・筆跡など	発信人・宛先など	発信者と受信者の番号、通信当事者の性別、発音の訛りなど	同左	発信と受信のアドレスなど
両者の峻別可能性	封書の場合、両者は峻別可能	両者は同時に扱われるし、秘匿の程度に差はない	両者は、同時に知得される	事業者が介在する頻度は低いが、傍受すれば同時に知得される。ただし共通線信号方式の導入以後は、区分可能	アドレス部分の情報だけを読み取ることは可能

情報セキュリティ大学院大学

ご質問は、この件（レイヤ別分離を前提にした融合法制）かと思う。放送と通信のＢとＣのところはもともと規制産業なので、現にある法律をどのように併せていくかということになるので、ある程度は融合できてきた。しかし依然として放送法と電気通信事業法があるということは、それほどは融合し切れていないというふうに私は評価している。

片方でＣとＤだが、Ｄは事業法がない非規制の分野になる。コンピュータはつくるほうもサービスするほうもずっと非規制で来たので、そこへ何かの規制を入れるというのは非常に難しい。それで苦労して、約款の不当条項等から入れていったらどうかと思っている段階で、まだまだだというのはご指摘のとおりだが、2 面は切り分けて考えているということだけお伝えしたい。

横内　それでは今度は小山先生、ご質問、コメントをお願いする。

小山　時間の関係で、ポッシャー氏のご報告について簡単なコメントをするにとどめさせていただきたい。

ご報告からわかるように、通信傍受一つとっても、日本とドイツでは桁が三つぐらい違っている。さらに、ドイツの場合には行政傍受も含めて、大盗聴やその他いろいろな方法が使われている。他方で、連邦憲法裁判所がそういったものについて逐一チェックをしていき、憲法上不十分な部分については違憲判断を出している。

連邦憲法裁判所は、頭から憲法違反という判断をしているわけではなくて、どこが足りないのか、あるいはどういう条件だったらやっていいのか、そういった形で修正を加えている。そのような連邦憲法裁判所の修正は、大盗聴あるいはコンピュータ基本権の問題といった、誰が見ても重大な基本権問題にとどまるものではなく、ご報告の中にもあったように、例えば日本のＮシステムに類似した自動車ナンバー捕捉照合やビデオカメラによる監視の合憲性にも及んでいる。

Ｎシステムやビデオカメラについて連邦憲法裁判所はどういう認識なのかというと、やはり法律の根拠がなければいけない。どういう場合に、どういう目的で撮るのか、その後どう処理するのかについて明確性を備えた法律でなければいけないし、比例原則も充足しなければいけない。そういった限定を加えている。

そのようなドイツの状況と比べると、日本の現状は次のようなものでしょう。憲法問題になりそうなことはやらないでおこう。せいぜいやっても通信傍受まで。しかも法律自体の要件が厳格で、使う現場は恐る恐る。それで年間20何件だ。そういうことがある一方、法律なしで組織法、警察法２条１項さえあれば何でもできるところはできてしまう。

ビデオカメラによる公共の場所の監視についてもドイツの違憲判決は、まさにそういった一般条項的なものでは不十分であり、特別な、もう少し詳細な授権規定が必要だと要求したわけです。

日本とドイツの裁判所の考え方を比べる上で興味深い材料を提供するのが、Ｎシステムの合憲性をめぐる議論です。Ｎシステムについては何回か裁判になっているが、ある地裁判決は、自動車の所有者は法によってナンバープレートをつけなければいけないとなっているから、走行車両のナンバー及びその車両が公道をどちらの方向に向けて通過したかの情報は、警察等の公権力に対して秘匿されるべき情報とは言えない。大体そのようなことを言っている。

さらに高裁では、先ほどのドイツの違憲判決を弁護側が引いて、ドイツではこういう違憲判決が出ていると主張したのに対し、高裁は、それはドイツの話だと言った上で、なおかつ次のように説示しています。ドイツはそのような公権力の行使は法律の定めに基づくことを要しているが、我が国においては、警察は警察法２条１項の規定により、強制力を伴わない限り犯罪捜査に必要な諸活動を行うことが許されていると解されるのであると。これが日本の高裁の認識であり、おそらくは最高裁の認識でもあるでしょう。

そのギャップがどこから来ているかというと、一つはポッシャーさんのお話にあった、情報自己決定権という観念があるかどうかというところです。古典的なプライバシーの権利との関係で言うと、Ｎシステムぐらいはいいじゃないかということになってくると思う。さらに、佐藤幸治教授の自己情報コントロール権説が挙げられます。裁判の中で原告は佐藤幸治説にのっとって主張する、国側も佐藤説に乗って応答する、裁判所も佐藤説に乗って判決を出す。結局は何の使い道にもならないという、そんな説になっている。あれとは違って、ドイツの情報自己決定権はもう少しシャープな説です。かつ、佐藤説では切り捨てられがちな自動車のナンバーや、公道でのビデオによる撮影等にも、力を持っている説ということになる。

ただ、恐らく日本の裁判所だけではなくて、それ以上に、田村先生をはじめとした警察の皆様方になかなかご理解いただけないのは何かというと、具体的な害悪が発生して初めて何かの権利を侵害したことになり、単にビデオで撮られた、あるいはどこかのデータベースに載ったというだけで、何が具体的な害悪なのかと。したがって法律の根拠なしにやってもいいはずだと、そうやって話が行くのだと思います。

ドイツの憲法裁判所のある判決から一言引用しておきたい。「秩序維持に当たる官庁、とりわけ警察は、当初は法律による特別な授権なしでも法益を予防的に保護し、あるいは後の刑事訴追をやりやすくするために、危険の前域、前段階において情報を収集した。その種の観察や情報処理の措置は、長い間、基本権侵害であるとは位置づけられてこなかった。しかし、このような措置の多数について、要するに基本権を侵害するという侵害的性格が承認されるようになった後には、警察はこれに対して法治国家が求める明確性・特定性の要求を充足する侵害の授権を必要とすることが確立した」というように言っています。これはポッシャーさんのお話のそもそものベースになっている、そういった認識だというふうに思う。

ポッシャーさんに対して質問ではなくてお願いがあります。情報自己決定権という権利、これはアメリカにはないし、日本でも多分あまり支持されていないと思うが、なぜこの情報自己決定権という権利が成り立つのか。実際に行動が束縛された等の具体的な害悪の発生前に、なぜ侵害というものを観念できるのか。もう一度ご説明いただきたい。

ドイツでも情報自己決定権は、間違ったコンセプトではないかという批判が随分ある。その点も含めて、ポッシャー先生のご見解をお聞きできればと思う。

ポッシャー　コメントの中にもあったように、一つひとつの法的な根拠について議論するよりも、まず明確にしなければならないのは、プライバシーの権利で何を守るのかということだ。それについてはドイツでも今取り組んでいる問題だ。

もともとの連邦憲法裁判所の国勢調査の判決では、情報自己決定権は所有物のようなものだと。自分のデータの所有者は自分であるということだ。所有権は侵害してはいけないというような考え方だった。

しかし、それが常に正しいわけではないということがだんだんわかってきた。データというのは社会の中でめぐりめぐるわけで、そのようなアプローチをするとなかなか正しい道には行かないということで、それが非難されている。

情報自己決定権はデータを守るということではなく、その権利が言っているのは、ほかの脅威が実現しないようにするための予防的な保護。それはもちろん自由と自立性にかかわるものだ。全く保護されていない状態でデータの侵害を受けた場合、どういう人が侵害しているかはわからない。その場合、自分自身の像が全く違った形で流布される可能性がある。そうすると自分の自律性がなくなるわけだ。

自律性というのは、自分が何を公表するかをちゃんと決められること、そして自分がどういう者でありたいかを制御できること、その上に立って自分の自由をどうやって行使していくかということだ。そのプライバシーのレイヤがなくなってしまえば、ほかの自由の行使に関しても非常に危険な状態になる。この脅威から守るということが、情報自己決定権の基本的な考え方だったと思う。つまり、自律性が脅威にさらされることを防ぐ。自律性に対する脅威は忍び寄ってくるものだ。基本権を考えなくても、全く知らないうちに忍び寄ってくる。アメリカではそういうのはないということだが。

一つ想像してみてほしい。学生が１週間、誰かからずっと監視されている状況で生活してみる。そうなるとどうなるだろうか。とる行動が変わってくる。戦略的に行動するようになる。

そのセミナーでは、学生にもどういうふうに感じるかということを聞いた。アメリカではテロに関して関心は高い。特定のテーマに関してインターネットでリサーチをするときデータベースにアクセスして、そのときブラックリストが出てきた場合、アメリカは監視社会なのでそういうものが見つかれば飛行場でも止められる。なので、テーマの選定にあたっても考えなければならない。要するにさまざまな検閲があるわけで、学生は事前に非常に戦略的にいるので、そういうテーマは選ばないようにする。

そのような事態に陥らないように、自分の本当のプライバシーのエリアを確保するということ、全く干渉されない空間をつくるということ。脅威が忍び寄ってくるというところが非常に問題なわけで、まさにそういうところを情報自己決定権は考えているということだ。自由、自律性が脅威にさらされないように、予防的に考えるという考え方だと思う。アメリカではそれが保護されていない。これは現在、ドイツだけではなく、EU でも非常に広がっている。

しかしアメリカでも、こういったものが必要だということを自覚していらっしゃる方は増えている。学術の場においても、プライバシーの権利を拡大すべきではないかという議論がある。ほかからプライ

バシー権を強くしなさいというような動きもあるし、アメリカの判例もそういうものがある。しかし、それがストレートなものではないということもあり、なかなか確立するのは難しいという状況がある。ドイツの場合はアメリカとは法律の展開の仕方が違うので、脅威が目に見えてきたときは、アメリカでもそういう影響を受けた判決が出てくると思う。

情報自己決定権は自律性を守るもの。それは行動の自由だけではなく、外部における自由、そして内部における自由。それも自律的に守るという、予防的に守るという意味がある。

板橋　私はポッシャー先生と四方さんにコメントと質問を用意したが、時間の関係もあるので、ポッシャー先生へのコメントと質問に限らせていただく。

まずコメントだが、ポッシャー先生のお話の中で、国内の安全を守るための国家による監視措置等の安全法制についてのアンビバレンスについて、「まさに憲法にとっての難題だ」と表現されているところが非常に興味深いと思った。そして、「新たな脅威に対する新たなツールを用いた対処」と「意図せぬプライバシー侵害」、その両面を考慮しなければならないと指摘されている点も、なるほどと思った。

また、先生はこのような憲法の課題について、有無を言わさず「ノー」ではないと言われている。そして、国際テロリズムの脅威に対しては、日常的な危険のような具体的なものとなるまでは、すなわち具現化するまでは、警察が動いてはならないということではまずいというご指摘をされている。憲法は、新たな脅威に対しても考慮を払う必要があるとしているが、まさにこの研究会もそういう思いで始まり、現在まで続いてきていると思った次第だ。

1点質問だが、先生は、ドイツは1995年の日本での地下鉄サリン事件のような大きなテロ攻撃は経験していないにもかかわらず、安全法制をめぐる政策は過剰な反応へと傾きがちであったと指摘されている。しかしながら、まさに地下鉄サリン事件を経験した、首都の東京の地下鉄で大量破壊兵器を用いた大規模テロ事件を経験した日本において、テロを未然に防ぐための情報収集の制度が不十分であり、例えばテロや組織犯罪対策のための本人確認法がない。ネットカフェやレンタカーなどを利用する者の本人確認が日本ではなされていない。一部、東京都で条例等ができているが、法律としてはない。それから、行政傍受のような制度も整備されていない。

大規模テロを経験したにもかかわらず制度が整備されていない日本を、先生はどのようにお感じになるのか。抑制的であるとお感じになるのか、もう少しちゃんとしたほうがいいとお感じになるのか、お聞かせいただければと思う。

ポッシャー　私が本日の皆様の講演を通じて学んだことは、多少驚きも含んでいる。というのは、通信の保護に関して法的な根拠としてはあまり大きく介入の余地がないのだということがわかった。皆さん全員がこれから考えなくてはならないのは、どの程度そのような措置が必要とされているのか。それは議論の中でも登場したことだ。

ドイツの反テロ法でもいろいろと議論があったし、諜報機関と連邦政府は、議会に対してどのようなツールをどのように投入したかということを報告しなければならない。報告の中にもあったように、実は思ったほどそうした手段、対策がとられなかった。中には、ツールはあるけれども一度も使われなかったツールもあった。

そうなると、では本当に必要なのかという疑問が当然わいてくる。人によってはいろいろ解釈もあったし、責任者、担当者も、使いづらいのだとか、いろいろな意見があった。中には、警察が成功をおさめるために必ずしも必要なツールばかりではないのではないか、そんな意見も当然あった。

これまでドイツの議論の中で我々が学んだことは、いろいろなツールをどのように形成するのかということは考えるだけの価値はあるということだ。当初、こういう権限を割と一括的にまとめて使うようにしたということがあったので、手続法上はもっと細かく見ていった方がよかったのではないか。どのようなときにどういうツールを使うのかをもう少し詳細に決めることによって、どのような脅威に対して、何を使うのかを決めることが、有意義ではないかと思う。

日本は、これまでほかの国々が何をしてきたかを見て判断できるという、とても有利な立場にある。私の提案としては、さまざまなツールを一括的な形でまとめて導入ということではなく、それぞれのツール、それぞれの手段をどのように投入するのか、どのように使うのか吟味されることをお勧めする。

そして、通信データの保全というのはかなり踏み込んだ手段であるということをぜひ覚えておいてほしい。今や誰もがスマートフォンを持って歩いている。そして、EUの指令によると6カ月以上2年間保存するということになっている。ということは、皆さんが今、1分、そして1分後、3分後、この先2年間、1分1分、どこにいるかということが全部記録される。ドイツのある新聞が実験を試みたことがある。この日この時間にこの医者に行った、こういうがんにかかっている、そのがんがこういうふうに転移した、全部全部記録されてしまう。

国民1人1人に対して2年間そういう情報を本当に保存する必要があるのか。それは、来る脅威に対して予防するために本当に必要なのか。その通信データ保全に取ってかわる何か代替案はないのか。もう少し考えてみる必要があるのではないかと思う。通信データの保全は、確かにプロバイダに要望をしてたデータを必要な時点でクイックフリーズ、凍結させるだけで十分ではないかということも併せて考えていただきたいと思う。

ドイツでは今、EUレベルでEU指令の実施を求められているが、その中で、EUレベルでももう一度議論し直して、本当に包括的な記録、すべての国民のデータを最低6カ月、行動範囲、生活に関連している行動すべてに関して6カ月から記録しなければいけないのかということを、これから議論することになっている。

横内　その中で先ほど冒頭に申し上げた、次の警察活動と通信の秘密というようなことで、ポッシャー先生がツールというようなことで、一括してまとめてではなくて個別に検討していくと、まとめに近いこともおっしゃっていただいた。

今、随所に通信傍受、行政傍受のお話もあったので、時間の関係で、今まで触れられていなかったところで触れておきたいところについて、幾つか協議をしてみたい。

まず、通信傍受のほうは石井先生と四方部長からもかなり詳しくあったし、ただいま小山先生からもドイツの状況等についてかなり詳しくご説明があった。これについては先ほど石井先生の話にあったとおり、さっき先生のおっしゃった、まさに罪種、対象犯罪を絞られているのを拡大する方向で現実に議論も行われているということなので、あと、何か今後の課題的なことで石井先生、何かさらに付言しておありだろうか。

石井　特にない。ちょっと考えてみるのは、例えばテロの場合についてどうするのかというようなことが本当はもっとあってしかるべきだとは思っているが、そういう議論があまり進んでいないという印象を持っている。

横内　通信傍受では、先ほど林先生からも少しお話が出ていたいわゆるインテリジェンスを目的にしたいわゆる行政傍受、これは日本ではそもそも認められていないが、これも今、板橋室長のお話の中にも

出てきたが、林先生はこの問題に関して何かさらにおありだろうか。

林　個人的な体験を話してよろしければ、2004 年に情報セキュリティ大学院大学をつくったときに、どういう学生を集めるのかという議論をした。最初はコンピュータセキュリティのような技術論で行こうということで、想定する学生の 7 割は技術系、3 割ぐらいが社会科学系ということで考えて始めた。実際はそのような比率で大体来て、満足するほどたくさん来ていただいてはいないが、来ていただいた方を分類するとそうなるが、技術系の 7 割のうちの 3 割ぐらいが実はマネジメントをやりたいと。会社で技術のほうは結構やっているので、マネジメント寄りでやりたいと言って、そちらになってきた。

私は最初のときから、サイバーテロみたいなものがその当時はまだそんなにはなかったが、ナショナルセキュリティを含めた情報セキュリティをどうするのかというのはずっと考えていた。しかし、それを前面に出すほどのノウハウもないので様子を見ていたのだが、だんだんそれが出てきて、今は警察も含めて防衛省やいろいろなところからも来ていただいたりして、だんだんそちらに行っている。

やはりセキュリティを考えていくと、それは情報セキュリティと言って絞ったところで、国を守るということと密接不可分になってくる。通信の秘密を考えるときには、犯罪に対するどうするかということと同時に、インテリジェンス活動の際にはどうするのかというのは検討しなければいけないのではないか。

今日のドイツの例は大変参考になった。アンビバレントなのは確かだが、その中でどういう仕組みを工夫すればいいのかを非常に明確に教えていただいたような感じがする。そのような観点からさらに検討いただければうれしいと思う。

横内　先ほど、ドイツの状況についてはポッシャー先生、小山先生からお話があったが、行政傍受では特にアメリカでは 9.11 以降、テロへの戦いということで相当広範囲にインテリジェンス目的の傍受が行われているとも言われている。この辺の事情も含めて、大沢先生は何かコメントがおありだろうか。

大沢　アメリカにおいて行政傍受は当初、9.11 以前はむしろ否定的であった。それはニクソン大統領のときのウオーターゲート事件のときに問題があって、インテリジェンスと捜査機関が一つになることによって、さまざまな情報が個人にとってあまり好ましくない形で用いられる。それから、組織も分離するということがあった。ただ、必要な場合については特別な裁判所を設けて、インテリジェンスと捜査機関との情報共有について考えていくという形をとってきた。

それが 9.11 以降、その垣根を取り払うという動きが愛国者法等で実際に行われてきたということかと思う。ただ、アメリカにおいても、最近の事情はあまりよく知らないが、基本的には両者は分離すべきだという考え方が強く背景にはあるかと思う。

アメリカの場合には大統領のリーダーシップがあり、特に戦争時においては大統領の権限を強くするというようなことがあったために、軍の司令官である大統領の権限の中でそういう情報の共有が進められたということがある。それが冷めてくれば、アメリカにおいては、組織あるいは権限の面でまた分離しようという動きが出てくるのではないかと考えている。

横内　それでは次に、携帯電話の GPS 機能を用いた位置探査に行きたいと思う。先ほど石井先生から、総務省のガイドラインが一昨年に改正されたということで、裁判所の令状だけでは足りない、本人への通知が必要だというふうに今はなっている。先生は、ガイドラインの措置は不要ではないかと先ほどもはっきりおっしゃっていた。私も、実務上 GPS を使った位置探査が実施された例はまだないと聞いている。実務上、本人への通知というのが大変大きな足かせになっているのだろうと思っている。

これに関して、先ほど石井先生からお話があったが、さらに先ほどのお話を敷衍して今後の課題なりについてコメントはおありだろうか。

石井　ガイドラインの実質的な理由は存じ上げないが、発想的には、捜査機関側が事業者を通じて当該端末に対して GPS の位置情報を送れという形でやるので、通信が発生している、だから通信の秘密の問題がかかわってきて、そのためにプライバシーの侵害にかかわるので通知しなければいけないというのが、総務省側の発想だと思われる。

ただ、先ほど言ったように、通信の秘密といっても、どういう会話をしたのか、どういう内容だったかという意味における通信の問題は強く保護しなければいけないと思われるが、この場合は単なる位置情報だから、どこでという形にしかすぎない。令状によって、そういったものを捜査機関が察知して構わないということが認められているので、それで十分正当化できるだろうと考えている。

横内　これについては総務省のガイドラインの解説を見ても、ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高いことから、令状に加えて、本人にはそれを知ることができないといけないと書いてある。憲法の観点から小山先生、このあたりについていかがだろうか。

小山　これはなかなか難しい問題だ。所長がおっしゃったようにプライバシーの中でも特に保護の必要性が高いということだが、どれだけ保護の必要性が高いのかということが一方ではあると思う。

先ほどのポッシャー先生のお話であったように、絶対的に侵してはいけないほど保護の必要性が高い領域というのもある。例えば個人の住宅の中、夫婦 2 人でいるようなところでの盗聴をやってはいけないなど、そのような場合だ。そこまで至るかというと、もちろんそこまでは至らない。

また、位置情報をとっているうちに、保護の必要性の高いような現場に陥るかどうかというと、位置情報だけであれば多分それもないと思う。

もちろんこれは保護の必要性が高いので、やみくもにとってもらっては困るということは言えると思うが、特に保護の必要性が高いと「特に」をつけて強調するほど高いのかどうかというと、私にはよくわからない。どれくらいの頻度でとるか、どれくらいの期間とるか、そういったことにもかかわってくる問題だろうと思う。

もう一つ、これはほかと比較すればいいと思うが、大盗聴ほどすごいことではない。例えば通信傍受と比較した場合どうなのか。通信傍受の場合のほうが、侵害の程度は大きいように感じる。したがって、対象犯罪をどういうふうに定めるか、令状を発する場合にどういう要件があれば令状を発することにするか考えていく場合に、通信傍受ほど厳格ではなくてもいいという感じがしている。そこからすると、先ほどご質問のあった当人への通知、利用者が知ることができるというのは、これをやったらそもそも〔公衆法？〕は成り立たないし、実体的にもそこまで要求するほどのものではないような感じが私はしている。

横内　実務のサイドとしては、憲法の先生から大変心強いコメントをいただけたと思っている。これも議論すれば尽きないが、時間の関係で、各論の最後ということでログの保存に移らせていただく。

これについては石井先生からもあったし、特に四方部長から、これは監視でもないし、そもそも通信の秘密を守るためにも必要なんだというお話があった。これに関しては大沢先生からご質問があると伺っているので、どうぞ。

大沢　私が最初に考えていた質問は、四方さんのご報告の中でサイバー犯罪条約におけるログの保存条項と諸外国の対応についてということで、アメリカ・日本・ヨーロッパの対応の相違が話されていたか

と思います。アメリカ・日本では、犯罪の嫌疑が生じた時点以後にログの保全要請が行われる。そのことについて事後追跡可能性というか、言葉でとらえて、それが法治主義や法の支配と密接不可分な関係にあるという理解をなされていたかと思っている。

その密接不可分というのは、どの程度のことをおっしゃっているのかというのが質問の趣旨だ。具体的に言うと、ログの保存について民間の事業者に対して保存の要請、保存を義務づけることまで考えることは可能とお考えなのかどうかということである。

四方　ロジックの途中が飛んでいたのかもしれない。現実社会でも確かに、犯罪が行われてから聞き込み捜査をしたり、場合によっては防犯カメラ、先ほど議論になったＮシステムなどいろいろなものを使ったりするわけだが、リアルの世界においては過去を追跡するツールがそれなりに幾つもある。

基本的にはサイバー空間は、今後技術が発展していくとまた違うのかもしれないが、通信ログの追跡でないと、この間の遠隔操作の関係も現実世界に持っていって捜査したという話もあるが、サイバー空間の中での捜査で行くとログの追跡しかない。ログの追跡ができないということは、違法行為が行われた場合に、行政的な措置にしても捜査にしても裁判にしても、結局何もできなくなる。そのぐらいの単純な話を申し上げたかっただけである。

その際に、嫌疑があってからの保全と一律の保全とでどういう違いがあるかというと、犯罪の発覚は往々にしてかなり後になることが多い。日本の実情で行くと大体、現在では法的な義務づけはないが、事実上、通信プロバイダの場合は2～3カ月程度保存しておられる場合が多い。2～3カ月後に発覚したものは追跡は全くできない。後で頼むとか何とかというのがそもそも空振りに終わる。初めからとってあってこそ、後で見つけて追跡ができるわけだが、少し発覚が遅れると全然追跡ができないという意味で、実はアメリカ・日本方式とEU指令方式とではかなり大きな違いがある。

確かに、EU 指令方式は包括的ではないかというご指摘はごもっともだが、先ほどからも議論があったように、ログというのは、先ほどの話にもいろいろあったが、通信内容まで保存させるわけではない。誰に対していつ通信があったかという、そこのところだけの記録なので、そういう意味で、個人の尊厳に対する侵害の度合いが随分低いのではないか。

通信ではないが、例えば我々捜査当局から見ると、類似の記録という意味では、銀行取引やクレジットカード情報の記録など、ある意味では人々の日常生活がもっとよくわかるような、中身も含めた記録がもっと長いこと記録されていることとのバランスからすると、通信ログについては足りないように感じるのが率直なところある。

法制面については、私の立場からどうこうと言える話ではないが、警察のほうでイニシアティブをとってという話では少なくともないかもしれないが、諸外国で実際にないことはない法制なので、論理的にはないことはないのかなと私個人としては理解している。

横内　ただいまの四方部長の答弁にあったとおり、犯罪の嫌疑が生じてから要請してするのでは、現実の犯罪の捜査としては極めて支障があるということで、EU 方式というか、そちらのほうへの言及があったと思う。

一方で、先ほどポッシャー先生から、やはり通信のデータの保全は重大な侵害行為であるというお話もあった。ドイツの状況はわからないが、日本の場合は、保存するのはそれぞれの通信業者でして、そこがいかにきちんと管理をするかという問題があろうかと思う。

警察がそれを必要な場合には、改めてそこで裁判所の令状を持って、それで必要な情報だけしか見る

ことはできない。そういった点では、仮に今のような形でなくて、四方部長が話したような、もっとさかのぼっての保存義務があっても、それほど大きな侵害は生じにくいのではないか思う。

ポッシャー先生から、今の日本の制度を踏まえて、先ほどデータの保全についてコメントがあったので、若干今の点についてコメントをいただきたい。

ポッシャー　いろいろな方法があると思うが、このデータ保全に関しては、あまりにも包括的過ぎるということで、EU委員会でもまた新たな議論が起こっている。

一つの代替法として議論されているのが、クイックフリーズ手法というものだ。それによって敷居を少し低くする。限定的に保全する。もちろん根拠が要るわけだが。特定の人について、コンタクト先、そういったデータを保全するということだ。過去の捜査との関連もあるが、捜査にどれほどの影響を与えるか、クイックフリーズでどれだけのことが得られるかを検証していく必要があると思う。データ保全を限定化するか、あるいは今のように包括的にするか、その二つのどちらの道をとるかで随分変わってくると思う。ドイツもまだそれに関しては最終的な答えは出ていない。

もう一つ、例えば包括的な保全をしようとした場合に重要なのは、第2ステップとして、データへのアクセスに対して高い敷居を設けることが大事だと思う。その点において、連邦憲法裁判所がやっていることに私はあまり満足していない。

全体のデータがあって、それは動画があったり、さまざまな関連性が見えたりする。嫌疑がなくても、ログを見れば、その人に対する情報がわかってくる。例えば誰と誰が浮気をしているとか、そういうこともわかってきたりする。例えば医者に行った、弁護士に相談に行ったなど、そういったこともわかってしまう。

ログの記録は、それだけでかなり危険なことだと思う。個人情報がかなり漏れる。あるいは、どういう新聞を読んだか、どういう記事を読んだか、インターネットでアクセスすればどういう内容を読んだかもわかってくる。そういうことを考えると、やはり敷居は高くしておく必要があると思う。

手続法的保障も必要だ。本当にその目的のためだけに使われるようにするということだ。そのデータに標識をつけるとか、そのデータがどこから来たのか。捜査当局からではなくほかから来たということ、そのデータの出どころがちゃんとわかるようにするということも大事だと思う。

さらに、濫用されないように、チェック機構も確立する必要があると思う。膨大なデータがあるわけなので、濫用されれば大変なことになる。例えば政治的な操作に使ったり、濫用の仕方もいろいろあると思う。政治面からのチェック機構も必要だと思う。どういうチェック機構をつくるか、それも考えなければならない。それによって、EUが考えているような、通信データの保全を法治国家的にまともな形にするという可能性もあると思う。

連邦憲法裁判所にとっても簡単な決定ではなかった。国勢調査に関して全く根拠のないデータ収集は許さないと言ったわけだ。通信データの保全というのは、まさに根拠のないデータの収集になってしまうわけで、そのデータを収集する段階で全くその目的はないわけだから、そういうことを考えると、連邦憲法裁判所も非常に難しい立場にあると思う。

しかしEUは、違憲なEU指令が出ているということなので、非常に難しい状況になっている。この通信データの保全が常に違憲であるというわけではないが、やはり何らかの措置が必要だ。この方向に行くとしたら、繰り返しになるが、データのアクセスに対する敷居を強くする、そしてチェック機構をしっかりと設定する、そういったことが非常に重要になってくると思う。

林　割り込んで申しわけないが、実効性のところも含めて議論したほうが将来的にはよいと思う。先ほどオニオンルータの話があったが、経路をタマネギをむくようにむいて残ったところしか伝えないので、さかのぼれないというのがあった。セキュリティの技術は守ると攻めるの交互のやりとりのようなもので、どれだけ実効性があるかということも併せて考えたほうがいいというのが一つ。

それから、途中を中継している人は多種多様な人がいる。信頼できる人もいれば信頼できない人もいる。犯罪行為に絡む人は信頼できないところを使うに決まっている。その面でもどうかなという感じもする。

全体を検討するのがまず最初だという四方さんのご提案だろうから、その点は同意するが、併せて実効性も検討しなければいけないという気がした。

横内　ポッシャー先生からは最新のドイツ・EU の状況をご紹介いただき、林先生からも実効性という重要なポイントをご指摘いただいた。

通信の保護のあり方

横内　予定の時間が迫っているが、冒頭に申し上げた通信の秘密の保護のあり方に触れておきたいと思うので、若干時間が延びてしまうかもしれないがご容赦いただければと思う。

通信の秘密の保護範囲については、林先生から具体的なご提案をいただいた。また、四方部長、石井先生もこの趣旨でのご発言があったと思う。

通信の秘密に、通信の内容だけでなくて、その存在や外形から知ることがいろいろできる事柄等も含まれるというのが通説だということだが、例えば、これは実務上の話だが、通信履歴を令状で差し押さえるときに、そもそも例えば保存期間が経過して通信履歴を持っていないようなところでも、その持っていないということすら現状では令状がないと教えてくれないのが現状だ。

通信履歴の有無が通信の秘密に含まれるとすれば、その延長線として運用がなされるということもあり得るのかもしれない。いずれにしても実務上の問題もあり、およそ通信内容が推知され得ないようなときでも、現実にそういった対応もなされている。

そういった現状も踏まえ、これについては林先生からかなり具体的なご提案も、3 層に分けるなどいろいろご提案をいただいたので、それに関連して皆様からご意見なりコメントをいただきたいと思う。まず、大沢先生と板橋先生からはこれに関連してご質問もあると伺っているので、まず大沢先生。

大沢　石井先生に対する質問のところで、最後のところ、信書に相当する電話とはがきに相当するインターネット通信の区別ということで、はがきの場合には第三者を排除する意図を持たないという点で信書と異なるというような意味かと思ったが、はがきとインターネットの関係は果たして同じなのかという気がした。

これは通信の秘密の保護範囲とも関係するかと思う。通信の秘密についてと通信の構成要素について明確に区別できるのだという考え方がその背景にあると思うが、このこと自体について私自身としては納得がいかないところもある。

所長がおっしゃるように、はっきりというのは難しい気がする。はがきがあり、信書があり、さらにインターネットが出てきたという背景の中で、事情を複雑にしている気がする。この点については最後にお話をすべきかもしれないが、プライバシーの権利についても、憲法の学者として憲法学でも個別具

体的な形でとらえていこうということがある。それは情報の概念というものが導入されて、それが多様であるということが前提になっている。したがって、個別具体的にもう少し対応していくということではないかと思った。

その意味では、はがき・信書・インターネットの対応をどのように考えるべきか、この対応が適切なのかという気が少ししたので、ご質問をした。

石井　例えが悪かったのかもしれない。はがきはご存じのとおり、差出人とあて先が書いてあると同時に、通信内容も平で書かれているから、はがき1枚に外形的情報から通信内容まですべてがある。おそらく、インターネットの通信も同じようなものになっている。パケットの場合はペイロードとそれ以外のところと一体になっている。という意味で、類似性がある。

結局は、通信事業者にしろ、途中の経由地の人たちにしろ、そのものを拾って見れば、悪意があるかどうかは別にして、見ようと思えば通信内容まで見られる。しかし、途中の人たちは恐らくはその辺は善意で、あて先のところだけ見ながら配達をしていくという状況がある。そのようなものは、通信内容保護といっても、そんなに厳格にされなければいけないのかというのは、疑問に感じているところがある。ただ、それでも通信内容であるから、保護しなければならないというのは認める。

もう一つ、はがきだということの言いたいことは、特に電子メールなどに関してはそういうことが強いと思う。電子メールを送信して受信サーバにたまっているメールは通信事業者の管理するものであるから、通信の秘密の対象になってくるはずだ。それを押収しようと思えば、傍受令状によらなければいけなくなってくるだろう。

はがきの場合は刑訴法100条があるので、その規定に従ってやっていけば足りる。電子メールの場合には、ISPのメールサーバに存在している電子メールについても、100条に準じたような扱いができないのかという対応関係が、まだよく整理されていないのではないかと私は感じている。

インターネットは確かに通信を使うわけだが、実際社会において見たときに、電話のような通信ではなくて、日常生活の行動の一部ではないかという部分が強いのが一つ。電子メールといっても、はがきぐらいの程度のものでしかないということがある。そうしたことにもう少し即したような法規制があってしかるべきだろう、ということを申し上げたかったということだ。

大沢　はがきも裏表があって、通常は表しか見ない。インターネットの場合はもう少し複雑な要素が入ってきているし、情報としてもさまざまな段階の情報がネットの中に入ってきている。はがきと同じにということではなく、インターネットはインターネットの特性を踏まえた形での判断をしていく必要があるのではないかという気がしている。

林　この図を見ていただきたい。私も石井さんと同じようなことを考えた。半分は支持して、半分はクエスチョンマークになるかもしれない。もともと、secrecy of communications の原点は secrecy of correspondence で、郵便の秘密だ。そのときに今の石井先生の議論はあり得たし、少なくとも封書の場合は中身と表書き裏書きは区別できた。

ところが電報になったときに、電報を覚えておられる方はこの世界におられないかもしれないが、頼信紙というのがあって、あて先と通信文を一緒に書いて処理するようになった。電話を交換手が交換するようになったときも、一挙に6通話ぐらいさばくのでずっとモニターしているわけではないが、中身とあて先は一緒の人が扱っているということになった。電話が自動交換になってもそのやり方は変わらなくて、途中で共通線信号方式というのが入ってきて、信号の情報と通話の内容を別チャネルで送るこ

とができるようになった。

それの行き先がさらにインターネットになって強化されたという感じになっているので、分離可能というところまでは私は石井説に同意だが、分離可能だからこうしなければいけないというところは議論があるかなという意味では、大沢先生に同意という、そういう立場に私はいる。

横内　林先生のご提案も含めて、保護対象に応じた保護のあり方を考えていく必要があるのではないかというのは、先ほどの発表でも皆様の共通認識だと思う。林先生のご提案についてコメントのある方がいらっしゃれば、挙手なりしていただければ。あるいは、最後のまとめで一言ずついただくときに言っていただいてもよろしいが。

会場からご質問も若干いただいている。時間の関係で一つだけ、これは林先生に、社団法人日本インターネットプロバイダー協会のキムラタカシ様からのご質問。プレゼン資料の７ページで、電気通信事業者以外には通信の秘密の保護の義務がないと書かれているが、そのようなことはない。この点についてコメントをいただきたい。

林　私の言い方が悪かったので、このようにご理解いただきたい。石井先生ほかでご指摘があったように、何人も守らなければいけない通信の秘密というのはある。その条文は「何人も」であるから、電気通信事業者以外にも係っているという意味で、そのことを私が抜かしてしまったので、申しわけない。

片方で私の説は、通信の秘密と他人の秘密を分けるということなので、他人の秘密については事業者でなければその責任を負わないという意味で、あの規定の適用はないということになる。

なお併せて、日本の事業者は皆、電気通信事業法で事業者の届出をしているとおっしゃるのは、大手はそうだと思うが、そうではない人もいるのではないかと思って発言した。もっと念頭にあったのは、アメリカ系のグーグルなどは日本の電気通信事業者ではなくて、市場シェアや重要性で考えるとそれは結構大きいので、それを念頭に置いていたということでご理解いただきたい。

横内　あと何人かの方からご質問をいただいているが、まことに申しわけないが、時間の関係で割愛させていただきたい。

本日は大変広い問題でいろいろな議論があった。本日の議論あるいは質問を踏まえて、最後にお一方ずつ全員の方からコメントをいただければと思う。

大沢　今日は、憲法学の方から見て非常に有意義な日であったと思います。というのは、プライバシーの権利について、柔軟に考えていくということと個別具体的に対応を考えていくということが指摘されたからです。その場合に、先ほど言ったような侵害の程度や範囲、保護の必要性など多くの要素を慎重に考慮する必要があるが、個別的な対応を積み重ねていくことの重要性が改めて明らかにされ、それが確認されたと思います。

今日は林先生のように、これまで長年経験がおありの方から、またそのほかの方からも有益なお話を聞けたということを非常にうれしく思っております。そこでの議論等からいくつかの点をとくに強く感じました。たとえば、ポッシャー教授のお話もお聞きすると、ドイツにおいては議会と連邦憲法裁判所の関係によって、変化する事態に対応するシステムができ上がっているのではないかという気がしました。法治国家的な対応ということなのだろうと思います。法律が執行され、その執行の在り方を再考するという形を通して、連邦憲法裁判所が憲法判断などを示すという形で、積極的に情報化社会に対する対応が前に進んでいるという印象を受けました。

これに対して、アメリカにおいてはそのような対応ではなく、議会があまり機能しない状況の中で、

大統領と裁判所との関係という中で対応しているように思います。それは、いわば政治的な、あるいは民主的なコントロールの中で対応しているのだと思います。

その点で、日本ではまだいずれの考え方もあまり展開されていないように思います。これから議論が始まるところかなという気がしました。そういう意味では、こういうフォーラムを積み重ねる必要があると思います。ポッシャー教授がこれからの日本に対して、外国の様子をしっかりと見て、いいものを取り入れるべきではないかとおっしゃったのは、日本の状況を踏まえて考える場合に有益のように思いました。その意味では、フォーラムの形で皆さんの関心が高まるような動きが出てきていることが、これからの動きのきっかけになればと思っています。その意味で今回のフォーラムは意義があったのではないかと思います。

小山　ごく簡単に１点だけ。今日は通信の秘密が随分問題になったが、憲法はあまり議論されていない分野がある。通信の秘密は憲法21条という花形の条文の中にあるのだが、21条の１項ではなくて２項のほうに入っている。

私が思うに、通信の秘密の本性がプライバシーなのかそれとも表現の自由なのかという、そういった議論はあまり生産的ではないと思う。憲法上の権利は、表現、プライバシー、宗教と縦割りでやっていく場合もあるが、結社の自由のように横割りでやる場合もある。すべての人権が縦割りとは限らない。通信の秘密は、縦割り的な部分はあったのだろうけれども、もう少し横断的な性格もあるのではないかと思っている。

もう一つ、通信の秘密に関してだが、ほかの憲法上の権利と同じように、通信の秘密にもコアになる部分と周辺的な部分とがあるはずだ。通話の内容がコアの部分だとすると、通信に関する事実はその周辺的なものだと思う。

それによって制約の可能性や要件なども変わってくるはずだし、逆に言うと、通信の秘密を広げれば広げるほど、制約の可能性も広く認めないとバランスをとれないというのはそのとおりで、どう考えるべきかだ。通信の事実を通信の秘密から切り捨てるというのは本末転倒な発想だ。そうではなくて、ここまで広げた上で、かつ制約の可能性を比較的広く考えていく。そういった考え方の順番がいいのではないかと思う。

通信の秘密が、通信の事実を切り捨ててしまうことになると、先ほど所長が「通信があったかどうかを聞くだけでも令状を持ってこいと言われる」とおっしゃった。それは当たり前で、そういった嘆きを最初から封じ込めるために、ここまで広げる必要がある（笑）。

板橋　３点ほど簡潔に。１点目は、林先生のお話の中で電気通信事業者と情報処理業者との違い、これは非常に興味深い。ヤフーは電気通信事業者で、グーグルは情報処理業者。情報処理業者だと電気通信事業法の適用を受けない。しかしよく考えてみると、どちらも日本でメールサービスをやっているのはなぜだろう。アメリカの力なのかというのが１点。

２点目は行政傍受についてだが、私はそろそろ検討すべき時期にきていると思っている。ただし、どのようにコントロールするか、歯どめをかけるかという問題がある。日本の議員の方々がどのくらい守秘義務を尊重してくれるのかという大変な問題がある。欧米諸国では議会がコントロールしているわけだが、我が国においては非常に大きな問題があると考える。先の秘密保全法制の議論においても、議員は対象から外せという議論があったと承知しており、そこは問題だと思っている。

３点目はログの保存について。ポッシャー先生がおっしゃったとおり、確かに利用については慎重で

あるべきだと思うが、そもそも事業者に保存義務を課さなければ、それ自体が残っていないということが起こり得る。やはり、一定期間のログの保存は事業者に課すべきだと思う。

この議論がどうなってしまったのか私はわからないが、アメリカでは通信容量の拡大で課金システムをつくろうかという議論がなされていたように思う。課金システムをつくると、当然ながらログは一定期間保存しなければいけないことになるので、こういう議論と併せて、事業者においても一定の義務を課す必要があるのではないかと私自身は考える。

林　まずは、このような機会をいただき、私の発表もさせていただいて、大変感謝している。通信の世界は専門領域だと思われている。私が今やっているセキュリティもどうもそう思われているようで、なかなかメインストリームの方と丁々発止やる機会がないので、大変感謝している。こちらのほうもそういうところへ出ていく努力をしたいと思うが、ペリフェラルだと思わないで、引っ張り出すほうも今後やっていただけると大変うれしい。

ポッシャー　皆様にご招待いただき、このような場をいただいたことに御礼申し上げる。皆様と日本の動向について意見を交換させていただけたこと、大変うれしく思う。日本のことはあまりよく知らなかったので大変よかったと思う。

ヨーロッパの大陸やアングロサクソンということではある程度わかっていたのだが、日本においてすぐに過度な反応をしていないということがわかった。今の日本の状況はチャンスであると私は思う。成熟した安全法をつくれるチャンスが皆様にはあると思う。ぜひとも皆様にはこれからの成功をお祈りしたい。

四方　私も大変貴重な機会をいただいて感謝している。

１点だけ補足させていただく。私が事例を五つほど紹介した中で言いたかったことの一つだが、国家による侵害ではないが、個人のパソコンの乗っ取りあるいは情報漏洩は、今日のメインの概念の一つが個人の尊厳あるいはプライバシーの保護だと思うが、パソコンを乗っ取られた人の尊厳はめちゃくちゃというか、とりたいものは全部とれるわけだ。

個別の事件については、被害者のプライバシーのために言うことがはばかられるが、皆さんも写真などをパソコンで保管されたりすると思う。まさしく夫婦の中だけの写真なども結構流出している。最悪の個人の尊厳の侵害のようなことが、私人間で行われている。乗っ取ってその人になりすまして、爆破予告するというのも随分ひどいものだと思う。

いずれも、通信事業者のパソコンを侵害するというのは直には難しい。個人のパソコンあるいは中小企業のサーバの侵害は割とやりやすいので、そこから入っていく。末端のユーザーの中にあるメールの情報やいろいろな情報、通信の対象になるかもしれない情報は、ひょっとしたら電気通信事業法上の通信事業者の取扱中の情報ではないかもしれないが、その人が蓄えているメールの内容は、乗っ取って見ようと思ったらいくらでも見られる。たまたま通信用のID・パスワードまで盗って通信事業者のデータサーバまで行ったら電気通信事業法違反も成り立つが、個人の尊厳という意味では、結構ひどいことが起こりつつある。

私は３年前ぐらいに情報技術犯罪対策課長に着任して２年半ぐらいいたが、その間に予想よりもずっとひどい展開になってきているという思いをしている。もちろん、通信を使った人の身体、生命に影響を及ぼすような犯罪もあるが、通信の秘密の根っこになっている個人の尊厳、プライバシーを侵害する事案もあるということをご紹介しておきたい。

石井　今日はご招待いただいて感謝している。私は本当にオーソドックスな刑法学者でドグマティカといいますか、こういう状況は苦手なのだがいろいろ勉強させていただいた。

皆さんすばらしい感想をまとめられていたので、私は少し違った観点で申し上げる。恐らく、現在の通信の秘密に関する落としどころというか状況は、林先生が提案2のスライドにおいて示されたような3層構造の中においてなされている。捜査機関においては捜査事項照会でとれるのか、通常の令状でとれるのか、傍受令状でとれるのかという形で対応されていると思われる。

ところが実際の運用においては、どうも真ん中のところのあたりが傍受令状で行かなければいけない感じになっている。つまり、本来は通信の付帯情報のところが通信内容にされてしまっているところに問題があるのではないかと感じている。

もう1点は、捜査機関がするのか行政機関がするのかという問題はあるにしても、日本の国家や社会が維持する上で必要な事柄に関しては，法律上きちんとした授権をすべきだろうというのがあるが、我が国においてはそれがなされていない状況があるのではないか。

刑法ではよく最近では敵刑法（Feindstrafrecht）と言われるが、本来の法治国家的な刑法の外側というか皮をかぶりながら、中では非常に敵対的な形において侵害的な刑事法的な政策がなされたりする。あるいは、かつてカール・シュミットだと思うが、例外状態という形において憲法の人権保障の問題、法治国家的な原理を停止させることが認められている。必要な授権がなされていないところにおいては、それが隠れた形においてなされていくということになる。

そういったことを防ぐためにも、きちっとした議論をした上で、必要な政策的な立法をしていくべきだろうと私は感じている次第だ。

【閉会挨拶】

警察政策研究センター所長（当時）、現宮城県警察本部長
横内　泉

今回のテーマは大変重く、かつ広いということもあり、議論を掘り下げることができなかった。ただ、平成 11 年に通信傍受法ができたときには「通信の秘密」の議論は大変盛り上がったが、その後ずっと下火になっている。これだけ通信技術が発達して、いろいろな問題が生じている中で、あまり正面から取り上げられていなかったのではないかと思う。

そういった意味では、今回のこのフォーラムがこの問題を議論する一つのきっかけになっていけばと思っている。そのためには、今までどうしても「通信の秘密」が出てくるだけで、主張するほうもされるほうも何かそこで思考停止的になってしまっている部分があったのではないか。

まず対話というか、私どもの研究会そのものが憲法の先生方と警察実務家という、世間的には相性が悪いとされているメンバーで構成されているわけだが、まずいろいろと議論をし、対話をしていく中で、それぞれ得るところもあると思う。特にこういった非常に重要な問題については、今後もさらなる研究をしてきたいと思う。また、皆様方に対しても、このフォーラムをきっかけに、この問題についてのご認識が深まっていただければ望外の幸せと思っている。

最後までご協力、またおつきあいいただいた講演者、パネリストの皆様、会場の皆様に御礼を申し上げまして、パネルを閉めさせていただきたいと思う。