第百七十七回国会　衆議院　法務委員会議録　第十五号

平成二十三年五月三十一日（火曜日）

午前九時開議

出席委員

委員長　奥田　建君

理事　滝　実君　理事　辻　惠君

理事　橋本　清仁君　理事　樋口　俊一君

理事　牧野　聖修君　理事　稲田　朋美君

理事　平沢　勝栄君　理事　大口　善徳君

相原　史乃君　井戸まさえ君

大泉ひろこ君　川越　孝洋君

京野　公子君　熊谷　貞俊君

黒岩　宇洋君　黒田　雄君

桑原　功君　階　猛君

橘　秀徳君　中島　政希君

野木　実君　三輪　信昭君

水野　智彦君　山崎　摩耶君

横粂　勝仁君　河井　克行君

北村　茂男君　柴山　昌彦君

棚橋　泰文君　丹羽　秀樹君

森　英介君　柳本　卓治君

漆原　良夫君　園田　博之君

城内　実君

法務大臣　江田　五月君

法務副大臣　小川　敏夫君

法務大臣政務官　黒岩　宇洋君

政府参考人（警察庁生活安全局長）　樋口　建史君

政府参考人（法務省刑事局長）　西川　克行君

政府参考人（外務省大臣官房審議官）　武藤　義哉君

参考人（成城大学法学部教授）　指宿　信君

参考人（法政大学大学院法務研究科教授）　今井　猛嘉君

参考人（慶應義塾大学法務研究科教授）　安富　潔君

法務委員会専門員　生駒　守君

委員の異動

五月三十一日

辞任　補欠選任

棚橋　泰文君　丹羽　秀樹君

同日

辞任　補欠選任

丹羽　秀樹君　棚橋　泰文君

本日の会議に付した案件

政府参考人出頭要求に関する件

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案（内閣提出第四二号）

○奥田委員長　これより会議を開きます。

内閣提出、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案を議題といたします。

本日は、本案審査のため、参考人として、成城大学法学部教授指宿信君、法政大学大学院法務研究科教授今井猛嘉君、慶應義塾大学法務研究科教授安富潔君、以上三名の方々に御出席をいただいております。

参考人各位に委員会を代表し一言ごあいさつ申し上げます。

本日は、御多忙の中、御出席を賜りまして、まことにありがとうございます。それぞれのお立場から忌憚のない御意見をいただければ幸いに存じます。どうぞよろしくお願いいたします。

次に、議事の順序について申し上げます。

まず、指宿参考人、今井参考人、安富参考人の順に、それぞれ十五分程度御意見をお述べいただき、その後、委員の質疑に対しお答えをいただきたいと存じます。

なお、御発言の際はその都度委員長の許可を得て発言していただきますようお願いいたします。また、参考人から委員に対し質疑をすることはできないことになっております。どうぞ御了承をいただきたいと思います。

それでは、まず指宿参考人にお願いいたします。

○指宿参考人　私は、今回提出されております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案につきまして、専門であります刑事訴訟法の立場から意見を述べさせていただきますので、申し述べる範囲につきましては、刑法の実体法部分については省略させていただき、専ら手続法の部分について意見を述べさせていただきたいと存じます。

お手元に、横書きの「サイバースペースにおける証拠収集とデジタル証拠の確保」という資料が配付されているかと思いますけれども、これはちょうど今月発売の法律時報に、偶然ですけれども私が書きましたものが掲載されましたので、本日はこれをレジュメがわりに使わせていただきながら、この論文の要旨を御紹介させていただきたいと思いますので、ごらんください。

本論に入ります前に、ちょうど先週、五月二十五日、イギリスがサイバー犯罪条約の批准をいたしました。これで欧州、いわゆるＥＵ諸国におきましては三十カ国目の批准ということになりました。しかしながら、イギリスは二〇〇一年に条約に署名してから、およそ十年、批准までかけておるところでございます。これで欧州の主要諸国は皆批准したわけでありますけれども、そこに至るまで、慎重な国内法の整備や討議、議論を踏まえてのことだと承知しておりますので、当委員会におかれましても十分な御審議をお願いしたいと思います。

それでは、内容に入らせていただきます。

私の論文では三ページ目になりますけれども、「記録媒体の差押え」というところから簡単に述べたいと思います。

刑事訴訟法のこのたびの改正で、百十条の二を新設し、捜査機関が差し押さえるべき記録媒体、いわゆるメディアと言われるものに記録された電磁的記録を、他の別のメディア、記録媒体に複写、印刷、移転させることで、記録媒体の差し押さえと擬制する、みなすわけでございます。

これまではデータを直接保存した、あるいは記録した媒体からこれを直接差し押さえるという規定がなかったものですから、これをつくるということで、この点では、情報化社会を踏まえた十分な捜査の体制を整えるという意味で、非常に重要な改正だと認識しておる次第でございます。

個々の問題につきましては時間の関係で省略させていただきますが、私が問題と考えていますのは、二百二十条一項は、逮捕の現場での無令状の捜索、差し押さえ、つまり、被疑者を逮捕した場合に、その場で捜査機関は令状がなくても一定の範囲で捜索、差し押さえができることになっております、これは現行の刑事訴訟法で。その準用がこの記録媒体の差し押さえにも及ぶというふうに法案ではなっているところですけれども、ただでさえ外部から認識しにくい電子的なデータを逮捕の現場で必要な範囲で捜索、差し押さえするというのは、どのような形で行えるかということについては、全くこれまで議論されたことがないわけでございます。

法案の提出の理由では、データの差し押さえに

ついても十分な特定ができるということで御提案されていると思いますが、この点、問題ではないかというふうに考えております。

続きまして、記録命令つきの差し押さえに移らせていただきます。

刑事訴訟法の九十九条の二の新設で、記録命令つき差し押さえという類型を置かれました。これは、従来ですと、何者かに命じてデータを出せという場合に裁判所による提出命令等があったわけですけれども、捜査機関はそういうものを利用できないわけですので、こうした規定が新設されたと了解しております。ただ、この条文には命令不履行の場合の罰則がありませんので、間接強制にはならないと考えます。

もし要請を受けた場合に、これを断れば、次には差し押さえ、先ほどのデータの差し押さえという処分もあることですから、恐らく協力するであろうということが前提になっている規定だろうと思うんですけれども、その場合であれば、何者にでもこれを適用するのではなくて、本条項のもとになっておりますサイバー犯罪条約の十八条が協力的第三者を念頭に置いているようですから、本条項についても、何人も対象とするのではなく、協力的な第三者、例えば電気通信事業者や、多数の者の通信を管理する大学とか、大規模な利用者を抱えているような組織を念頭に置いた方がよいのではないか。提出命令も公私の団体というふうになっているので、それに倣った方がいいのではないかと思います。

それから、リモートアクセス、次に移らせていただきます。

刑事訴訟法九十九条の二項は、いわゆる捜索、差し押さえの対象となっているデータを持っている通信機器からさらに別のところに接続している場合に、その別のところのコンピューターからデータを取得することができる、こういう処分を認めようとしているわけです。これはリモートアクセスと呼ばれます。

その場合に、何でもかんでもつながっていればデータをとれるというようなことにはなっていないのは確かであります。どのようなデータを取得してよいかは特定要件が明示されていまして、接続性、関係性、使用の蓋然性が列挙されているので、限定的であろうかとは思います。

しかしながら、リモートアクセスとなりますと、捜索、差し押さえの対象となっているコンピューターからその先は不可視の世界でありますので、リモートアクセスの場所的範囲が、いわゆるネットワークでつながっている疑似的な空間、サイバースペース上であればどこでもよいのかということになってまいります。

今日、リモートな状態でデータをやりとりするということが非常にふえております。いわゆるオンラインストレージ等、そのようなサービスを利用する場合、どこにデータがあるかわからない、こういうことですと、場所の特定という観点から、刑事訴訟法、ひいては憲法三十五条で要求されている場所の特定という点で問題があるのではないかというふうに考えます。

次に、保全要請に移らせていただきます。ちょっとスキップさせていただきます。

刑事訴訟法百九十七条に新たに三項から五項を設けて、捜査対象者の通信記録が消去滅失されないように、一種の凍結のような処分をプロバイダーに要請する保全要請の新設がされようとしています。この要請は、令状に基づかない処分ということになっておりますけれども、この第一の懸念は、通信履歴の保全要請と通信傍受との類似性にあろうかと思います。

法案説明趣旨によりますと、本条項は、通信の傍受ではない、記録データへのアクセス機会を確保するための措置にすぎないという御説明でありますけれども、イメージとしましては、電話の通話履歴のデータを保存させておくだけだということになるので、通信傍受法の意味している、内容を知ることではないということになろうかと思いますが、言うまでもなく、通信傍受法が対象としているのは通信の内容でありまして、通信記録だけを知りたい場合は通信傍受法を利用するわけではありません。

恐らく、今日、捜査の現場では、通信記録を取得する場合には検証許可状という強制処分が予定されているところと思うのですけれども、この場合に重要なのは、通信傍受の場合には、例えば、対象犯罪が限定されていること、事後的に対象者に通知しなければならないこと、また、国会で報告することが義務づけられております。これに対して、通信記録にはそのような制約が一切ございません。

ですので、保全要請によって過去の通信履歴を取得することと、将来分の通信記録については、検証許可状を組み合わせれば、相手方に事後的通知をすることもなく、国会に報告することもなく、組織犯罪に限定された罪種にもかかわらず、通信履歴を取得できるということになってしまうわけであります。

これは当局の公式見解でありますけれども、通信記録も憲法上の通信の秘密によって保護されるという見解に照らしまして、侵害される法益とのバランスを失しているのではないかというのが私の見解でございます。

最後に、電磁的記録の没収に移らせていただきます。

刑訴法四百九十八条の二では、不正につくられた電磁的記録等を没収すると。この没収というのは、有体物ではないので、とっていくわけではない。では、どうするかというと、データを複写した後、そのもとあった保存されていたデータを消去するということで没収に擬制しようとしているわけです。

問題なのは、没収されたデータの完全性ないし真正性であろうと思います。要するに、これは没収したデータですというふうに捜査機関あるいは訴追機関が主張したとしても、本当にそれがそうなのかどうかということを確かめようがないのではないか。言うまでもないことですが、昨年発生した郵政不正事件におけるプロパティー情報の検察官による改ざん事件にあらわれているように、電子データというのは非常に脆弱なものでありますので、この点については、十分な収集手続や具体的方策についてのきめ細かい対応が不可欠だと考えます。

最後に一言申し述べさせていただきますが、今日のコンピューター技術の進展にいささかサイバー犯罪条約自体も追いついていないといいますか、時代おくれになっています。これは、今日最も懸念されるのはクラウドコンピューティングの技術でございます。すなわち、データがどこにあるかわからないという状態です。つまり、被処分者、対象者が管理しているデータがクラウドコンピューティングのサービスを利用していますと、一体そのデータがどこにあるかわからない。ということは、どの国の法律を適用していいかわからないということで、現在、欧州評議会では、このクラウドコンピューティングの技術とサイバー犯罪条約の定める規定とのそご、あるいは条約の整備のおくれが非常に大きな問題となっているところであります。

このような技術革新に対応できるような法整備が今回の場合には欠けているのではないかというのが私の見解でございます。

御清聴どうもありがとうございました。

○奥田委員長　どうもありがとうございました。（拍手）

次に、今井参考人にお願いいたします。

○今井参考人　おはようございます。法政大学大学院法務研究科の今井と申します。

本日は、貴重な機会を与えていただきまして、大変光栄に存じております。どうぞよろしくお願いいたします。

私は、刑法、刑法実体法を専攻する者といたしまして、本法案に賛成する立場から、刑法の改正部分のうち、特にサイバー犯罪関係のものについて意見を述べさせていただきます。

時間の関係もありますので、主要な点に絞ってお話ししたいと思います。

まず、不正指令電磁的記録に関する罪の新設に

ついて申し上げます。

この罪は、いわゆるコンピューターウイルス、最近ではマルウエアという呼び方も一般化してきているようでありますが、そのような不正プログラムを作成、提供、供用、取得、保管する各行為を処罰の対象とするものであります。

御案内のとおり、コンピューターウイルスの蔓延は憂慮すべき社会問題となっておりまして、これに適切に対処する必要性かつ緊急性があることは多言を要しないところであります。

最近でも、例えば、新聞報道によりますと、東日本大震災の発生に乗じまして、「福島原発最新状況」とか「被ばくに対する防護対策について」といったタイトルのメールに、「放射能が関東の人間に与える影響」などのファイル名がつけられたコンピューターウイルスを添付して送りつけ、この添付ファイルを開くとパソコンが感染するという手口でコンピューターウイルスが広がったようであります。このようなウイルスは、感染いたしますと、そのパソコンを外部から操作できるようになったり、パソコン内の情報を知らない間に抜き取られたりするという悪質なものであったようでございます。

コンピューターウイルスというものにはさまざまなものがありまして、次々と新種ないし亜種のウイルスが発見され、その都度、ウイルス対策ソフト会社等は、多大な努力を払いまして、ウイルスの最新定義を入手あるいは更新するなどして対応しているようでありますが、まさにイタチごっこの状態が続いているというのが現状ではないかと思われます。もちろん、コンピューターの使用者が、みずからこのようなセキュリティーソフトを利用するなどして自衛の措置を講じるということは、それはそれで望ましいことでありますけれども、現実には、それだけでは対応し切れない状況に至っているわけであります。

このようなコンピューターウイルスの蔓延を放置いたしますと、コンピューターを使用する一般国民としては、コンピュータープログラムを実行するに際し、もしやウイルスではないか、これを実行したらコンピューター内のファイルが消去されたり個人情報が抜き取られたりするのではないかという不安を抱かざるを得なくなりまして、ひいてはコンピュータープログラムを安心して使用することができなくなります。

それはすなわち、コンピューターを円滑に使用できなくなるということを意味するわけでありまして、今日、コンピューターが、私たちの日常生活においても、企業の経済活動においても、あるいは政府等の公共機関のサービス提供においても、非常に広い範囲で極めて基礎的なインフラとして使用されているということを考えますと、コンピューターを円滑に使用できなくなれば、私たちの生活のあらゆる局面に影響が及ぶと言っても過言ではないように思われます。

このように、コンピューターウイルスが蔓延し、コンピュータープログラムに対する信頼が揺らぎますと、社会全体に悪影響が及ぶということになります。そのような事態を防ぐためには、プログラムに対する社会一般の信頼を確保するということが極めて重要であります。

そこで、今回新設される不正指令電磁的記録に関する罪でありますが、本罪は、そのような社会的法益に対する罪として構成されているものと理解しておりますが、今申し上げましたような事情に照らしますと、その保護法益のとらえ方は実態に即した適切なものであろうと考えております。

こうした理解に対しましては、コンピューターウイルスに関する罪は、個々の電子計算機の適正な機能を保護法益とするものとして構成すべきであるとの考え方を前提といたしまして、器物損壊罪や業務妨害罪などの個人的法益に対する罪の予備罪として構成すべきであるとする考え方も論理的にはあり得ると思われます。

しかしながら、先ほど申し上げましたような社会の実態、すなわち、今日、コンピューターが社会の隅々にまで基礎的なインフラとして波及しているという実態を直視いたしますと、それを侵害するウイルスというものは、個々の電子計算機に被害を与えるにとどまりませず、それを超えて社会一般に重大な影響を与えるのでありますから、そうした実態を正面からとらえまして、社会的法益に対する罪として構成する方がより適切ではないかと考えております。

こうした理解は、既に刑法典の中で、文書偽造罪や通貨偽造罪でとられているものであります。すなわち、それらの罪におきましては、個々の行使場面における被害にとどまりませず、社会一般における文書や通貨に対する公共の信頼を保護するものとして社会的法益に対する罪と解されておりますが、今回の想定されている犯罪も同様のものであろうと考えております。

また、予備罪として構成する場合、電子計算機損壊等業務妨害罪や電磁的記録毀棄罪等の予備行為を処罰することになると考えられますが、そうしますと、大きな社会問題となっている事例群、例えばパソコン内の情報を勝手に流出させるような情報漏えい型のコンピューターウイルスについては、処罰の対象から外れてしまうというおそれがあります。

さらに、現行刑法において、予備罪、予備行為というものは、例えば殺人罪ですとか強盗罪といった、非常に凶悪で重大な犯罪についてのみ予備が処罰されるということになっております。そういたしますと、コンピューターウイルスに関する罪がそれらの重大かつ凶悪犯罪に匹敵する害悪を生じさせるものと言えなければ、予備罪構成は困難であると思いますけれども、そういった認識はなかなか理論的には難しいのではないかと思っております。

次に、コンピューターウイルスの作成行為を処罰対象とすることについては、処罰の時期が早過ぎるのではないかという御指摘もあるものと聞いております。

しかしながら、コンピューターウイルスを作成する行為は、コンピュータープログラムに社会の信頼を害すべきものを新たに現出させる、要するに、これからウイルスが出ていって、社会に害悪を引き起こす根本、基礎となる行為でありますから、これはこれで大変違法性が高い行為だと思います。この点、通貨偽造罪や文書偽造罪の罪、あるいは有価証券偽造などの罪におきましても偽造行為というものがそれ自体処罰対象とされておりますことと同様ですし、あるいは、薬物犯罪においてはその製造行為が処罰対象とされていることとも基本的に同様であると理解できます。

したがいまして、個人が自己のコンピューターでウイルスを作成しただけの段階でありましても、人の電子計算機における実行の用に供する目的でコンピューターウイルスを作成したという場合には、プログラムに対する社会の信頼を害する危険が発生しているというべきでありまして、当該作成行為を処罰の対象とすることには十分合理性があると考えているところであります。

次に、わいせつ物頒布等の罪に関する改正について意見を申し上げます。

今回の法案では、刑法第百七十五条につきまして、幾つかの点で改正を行うこととしているようでありますが、そのうち主要な点について申し上げますと、まず、電気通信の送信によりわいせつな電磁的記録を頒布した者が処罰対象に含まれるというふうになっております。

今日、わいせつな画像を電子メールやインターネットなどのネットワークで頒布する行為が多々見受けられるわけでございますが、現行の百七十五条は、対象物として有体物であるわいせつ物を想定していると解されますので、そのような行為に本罪、現行の百七十五条を適用し得るかについては、下級審の裁判例でも判断が分かれているところでございます。

すなわち、平成十二年七月六日の横浜地方裁判所川崎支部判決におきましては、電子メールにわいせつな電磁的記録を添付して不特定多数の者に送信する行為につきましては、このような画像データはインターネットにおけるメールシステムを媒体とするわいせつ図画に該当すると判示し

て、わいせつ図画販売罪の成立を認めております。

しかし、同種の行為につきまして本罪の成立を否定したものもありまして、それは例えば、平成二十一年六月十六日の札幌高裁判決であります。ここにおきましては、インターネットを通じて不特定多数の者に有償で提供する目的でわいせつな動画ファイルを自宅のファイルサーバー等に蔵置させたという行為につきまして、有体物でない動画ファイルを販売する目的でファイルサーバー等を所持したということでは、わいせつ図画販売目的所持罪が成立しないということで、本罪の成立を否定しております。

このように、下級審裁判例の判断は分かれておりますけれども、実質的に考えますと、ネットワークを通じてわいせつ画像を頒布するという行為は、有体物としてのわいせつ物を頒布する行為と違法性の点では同等と言うべきであります。

したがいまして、今回想定されております改正後の百七十五条第一項後段におきましてこのような行為が処罰の対象に含まれるということは、適切なものだと考えております。

また、現在の百七十五条後段におきましては「販売の目的」という文言が使われておりますが、今回の法案では「有償で頒布する目的」という文言が使われております。「販売」という文言は、これまで、基本的には有体物を想定してきたものでありますけれども、今回の改正では、ネットワークを利用して電磁的記録という有体物以外の情報を拡散させる行為を処罰対象に含めることとしておりまして、このような行為につき、有体物の場合と同様に「販売」という文言を用いることが適当かという疑問もあったところであります。

一方で、有体物としてのわいせつ物についても、従来、例えば、有償でレンタルするように、必ずしも所有権の移転を伴わない形でわいせつ物を拡張させる行為もあったところであります。改正後の百七十五条二項におきまして「有償で頒布する目的」と規定されておりますのは、このようなことを踏まえたものであると思われまして、従来の「販売」との文言では捕捉できない行為、有体物の所有権の移転を伴わない行為をも適切に捕捉する改正であると考えております。

次に、電子計算機損壊等業務妨害罪の未遂犯処罰規定の新設について簡単に申し上げたいと思います。

この規定でございますけれども、現行法では、電子計算機損壊等業務妨害罪は既遂類型でありまして、未遂罪は処罰されておりません。しかし、最初に申し上げたような、コンピューターウイルスというものが感染していき、不特定多数の人々のコンピュータープログラムに害悪を加えるという状況を考えますと、その直前である未遂類型についても当罰性が否定できないところであります。そこで、そういった対応を可能にするために、電子計算機損壊等業務妨害罪に未遂規定を含めるというのが今次の改正の趣旨だと理解しておりますが、これも適切な対応であろうと思っております。

以上、サイバー犯罪関係の刑法実体法の改正部分に関しまして、主要な点について私の見解を申し上げました。サイバー犯罪への対処は大変重要な、緊急を要する課題でありますので、この法案が一日も早く成立することを願っております。

御清聴どうもありがとうございました。（拍手）

○奥田委員長　どうもありがとうございました。

次に、安富参考人にお願いをいたします。

○安富参考人　慶應義塾大学法務研究科の安富でございます。

本日、この法務委員会におきまして参考人として意見を述べる機会をちょうだいいたしましたこと、まことに光栄に存ずる次第でございます。

私は刑事訴訟法を専攻しておる者でございますので、主にサイバー犯罪関係の手続法の整備につきまして、今回の法案に賛成する立場から意見を述べさせていただきたいと思います。

御案内のとおり、現行の刑事訴訟法は昭和二十三年に制定されたものでございまして、当時は今と違いまして、コンピューターとかネットワークといったようなものは普及もしておりません。証拠収集手続といいますと、有体物というものの存在、これを念頭に置いて行われてきたということは御案内のとおりでございます。したがいまして、刑事訴訟法の定めます捜索、差し押さえ、検証、こういった手続は、いずれも基本的に有体物を前提として構成されているところでございます。

しかしながら、一九八〇年代になりますと、パーソナルコンピューターというのが普及をいたしました。また、一九九〇年代に入りますと、コンピューターネットワークというものが目覚ましい発展を遂げるに至りまして、我々が日常生活を送り、あるいは企業活動を初めとする社会経済活動を行う上で、コンピューターあるいはネットワークといったものは、我々の社会におきます不可欠な社会的インフラというふうになったものと思います。

そして、当然のことなんですが、このようなコンピューターやネットワークが我々の活動の基盤となりますと、これを利用して犯罪を犯すという者も出てまいるわけでありまして、いわゆるサイバー犯罪というのは、コンピューター、ネットワークを利用して行われますし、サイバー犯罪以外におきましても、コンピューターや携帯電話などを利用して行われる、こういう情勢にあるところでございます。

その結果、犯罪に関する証拠も、コンピューターやハードディスクなどの記録媒体に電子データとして残されるということが多くなっておりまして、刑事事件の捜査、公判において、そのような電子データ、これは法律上は電磁的記録というふうになっておりますけれども、それを証拠として的確に収集するということが不可欠となっている状況でございます。

このようなことから、今回の改正におきまして、基本的に有体物を前提としている刑事訴訟法による証拠収集等の手続を、コンピューターや電磁的記録の特質に対応するものとして改正をしようということは、まことに時宜にかなったものと考えているところでございます。

そこで、以下におきまして、本法案につきましての主要な事項について私の考えを述べさせていただきたいと思います。

まず第一に、電磁的記録に係る記録媒体の差し押さえの執行方法、これは百十条の二、百二十三条の第三項、二百二十二条第一項関係でございますが、この整備について申し上げさせていただきたいと思います。

例えば、コンピューターのハードディスクの中に犯行計画を書いた文書のファイルあるいは電子メールといったものが記録されている場合、現行法のもとでは、そのコンピューターという記録媒体自体を差し押さえるということが考えられるわけであります。

しかしながら、近時のコンピューターなりは大容量のサーバーであるというような場合がありまして、これを差し押さえるということになりますと、差し押さえを受けた者の業務に著しい支障を生じさせるというおそれがありますし、他方で、捜査機関にとっても、そのサーバー自体を差し押さえるという必要はなく、特定の電磁的記録を取得することができれば捜査目的を達成できるという場合があります。

こうしたことからいたしますと、差し押さえ対象物が電磁的記録が記録された記録媒体である場合に、差し押さえをする者が、その記録媒体自体の差し押さえにかえて、当該記録媒体に記録された電磁的記録を他の記録媒体に複写するなどした上でこれを差し押さえるということができる、こういう方法は極めて合理的なものであるというふうに思われます。

この差し押さえの執行方法に関しまして、電磁的記録を他の記録媒体に複写等した上でその媒体を差し押さえる方法をとり得る場合には、当該電磁的記録媒体自体の差し押さえはできないこととする、こういう意味での、いわゆる補充性という

言葉が使われますが、こういう意見があるということを伺っております。

しかしながら、例えば、手帳の中のある特定の記載が真実であるか否かということが問題となる場合があります。その際、その記載内容だけから判断するというのではなく、その前後にどういうことが記載されているのか、前後と比較して筆跡が同じなのか、あるいは筆記具の太さや色合いは同じなのか、後で書き足した形跡はないのか、あるいはまた何か消されたような形跡はないのか、こういった、問題となる記載がなされている状態を含めた全体から判断されるということが多いのだと考えられます。

この点は電磁的記録についても同様でありまして、その内容等が真実であるか否かということを見きわめるためには、それが記録されている状態やデータの削除痕跡なども含めて、いわゆるデジタル・フォレンジックという手法を活用して十分に捜査をする必要があるわけでありまして、そのためには記録媒体自体を差し押さえるということが重要である場合も少なくないというふうに思われます。

そして、複写等の処分を原則とした場合には、捜査機関は、差し押さえの現場において、差し押さえ対象物である記録媒体に記録されている個々の電磁的記録すべてについて、今述べましたような、記録媒体自体の差し押さえが必要なのか、あるいは複写等の処分で足りるのかということを判断しなければならないことになるわけでありますが、これは捜査における迅速性の要請にも反しますし、時には不可能を強いることにもなりかねません。

したがいまして、電磁的記録に係る記録媒体の差し押さえについて、複写等の処分ができない場合に限ってこれを行うことができるとする、こういうことは適当ではないというふうに考える次第でございます。

次に、電気通信回線で接続している記録媒体からの複写、これは九十九条の第二項、二百十八条第二項、百七条第二項、二百十九条の第二項関係でございますが、これについて申し上げたいと存じます。

今日、コンピューターはネットワークに接続されているのが通常でありまして、自己のコンピューターで処理すべき電子ファイル等を、ネットワークで接続している先の、物理的には離れた場所にある別個の記録媒体に保存するということも一般化してきているところでございます。

このような利用形態が一般化しますと、そもそも、必要な電磁的記録が保存されている接続先の記録媒体の所在等を把握すること自体、困難を伴いますし、仮にその所在等を把握することができたとしても、データが分散して保管されている場合には、さまざまな場所にある多数の記録媒体について差し押さえ等を行わなければならないということにもなります。

しかも、一たび強制捜査に着手するとすれば、被疑者やその関係者に捜査を察知され、証拠となる電磁的記録を他の記録媒体に移転するなどして瞬時に隠匿あるいは隠滅ということをされることにもなりかねません。

こういうことを考えますと、今回の法案で新設される予定でありますが、電気通信回線で接続している記録媒体からの複写というのは、必要かつ合理的なものというふうに評価されるところであります。

ただ、この点に関しましては、憲法三十五条との関係で問題があるという御指摘もあるようでございます。私は、この点は何ら問題はないというふうに考える次第でございます。

すなわち、まず、憲法の第三十五条第一項との関係で申し上げますと、憲法三十五条第一項の趣旨は、正当な理由、すなわち、その場所及び目的物について捜索、押収を行う根拠が存在することをあらかじめ裁判官が確認し、それを令状に明示して、その範囲でのみ捜索、押収を許す、こういうことによって、捜査機関の一般的、探索的な捜索、押収活動というものを防ごうということにあるわけであります。

この点、電気通信回線で接続しております記録媒体からの複写をする場合には、裁判官の発する令状に、差し押さえるべきものである電子計算機のほか、「差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であつて、その電磁的記録を複写すべきものの範囲を記載しなければならない。」ということとされているわけでございまして、これによりまして、複写の対象となる記録媒体は特定、明示されるものということになります。

この複写をする場合には、接続先の記録媒体の物理的な場所、これは令状に示されないわけでありますけれども、これ自体、別段問題を生ずるものではありません。

例えば、所在が一定しない自動車内の捜索、差し押さえということをすることがありますが、この場合には、捜索場所としての自動車及び車内にある差し押さえるべきものが特定、明示されていれば足りるわけでありまして、捜索の際にその自動車がどこにあるかということは問題にならないということと同じでございます。

このように、捜索、差し押さえに当たりまして、常に場所の特定が必要だということになるわけではないのでありまして、実質的に見て、先ほど申し上げました憲法三十五条第一項の趣旨が満たされていれば足りるというところであります。既に申し上げたところでございますけれども、電気通信回線で接続している記録媒体からの複写というのは、その趣旨を十分満たしているものと考えております。

また、憲法の第三十五条二項との関係で申し上げますと、この趣旨は、場所や対象が別個であったり、同一の場所や対象でも機会が異なれば、そこに特定の目的物があり、あるいは関連性のある事項が認知できる蓋然性、すなわち憲法三十五条第一項の言うところの正当な理由の有無の判断も異なってくるのが通常であるということから、それぞれについて、その都度、裁判官が確認した上で、捜索、押収の処分を許す、こういうことにさせよう、これがその趣旨であると考えられます。

この点、複写の対象となります記録媒体につきましては、第九十九条二項にございますが、「電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認める」に足りる状況にあるもの」、こうなっておりまして、実質的に見れば、当該電子計算機と一体的に使用されているものでありまして、関連する証拠が存在する蓋然性は共通して認められるところであります。正当な理由の有無の判断というのは、その電子計算機と一体的なものとして行うことができるというふうに考えるところでございます。

したがいまして、憲法第三十五条二項との関係でも問題がないというふうに考えております。

この複写の処分につきましては、その対象となる記録媒体の範囲が広くなり過ぎるのではないかという懸念が示されていると聞いております。

しかしながら、今回の法案におきまして、複写の対象となる記録媒体の範囲を明確にするため、差し押さえるべき電子計算機に電気通信回線で接続している記録媒体のうち、「当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるもの」に限定するとの修正がなされております。

したがって、例えば、ネットワークで接続されていてアクセス可能な記録媒体であればすべて複写の対象となるということにはならないというふうに考えておるわけでありまして、この複写の処分の範囲は適切に限定されるものと考えております。

次に、保全要請について申し上げたいと思います。

例えば、不正アクセス行為の罪などにおきまし

て、犯人の特定等のために通信履歴を確保するということが極めて重要であると言えます。しかしながら、通信履歴は一般に短期間で消去される場合が多く、捜査に必要な通信履歴につきましては、プロバイダー等の保管者に対してこれを消去しないように求めて、迅速に保全する必要性が大きいと言えます。

現在も、捜査実務におきまして、差し押さえ許可状の発付を受ける前の段階で通信履歴の任意の保全を求めている場合があるというふうに聞いておりますが、その保全を求める法律上の根拠を明確にしておくことはプロバイダー側にとっても望ましいことでありますし、今回の改正で保全要請の規定を設けることとされたのは適切なものと評価しております。

この保全要請につきましては、憲法二十一条二項が保障している通信の秘密を侵害するものではないか、またあるいは、保全要請については裁判官の発する令状を要するものとすべきではないか、こういう御意見があると承っております。

確かに、通信履歴も通信の秘密に含まれるということではあろうかと思いますが、既に申し上げましたけれども、電気通信を利用した犯罪におきまして、犯人の特定等のために通信履歴を確保する必要性が大きい、また、通信履歴は一般に短期間で消去される場合が多いことから、その迅速な保全を可能とする必要性も大きいというふうに言えます。

他方、保全要請の対象は、通信事業者等がその業務上の必要性から実際に記録している通信履歴に限られておりますし、その通信履歴を消去しないよう求めるものにすぎず、それだけで通信履歴が捜査機関に開示されるものではありません。捜査機関が通信履歴を取得するためには、別途、令状が必要となってくるわけでありまして、あくまでその準備として、一時的に、本来その通信履歴を保有する権限を有しているプロバイダー自身が、それを消さないで手元に置いておくというものにすぎません。

保全要請がこのような性質のものであるということ、すなわち、通信事業者等がその業務上実際に記録している通信履歴を消去しないように求めるものにすぎず、それだけで通信履歴が捜査機関に開示されるものではありません。要請に応じなかったとしても罰則等の制裁はないことからいたしますと、保全要請に当たって裁判官の発する令状を要するということは必要ないと考えております。

むしろ、仮に保全要請について令状を必要とするというようなことになりますと、その準備のために別の令状を得なければならないということになってしまって、通信履歴の迅速な保全を図るという保全要請の趣旨が没却されることになるのではないかというふうに考えるところでございます。

以上、主要な点に絞って、今回の法案についての私の見解を申し上げさせていただきました。

この法案がこの国会におきまして御理解を得まして成立する運びとなりますことを祈念して、私の意見陳述とさせていただきたいと思います。

どうも御清聴ありがとうございました。（拍手）

○奥田委員長　以上で参考人の方々の御意見の開陳は終わりました。

○奥田委員長　これより参考人に対する質疑に入ります。

質疑の申し出がありますので、順次これを許します。稲田朋美君。

○稲田委員　おはようございます。自由民主党の稲田朋美です。

本日は、参考人の先生方には、お忙しいところお越しいただきまして、有益な御意見をどうもありがとうございます。今、先生方から述べられたところと重なる点もあろうかと思いますけれども、質問をいたしたいと思います。

指宿先生からは刑事訴訟法の立場から、また今井先生からは実体法上の立場から、安富先生からは刑事訴訟法の立場から御意見をいただきました。

まず、実体法の点について今井先生にお伺いをいたしたいと思います。

このたび、この法案で、いわゆるコンピューターウイルスの作成自体を犯罪の構成要件としております。この点については、コンピューターウイルスでだれかのコンピューターの機能を実際に阻害したりしようとする前に、作成した段階で罰するとすれば、プログラマーのソフト制作活動を萎縮させるのではないかとか、表現の自由を阻害することになるのではないかとか、また、実行の用に供する前の段階で処罰するということは共謀罪に通底するような問題があるんじゃないかということが、この委員会の質疑の中でも出されております。

これに対しては、正当な理由がないという要件ですとか、あと、人のコンピューターにおける実行の用に供する目的という要件で絞りをかけているので、そのような問題はないという趣旨の答弁が当委員会でなされておりますが、こういった懸念について、今井先生、実体法上の立場からどのようにお考えか、お聞かせください。

○今井参考人　ありがとうございました。

まず、例えば、プログラマーの方がシステムの脆弱性をチェックするためのソフトを作成するという場合には、確かに、それを一回使ってみて確認をする必要があるということは承知しておりますけれども、この条文案を見ますと、今委員御指摘のように、「正当な理由がないのに、」という絞り、それと「人の電子計算機における実行の用に供する目的で、」という目的、二つの絞りがかかっております。

例えば、プログラマーの方が業務においてシステム防衛のためのソフトをつくっている場合には、当然ながら、「正当な理由がないのに、」という目的が欠けますので、本罪には当たらないことになります。

また、もう少し一般的に、ウイルスとしても機能し得るようなソフトを作成しただけで本罪が成立するということにつきましても、後の要件であります「人の電子計算機における実行の用に供する目的」、これがあってそういったプログラムをつくるときには、後にプログラムを悪用される危険性が高まるということが言えますけれども、そうでない場合には同様の危険を認定できないということになりますので、御懸念の点はないように理解しております。

○稲田委員　ありがとうございます。

次に、保全要請について、指宿先生と安富先生にお伺いをいたします。

今回の法案では、プロバイダーなどに対して、業務上記録している電気通信の送信元、それから通信日時その他の通信履歴の電磁的記録を三十日を超えない期間で消去しないように求める手続が用意をされております。そして、最大六十日となっておりますが、条約では九十日以内となっております。その期間について、短過ぎないのか、それとも長過ぎるのか、どのようにお考えであるかという点。

そしてまた、この保全要請の手続については、応じなくてもペナルティーなどは規定をされておりません。実効性を担保するために罰則を定めた方がいいのではないかという意見もありますけれども、期間の面と、そして罰則の面、実効性の面についてお伺いをいたします。

○指宿参考人　期間の点でございますけれども、例えば、アメリカ合衆国は九十日というふうになっております。これは、かなり初期にこうした法律を整備したという関係でそのような長期になっていると考えます。我が国でも、当初は九十日という提案がなされていたところでありますけれども、これに対して、いわゆるプロバイダー側、保全しなければならない側の負担という観点から短縮されたというふうに聞いております。

この点では、やはり、小さいプロバイダーであれば、その保全にかけるコストをどこまでカバーできるかということがございます。余りにも負担

が大きいということになりますと、これはユーザー側の、利用者の料金にはね返るということになろうかと思います。また、大規模のプロバイダーの場合には、特定のユーザーの記録を保全することに、非常に技術的に難度が高くなるということが予想されるところであります。

そういったさまざまなコスト面から、今回は最大六十日ということになったのだろうというふうに思いますけれども、それでも、プロバイダーによって、記録している通信記録というのはさまざま、非常にバラエティーに富んでいるところでありまして、これをどこまで義務づけるかというところについては、技術的には、受ける側からすると、恐らく多大な問題があるかというふうに思います。

したがいまして、後半の御質問になりますけれども、これを義務づけるということになると、業法に対して非常に、別の面から先に義務づけを課しておかないと、どのような範囲で業者は記録しなければならないのかということを先に定めておかないと、やはり無理であろうというふうに考えます。

この点、欧州では、通信利用者の通信記録をすべて指定が来る前に記録する、これはデータ保存というふうに呼んでおりますけれども、一括してすべて保存するという、このような制度がとられているところでございますけれども、これは、欧州のプロバイダー産業に対して極めて重いコスト負担を課していて、国際競争力を落としているのではないかという批判が極めて強いところでございます。

また、この一括保存方式につきましては、私の論文でも紹介しておりますとおり、各国の裁判所で、理由はさまざまでありますけれども、主にプライバシー保護の観点から違憲判決が相次いでおりまして、欧州評議会、EUの内部でも、この一括保存方式については、もう見直さなければならない、技術的、コスト的、そしてプライバシーの面でもというふうになっていて、やはり利用者の拡大、技術の進歩、さまざまな周辺事情、あるいは経済事情、国際競争市場、そういった観点からこの問題についてはさまざまな議論がされているということをつけ加えておきたいと存じます。

○安富参考人　お答えいたします。

期間の点でございますけれども、この点は、サイバー犯罪条約が九十日ということで、当初の法案ではそうなっておりましたけれども、今もお話ございましたとおり、プロバイダーの方の負担ということを考えますと、三十日というふうにして、さらに延長で六十日というふうにされているものと承知しておりまして、これはそれなりの理由があるものというふうに考えます。

罰則の点ですが、これは保全の要請ということでございまして、通信記録について必要がある場合には令状をもって差し押さえるということのその前提でございますので、そこに罰則をつけた形での義務づけを課すというのは、プロバイダーに対する負担としては余りにも大き過ぎるというふうな考えを持っています。

以上でございます。

○稲田委員　次に、指宿先生にお伺いをいたします。

先生の以前の論文で、記録命令つき差し押さえの被処分者が被疑者である場合、データの提出が供述に当たるとすると、憲法の禁ずる自己に不利益な供述の強要に当たる場合があるのではないかという疑問が呈せられていたかと思います。この点について、指宿先生の御意見をお聞かせいただきたいと思います。

○指宿参考人　今回お配りしております論文でもその点につきましては触れているところでありますので、そこを参照しながらお答えしたいと思います。ページ数でいいますと八十七ページ、「記録命令付き差押え」の後半部分にございます。

特に、差し押さえデータが音声データ、音声ストリームのバックアップ等である場合に、これが供述に該当するのではないかという懸念があると思います。

もしもこの蓄積された音声データは供述ではないという解釈をとれば、これは単なる電子データということになりますので該当しないということになるかもしれません。しかし、例えば、それが未聴のものである、まだ聞いていないものがただ一時的にストックされているような場合であるとか、供述に極めて近い場面も考えられるのではないかというふうに考えますので、ここを一律に考えることは難しい。もしこれが適用されるということになると、司法府の判断を仰がなければならなくなるのではないかというふうに考えます。

○稲田委員　では最後に、今回の法案では、差し押さえの目的である電磁的記録を別の記録媒体に複写した上で、その複写した記録媒体を差し押さえるという手続が新設されました。大阪地検特捜部で、証拠のフロッピーディスクを改ざんしてしまったという、本来あってはならない残念な事件もありました。この手続においては、原本に当たる電磁的記録と複写した電磁的記録の同一性を担保する必要があると思いますけれども、安富先生、どのようにお考えでしょうか。

○安富参考人　お答え申し上げます。

今御指摘にありましたような、原本とそれからその複写物の同一性ということでございますけれども、それにつきましては、その捜索の過程あるいは押収の過程において原本性を確保するような、チェーン・オブ・カストディー、こういうふうに呼んでおりますけれども、そういうような一連の手続を踏むということ。これにつきましては、既にいわゆるデジタル・フォレンジックの技術というもので確立しているところでございますので、そのような技術を応用していただきまして、その同一性の確保というものに努めていただきたいというふうに考えております。

○稲田委員　先生方、どうもありがとうございました。

○奥田委員長　次に、階猛君。

○階委員　民主党の階猛です。

本日は、参考人の皆様、ありがとうございます。

時間も限られておりましたので、きのう恐らくお手元に私からの質問要旨ということでお届けさせていただいたと思うんですが、六問用意しておりますので、お一人二問ずつ、順次お聞きしていきたいなと思います。

まず一つ目の質問は、指宿先生にお願いしたいんですが、今、国の方では、東日本大震災の復旧復興ということに全力を挙げております。しかるに、この法案は復旧復興とは直接関係ありません。また、折から、冤罪事件、いろいろありまして、検察の権限の行使というものに国民は疑念を抱いている、こういう状況があります。翻って、この法案、今この時期に国会で審議する緊急性、必要性、重要性はあるのかどうか、この点について御見解をお願いします。

○指宿参考人　御質問の趣旨はよく承知いたします。

私は、震災の復旧や災害については専門外ですので、その点についてのお答えは差し控えさせていただきたいと存じますけれども、この法案、もともとの法案が上程されてからほとんど議論がされないまま、国会で、言葉は悪いんですけれども、たなざらし状態になっておりましたので、やはり私の目からは、審議の期間というのがちょっと不十分なのではないかというふうに考えております。このときに急がなければならない特別な理由というのが私には承知しかねますので、ぜひとも慎重な御審議をお願いしたい。

各国の状況あるいは現在の技術的な点については、先ほど申し述べさせていただいたとおりでございます。

○階委員　ありがとうございます。

それでは、今井先生にお伺いします。

今回のいわゆるコンピューターウイルス作成罪の構成要件を見ますと、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」というのがコンピュー

ターウイルスの定義なのではないかと思います。

ところで、昨今、チュニジアですとかエジプトですとか、インターネットを通じて政府に対して権力を批判するような動きがあったときに、権力側もそれに対抗してインターネットをなるべく使わせないようにするとか、そういう動きもあるわけであります。

仮に、国家権力が自己の都合が悪い情報を遮断しようとした場合、それに対して国民の側がその遮断措置を逆に突破しようとした、解除しようとした場合、国家権力の側からすると、不正な指令というふうにいうんじゃないかと思うんですね。何かそんな危険を感じるわけですけれども、不正かどうかという判断が国家権力によって恣意的といいますか、国家権力寄りに判断される可能性というものはないものかどうか、この点についてお願いします。

○今井参考人　お答えいたします。

本罪、百六十八条の二として考えられている条文案に即してのお答えとなりますけれども、ここで不正にと書いてありますことの趣旨は、予定されています本罪が対象としている保護法益に照らして不正ということになるべきでありまして、これは先ほど申し上げましたけれども、コンピュータープログラムが現在社会的インフラとなっているという状況で、一定のプログラムについて、通常、人が想定するような動作をするかどうか、それを異なった態様に変えてしまうということが不正と定義されるわけでございますので、今言われたようなこととは直接関係ない解釈、むしろ無関係の解釈により正当か不正かが判断されるのではないかと理解しております。

また、「不正な」という解釈について若干広い解釈をとる方がいたとしても、この百六十八条の二の柱書きにおきまして、先ほども申しましたが、「正当な理由がないのに、」という要件、「人の電子計算機における実行の用に供する目的で、」という二つの絞りがかかっておりますので、濫用的な解釈に至る可能性は大変低いと私は理解しております。

○階委員　何が正義かどうかというのはなかなか一義的には決められないので、「不正な」というような表現はむしろ使わない方がいいんじゃないかなというふうに私は感じました。

三点目ですけれども、安富先生にお伺いします。

記録命令つき差し押さえ、あるいは複写、印刷物の差し押さえということが今回の法改正に含まれておりますが、コンピューター自体を差し押さえる従来のやり方よりも、捜査機関側にとって、証拠のいいとこ取りといいますか、都合のいいところだけを証拠として差し押さえる危険が高まるのではないかという懸念があるんですけれども、その点についていかがでしょうか。

○安冨参考人　お答えをさせていただきたいと思います。

現行法におきましても、差し押さえというのは「証拠物又は没収すべき物と思料するもの」、これを対象としているということでございまして、一般的に、被疑事実との関連性があるということが思料されるというものを差し押さえることができるということになっているわけでございまして、今回の立法措置、これは、差し押さえ対象物であるところの記録媒体のうち捜査に必要な特定の電磁的記録を対象とするというものでありますので、差し押さえを受ける者にとってより侵害的でないといいますか、そういう形での方法を認めているものでございますので、これによって、委員御指摘のような形での証拠の収集の危険性というものが高まるということにはならないというふうに思っております。

○階委員　前田検事の問題もそうだったんですが、検察はともすれば、供述に沿うような、犯罪を裏づける積極証拠の収集については時に偽造もするなどして一生懸命集めるんですが、消極証拠の収集については消極的だと私は思うんですね。そういった意味で今お尋ねしました。なるべく証拠は広く、積極も消極も集めるべきだということを言わせていただきます。

四点目、また指宿先生にお尋ねしますけれども、通信履歴の保全要請ということが今回定められておりまして、この要件、「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」ということなんですが、その要件を具備しているかどうか判断できるのかという疑問があります。

「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」といいながらも、結果的に差し押さえ等に至らなかった場合は、それでは必要がなかったという話になってしまうのではないか。その場合、結果的に差し押さえられなかったんだったら、もとの要件は具備していなかったということになって、違法ということにもなるのではないかと思うんですが、この疑問についてお願いします。

○指宿参考人　まず、「必要があるとき」という言葉遣い、文言ですけれども、これは刑事訴訟法では幾つも見られるところでありまして、捜査機関が必要性を判断するということは、この場面に限らず認められているところです。

御質問の趣旨は、保全要請が実施できなかったときに、当初の保全要請の必要性の判断が誤っていたのではないかというところだろうと思います。

これは、誤っていたかどうかもだれも判断することができないというのが、恐らくこの保全要請の隠れた問題点なのではないかというふうに考えますので、被処分者がこの要請が違法であったというふうに直ちに訴えるとは思えないんですけれども、例えば合衆国の場合、保全要請をかけますと、それに発生したコストを捜査側に請求することができます。しかし、我が国の場合はコスト負担の規定がございません。そうすると、例えば、仮定、仮説ですけれども、プロバイダーが多大のコストを負担した場合に、国に対してあるいは警察に対して損害賠償を求める訴えを起こすということは考えられるところであります。その場合に初めてそうした必要性の判断の適法性が司法府によって判断されるということになるかもしれません。

○階委員　その必要性について疑義が生じないようにするためには、やはり捜査機関としてはなるべく差し押さえに持っていこうというのが通常あり得るのではないかと思います。

そこで、今井先生にお伺いしたいんですが、保全要請をした場合ですけれども、今申し上げたように、なるべく差し押さえに持ち込もうということで、捜査機関が行き過ぎた取り調べをするのではないか、差し押さえの要件を具備するために、なるべくそれに資するような取り調べを行うのではないかというふうに思うわけであります。今行われている検察改革は、取り調べに過度に依存する捜査手法を改めるということを主眼とすることと矛盾しているような気がしますが、この点、いかがでしょうか。

○今井参考人　私は刑法実体法が専門なので、その範囲でわかる限りで、今回の法案を見て感想を述べさせていただきます。

まず、保全要請という今回の制度ができますならば、むしろ取り調べに依存しない捜査を行うことが進むのではないかと思っております。通信履歴を含めまして、客観的な証拠の収集に重点が置かれるということになっていくのではないかと思います。

また、保全要請は、この法案に書いてありますように、差し押さえまたは記録命令つき差し押さえをするため必要があると判断した場合に行うものでありますけれども、そうした判断を行う際には、供述証拠もそうでしょうが、非供述証拠であります通信履歴等を総合的に判断いたしますので、委員が御指摘のような事態は必ずしも生じないのではないかと私は理解しております。

○階委員　まだもう少し時間がありますが、最後の質問になります。では、これは、時間がありますのでお三方にお聞きします。

今、ソニーの個人情報漏えい事件が大変話題になっております。全世界で一億人にも上る方の個

人情報がハッカーによって漏えいされてきた。私は、これは国際的サイバー犯罪の極致であると思っていますけれども、しかしながら、警察庁であるとか検察にお話を聞いていても、現行法でも不正アクセス禁止法などで処罰可能なのに、捜査に消極的なんです。

そういったことを踏まえると、今回、法改正して国際的サイバー犯罪に適用すると言っていますけれども、何となく、今の法律も使いこなせていないのにそんな必要があるのだろうか、法改正しても宝の持ち腐れにならないのかどうかということを懸念するわけですが、指宿先生から、最後にこの点についてコメントをお願いします。

○指宿参考人　まず、我が国の捜査機関がこのソニーの事件を捜査するといたしまして、漏えい元であるサーバーについて、それがどこに所在しているかということで、捜査が実施できるかどうかということがまず大きな問題となろうかと思います。これが仮にアメリカ合衆国のサーバーである場合には日本の捜査権は及ばないというのが通常の解釈であります。

私が懸念していますのは、今回の法案が通過しますと、これまでの、私が今述べたような考え方ではなく、越境的な捜査、国を越えた捜査が可能になるということ、その可能性を認めている法案だろうと思います。

サイバー犯罪条約では、国を越えた警察の捜査、例えば、他の国のサーバーにあるデータを取得するには相手国の同意、承諾が必要だということになっておりまして、越境的捜索はサイバー犯罪条約では現在認められておりません。しかしながら、先ほどから何度も申し上げておりますとおり、例えばリモートアクセスや、現行犯逮捕時のその場での電磁的な記録の差し押さえということになりますと、その先がどの国であっても差し押さえてよろしいというふうに条文上は読めるわけでございます。そうしますと、これは明らかにサイバー犯罪条約の趣旨と大きなそごが認められるところです。

今日、越境的捜索を文言上明らかに認めているのは、私の知る限り、ベルギーとオーストラリアだけです。そのうちベルギーは、EU、サイバー犯罪条約署名国ですが、オーストラリアは、この条約には署名しておりませんし参加していないので適用外となりますけれども、我が国がこの条約をもし批准しようとするのであれば、域外捜索について条約と抵触するような規定を採用するということはいかがなものかというふうに考えます。

ちょっと御質問の趣旨から外れてしまいましたけれども、お答え申し上げます。

○階委員　済みません、私、ちょっと時間を読み違えていまして、時間が参りましたので、お二方には大変失礼ですが、ここで終わらせていただきます。

ありがとうございました。

○奥田委員長　次に、大口善徳君。

○大口委員　公明党の大口善徳でございます。

本日は、安富先生、今井先生、指宿先生、ありがとうございます。

それでは、まず今井先生に、実体法の立場から、この不正指令電磁的記録作成罪の構成要件の解釈についてお伺いをさせていただきたいと思います。

実は前回、大臣に対して、私は、フリーソフトウエアを公開したところ、重大なバグがあるとユーザーからそういう声があって、それを無視してプログラムを公開し続けた場合、それを知った時点で少なくとも未必の故意があって、提供罪が成立するという可能性があるか、こう質問いたしましたところ、大臣から、ある、こういう回答を得たわけでございます。

そこで、そのバグというものが、これが、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令」にそもそも該当するのかということが一点でございます。

そして、インターネットにおいて、フリーソフトを公開し、それに対して、バグについての報告を踏まえて何度も改訂し、徐々によりよいソフトウエアの完成を目指していくという文化があると言われておりまして、すべて利用者の責任で使うことを条件に、自由なソフトウエア開発と自由な流通を促進するということによってソフトウエアが発展してきた歴史的経緯があるわけでございます。

そういうことで、その途中の段階でバグがあるソフトを公開していくことが提供罪として罰せられると、このような文化を阻害して、だれもフリーソフトを公開しなくなってしまうおそれがあるのではないか、こういうふうにも危惧されているわけです。この点についてお伺いしたいと思います。

○今井参考人　お答えいたします。

バグというものが、フリーソフトに限らず、ソフトに不可避的に起因しています望まない動きだというふうに考えますと、そのようなものがここで挙がっている百六十八条の二第一項の一号に当たることは否定できませんが、しかしながら、その不正な動作がどの程度のものであるかということが問題でありまして、重大なバグと先生はおっしゃったかと思いますが、そういったときには、可罰的違法性を超える程度の違法性があるということですので、これに当たることは十分考えられると思います。

二番目の御質問で、特にフリーソフトウエアの場合に、アップロードしてよりよいものに変えていくという文化を阻害するおそれがないかということでありますけれども、私の知っている限りでは、通常、そのようなソフトをアップロードしたときにはバグもあり得るということを潜在的なユーザーの方にもお示しをして、その方々の承諾を得て使っていっているのではないかと思いますので、個々の利用者が一定の危険を認識し、あり得る不都合を承諾して行っている限りにおいては、やはり違法性がないという理解も十分可能であろうと思っております。したがいまして、現在のようなアップロードの仕方、ソフトウエアの展開、提供について御懸念の点はないのかなと思っております。

○大口委員　もう一点、今井先生にお伺いいたしますけれども、今回、電子計算機損壊等業務妨害罪で未遂規定を新設した。これと、この不正指令電磁的記録の提供罪が重なる場合があると思うんですが、この場合の関係性についてお伺いしたいと思います。

○今井参考人　確認させていただきますが、電子計算機損壊等業務妨害罪の未遂とウイルス作成罪の提供の関係でございますね。（大口委員「はい。そうです」と呼ぶ）はい。

まず、提供といいますのは、百六十八条の二で想定されていますウイルスと呼ばれるソフトをつくり、これをそれとして相手方に与えるということでありますので、まだその段階では、もちろん所要の二つの主観的要件を満たしている必要がありますけれども、個別の電子計算機の中にそれを入れて、動作可能な状況にするまでには至っていないわけでございます。

他方で、電子計算機損壊等業務妨害罪というのは、コンピューターの中で不正なプログラムを走らせ、そして業務が妨害される、その未遂というのはその直前行為でありますから、私の理解では、業務妨害の未遂の方がより実害発生に近い段階を捕捉するものとして想定されていると思います。

○大口委員　次に、指宿先生、安富先生にお伺いしたいと思います。

まず一つは、今回、リモートアクセスが認められたわけでございますけれども、このリモートアクセスの場合の場所的な特定というものは、捜索・差し押さえ許可状もこれは特定できないということで、安富先生がお示しになっていますように、刑訴法百七条の二項で複写すべきものの範囲を特定しているのでこれは憲法三十五条一項に違反しない、こういうことでございますが、その点につきまして、この複写すべきものの範囲の記載というのは具体的にはどういうことが書かれてい

ればいいのかということについて、指宿先生、安富先生にお伺いしたいと思います。

○指宿参考人　御質問の趣旨は、百七条二項の「電磁的記録を複写すべきものの範囲を記載しなければならない。」の文言の解釈ですか。（大口委員「はい。そうです」と呼ぶ）

これは恐らく、当該被疑事実に関連するデータの、例えばこれこれの犯罪に関する日記であるとか計画であるとかを記載した電磁的な記録というような形で列挙されるのではないかというふうに考えます。また、例えば不正な取引を明記した記録であるとか、そういうことで範囲が特定されていくのではないかと想像いたします。

○安富参考人　お答えいたします。

関連性との関係につきまして、具体的に当該被疑事実との関連性があるというふうに考えられるものといいますか記録媒体について、個々具体的にそのケースごとに記載していくということになるのだろうというふうに考えられますので、ある被疑事実に関する何々を記載した電磁的記録というような形で書いていくものだというふうに想像されるところでございます。

○大口委員　次に、指宿先生にお伺いをいたします。

クラウドコンピューティングの技術がこれだけ進展して、データの保存先が国内でないことが少なくない。そこで、リモートアクセスとクラウド技術の衝突ということを先生おっしゃっているわけでございますけれども、こういう場合に、サイバー条約が十周年を迎えて、域外、越境的捜索の許容の議論が今行われているというふうに論文に書いておられますけれども、この議論が今どういう状況なのか、お伺いしたいと思います。

○指宿参考人　私、水曜日にここに出頭するよう依頼されまして、急遽ヨーロッパにコンタクトをとりまして確認をさせていただきました。

現在、資料提供いただいているのは、欧州評議会でサイバー犯罪条約の改定の主任を務めておられるアレクサンダー・シーガー氏から情報提供をいただきまして、現在の欧州での議論状況をまとめたペーパーをいただきました。

現在、欧州評議会で最新の議論をまとめたものといたしましては、昨年の八月に、クラウドコンピューティングとサイバー犯罪の捜査、こういうディスカッションペーパーが出ております。

現時点では、今日のこのクラウドコンピューティングの技術にとって何が克服しなければならないことかという課題整理と、それを解決するための技術的あるいは国際協調の枠組みの可能性を列挙するということ、そして、それを行うにしても、どのような条件をクリアしなければならないかということを洗い出す作業が行われております。

学問の世界でありますが、学説の方ではさまざまな研究ないし発表がございますが、これについてはきょうは省略させていただきますけれども、現実に私どもが、例えば先生方でも、グーグル社の提供していますGメールをお使いの先生もおられるかと思うんですが、ブラウザー上でメールを読み書きするサービスですけれども、これはいわゆるクラウドコンピューティングで運用されているところですので、利用者の添付ファイルがどの国のサーバーに保存されているかは特定ができない。しかも、それはだれも制御できないわけですね。時々刻々、その保存場所は変更されていくわけです。それがまさにクラウドコンピューティング技術でございます。

それから、ストレージサービスでも、例えば、最近非常にユーザーのふえていますドロップボックスというストレージサービスがございます。これは、コンピューターのスクリーン上でドラッグすることによって自分のデータを簡単にストレージにほうり込むことができるサービスですけれども、このドロップボックスも、データが保存されるサーバーは各国に散らばっていまして、それを特定することはできません。

このような、クラウドプロバイダーと申しますけれども、クラウドプロバイダーの今のビジネスの進展を妨げるような形で越境的な捜索を優先させるということがあってはならないというようなやはり産業界の要請とのバランスをとりながら、現在、その仕様の確定が進行中でございます。こしがサイバー犯罪条約十周年なので、十周年に間に合うかどうかは私は承知しておりませんけれども、急ピッチで作業が進んでいるというふうに仄聞しているところでございます。

○大口委員　指宿参考人にもう一つお伺いしたいんですが、保全要請とそれからその後の差し押さえの時間的な幅ということについて、先生はアメリカの連邦法を引用されて、法執行機関からの要請について、裁判所による令状発付手続またはその他の手続が進行している間という制約がつけられているということで、そういう担保が置かれるべきだ、こういう御主張でございます。アメリカだけじゃなくてカナダも、緊急の状況、令状が間に合わない期間、こういう制限をつけていると。

海外からの保全要請の場合は、これは三十日とか六十日、時間がかかるわけですけれども、国内においては、これはやはり差し押さえとの近接性というのが大事だと思うんですが、この点についてお伺いしたいと思います。

○指宿参考人　私の主張は論文に書いてあるとおりでございますけれども、法案の中でも、必要がなくなったときには保全要請を取り消すということが捜査機関に義務づけられておりますので、我が国におきましてもそうした配慮が一定なされているとは思います。

しかしながら、諸外国でなぜそうした近接性が要求されているかというと、捜査機関に努力義務を課す、それは、必要性がなくなった場合に取り消すのではなくて、常に相手方に負担をかける処分であるということを捜査機関に認識させ、できるだけ負担が軽減されるような方向で諸外国では規制をかけているのではないかというふうに思料いたします。

○大口委員　ありがとうございました。以上で終わります。

○奥田委員長　次に、城内実君。

○城内委員　城内実でございます。

本日は、先生方、お忙しい中をお越しいただきまして、ありがとうございます。

まず、指宿参考人に質問したいと思います。

指宿先生は、先ほど、通信履歴の保全要請及び差し押さえについてはいかなる犯罪類型も対象とできる、通信傍受法の場合は非常に限定的で、いわゆる組織犯罪といった形であるにもかかわらず、今回の場合は非常に広範囲であるということをおっしゃいましたが、これと憲法との関係について、もう少し具体的に御説明いただければと思います。

○指宿参考人　通信傍受法の導入に際しましては、通信の秘密あるいはプライバシーの保護との関係で国会で非常に激しい議論が行われ、さまざまな条件のもとで実施されるということになったと承知しておりますので、やはりそのこととの比較ということを抜きには考えられないのではないかと考えております。

まず、通信の秘密の方からスタートいたしますと、事業法でもそうですけれども、通信の内容、記録、双方ともが通信の秘密によって保護されております。ただ、通信傍受法は専ら内容を知るための手段を捜査機関に与えるためということでしたので、当時、通信の記録についてどのように取り扱うかということは主な議論の対象にはなっておりませんでした。ところが、サイバー犯罪条約を見ますと、条文上明確に、これは通信の内容の傍受についての法整備と通信記録の法整備とを条文を分けて規定しているところであります。

恐らく、通信内容につきましては既に我が国ではもう解決済みだということですので、そこで今回の通信履歴、通信記録の保全ということが出てきたというふうに理解しておりますが、そうなりますと、通信傍受の場合の通信の秘密の保護のレベルと通信記録の通信の秘密の保護のレベルをやはり関連づけて考えておくべきなのではないかというのが私の見解でございます。それは、諸外国

と違いまして、我が国の憲法では通信の秘密を明示的に憲法上保護しており、アメリカ合衆国のようにそのような憲法上の直接の規定を持たない国とは事情が異なるというのが私の見解でございます。

○城内委員　今まで話を聞きまして、指宿先生はどちらかというと慎重、反対というか、侵害法益の大きさに比べて強制の要件が緩やか過ぎるということですが、他方、今井先生、安富先生は、今非常にコンピューター犯罪がふえているという社会的な要請もあって、むしろ前向きで積極的であり、かつ、先ほど安富先生おっしゃったように、犯人特定のために通信履歴は必要であるから、保全要請というのはこれはもう必要である、そういう前向きなことをおっしゃいました。

　私は、先ほどどなたかも御指摘されたように、保全を要請する場合でも、大きなプロバイダーであればいいんですけれども、小さなプロバイダーの場合はいろいろとコストや手間暇がかかって、これは非常に業務を妨害するようなことが十分あると思うんですが、その点について改めて今井先生、安富先生からお答えいただきたいと思います。

○今井参考人　先ほども申しましたが、私は専門が刑法実体法の方でございますので、手続法の方に関して熟知しているわけではございませんが、先ほどお答えしましたように、今回の保全というものがいわば外形的に情報を保全するという方向で考えておられるようでございますので、コストについても、それほど大きなものが発生するとは考えておりません。

○安富参考人　お答えをいたします。

　これはあくまでも保全の要請ということでございますので、その限りにおいてそれぞれのプロバイダーができるところでやるということを前提としている規定であるというふうに理解しておりますので、できないところはやむを得ないということになるのではないかというふうに承知しています。

○城内委員　またちょっと別の論点に移りますが、指宿先生は、この論文の中で、通信履歴については電子メールに関する範囲の点で解釈上争いの余地があるということを述べておられます。もし通信履歴としてログなどをすべて網羅するとするならば、電子メールのいわゆるヘッダー情報ですね、何月何日、だれが、どこのサーバーからどういったサーバーを経由して、どこのアドレスに行ったのかというような、こういったヘッダー情報のうち、件名が含まれるかどうかが問題となり得るというふうに指摘しておられます。

　確かに、例えば件名で、私がつくったウイルスについてなんという件名は、その内容を件名の中にほとんどそれをあらわしていますから、これについてどうするのかというのは、当然、議論が起きてくると思いますが、この点について指宿先生から、どのようなものまで含むべきで、含まないのかということをお答えいただくとともに、今井先生、安富先生からも御意見をお伺いしたいと思います。

○指宿参考人　まず、通信の、いわゆる電子メールの場合、ログと言われるものですけれども、どの範囲でこれを記録するかは、それぞれのプロバイダー、業者ごとに異なっているようでございます。私は業者の者ではないので詳しくはわかりませんけれども、これは一律に決まりがあるわけではございません。

　他方、サイバー犯罪条約を見ますと、何が通信の記録、履歴なのかということにつきましては、電子メールの場合、通信のログに当たるものとして、記録するべきものは明示されております。これは参考資料の方にサイバー犯罪条約の条文がございますので、ごらんいただきたいと思います。それに対しまして、我が国の規定ぶりは、通信履歴の最後に等というふうに、列挙されたもの以外も含ませることが可能なようになっております。

　私が気になるのは、やはり、サイバー犯罪条約が限定列挙であるのに対して、我が国の条文案の場合は、これがいわば例外といいますか、落ち穂拾い的に何でも入れてしまえるような形になっているというところが気になる点でございます。

　それは恐らく、条文作成者の立場からしますと、業者ごとに記録している項目が違うのであるから、それを一律に規定してしまうのはいかがなものかという発想があるのだろうと思うんですけれども、そうなりますと、今御指摘のあった、ヘッダーの中のいわゆる件名の部分を含ませるかどうかということが問題になってまいるかと思います。

　この件名部分につきましては、アメリカ合衆国の場合はこれは通信本文とみなされておりまして、記録としては傍受できないということになっているので、この点、我が国ではこれまでほとんど議論されたことがないテーマですので、もし、このまま記録を取得するということになりますと、我が国でこの取り扱いをどうするかという具体的な指針が必要になろうかと存じます。

○今井参考人　業者が保存している電子メールの保全をする際の具体的な問題でございますけれども、今、指宿参考人からも御指摘がありましたように、メールのサブジェクト及びヘッダーについて、どこまでが通信の秘密の保護に当たるかということは、各国によって状況が異なっております。

　アメリカの話は今御紹介があったと思いますけれども、私の知る限りでは、イギリスなどではまた伝統的に異なった意見もあるところであり、それがゆえに、ヨーロッパにおけるサイバー犯罪条約等でも議論がされているところですが、我が国の法案で通信履歴等と書いてあるところは、先ほどのウイルス作成罪の場合と同じ解釈がなされるべきでありまして、通信履歴を保全する目的との関係で必要最小限度、他方で、その対象となる業者の特性を踏まえた判断がなされるわけであり、そこにも刑事訴訟法の原則である、あるいは一般的な行政法規の原則である比例性の原則、補充性の原則が働きますので、その限りにおいては特に不都合なことはないものと理解しております。

○安富参考人　お答えをいたします。

　通信履歴というのは、一般的には、通信の日時、それから通信元、通信先というふうに考えられるところでございますが、本案におきましては、などという文言が入っているので、そのいわば外延部分といいましょうか、どこまでがそれに含まれるのかということは問題になる点ではあろうかとは思います。

　しかしながら、今、今井参考人もお話しになれましたように、本来、この通信履歴を保全要請というのは、その先の、差し押さえるために差し押さえの対象を特定していく、あるいは犯人特定のために使うという目的があって、捜査上限定的にそれを利用しようということがあるわけでございますし、必要最小限度の範囲で通信履歴を保全するというのは、これは刑事訴訟法における比例原則というふうに言っていいかと思いますが、当然のことであろうかと思います。

　その意味では、何のために使うのかということを考慮した上で、おのずからその通信履歴の内容というのは決まってくるのではないかというふうに理解いたします。少なくとも、通信内容に踏み込むということは、これは許されないことであるということは理解しているところでございます。

○城内委員　今御指摘あったように、通信内容に踏み込まないようにということですが、件名についても、これをどう扱うかによっては通信内容そのものとみなされる場合もあるので、ここら辺はやはりもう少し捜査当局がきちんとルールをつくって適用しないと、どんどん通信内容に踏み込んでいくような危険性があるんじゃないかなと私は若干そこは懸念しているわけであります。

　最後の論点ですけれども、先ほど、クラウドコンピューティングの話がありました。これは、先ほど御説明もあったように、昔はプログラムやデータは手元にあるデータストレージという保管機器に保管していたんですけれども、昨今、データやプログラムの大容量化、多様化が進むにつれまして、コスト面でより安くしようということ

で、グーグルとかアマゾンを初めとするＩＴ企業が大型サーバーをたくさん持っていますので、それを使って、ユーザーが自前のサーバーやプログラムを持つことなく、安価に、あるいは平易にデータを使うことができるようになったということです。

こういう状況があれば、捜査機関が保全あるいは差し押さえをしようとしたデータが海外にある、あるいは次から次へと移ってどこにあるかわからなくなってしまうというような、それからまた捜査共助の問題も出てくると思うんですが、この点についての法制化をやはり十分検討しないと、法益の趣旨はわかるんですけれども、絵にかいたもちになってしまうんじゃないかなと思うんです。

その点について、一番お詳しいと思われる指宿先生から再度御説明いただきたいと思いますし、また、もし時間があれば、今井先生、安富先生から一言ずつ、この点について御意見を述べていただきたいと思います。

○指宿参考人　時間も限られておりますので、簡単に申し述べさせていただきます。

例えば、クラウドコンピューティングによって提供されている国民の電子的な財産をどのように保護するかという観点から見ました場合、現在、これは世界的に見ましても非常に複雑な問題を抱えております。

例えば、審議中のこの法案とは直接はかかわりませんけれども、プライバシーの保護の問題、個人情報の保護の問題。一体どの国のどの規定がそのクラウドサーバーに保存されているデータに適用されるのか。そのプライバシーの保護を、一体だれが、どのレベルで、どの国あるいは条約の要件に基づいて保護する責任を負うのか。まさにサイバースペース時代の法体系という、刑事訴訟法に限らない、あらゆる分野の法分野において整備、検討が国際的に求められている時代でございます。

私が先ほど紹介しましたヨーロッパの検討も、単に犯罪捜査のためのみならず、プライバシーの保護でありますとか、そうした観点からも検討が同時に進められているところでありますので、本委員会におかれましては、サイバースペース時代のデータの保護、あるいは個人の通信の秘密の保護という広い視点で、御検討、御審議賜りたいと存じます。

○奥田委員長　今井参考人、御意見があれば簡潔にお願いいたします。

○今井参考人　ごく一言申し上げますが、今委員御指摘のように、サーバー等が海外にある際の捜査に対しては大変難しい問題があると承知しておりまして、捜査共助の効果的な実現が図られなければいけません。

その際、前提としては、刑法実体法としては、日本の刑法が適用できるかどうかということで、刑法四条以下の条文の適用が問題となりますが、その先に捜査共助が問題となったときには、伝統的な国際刑法の理論によると、双罰性の理論というのがございますので、Ａ国とＢ国との間でともに処罰されるような類型にあって初めて捜査共助ができるということになります。

そのためには、今回審議されております法案の実体法部分はまず何よりも通していくことが今後の捜査を有効に行うために必要でありまして、その先の各国協調したあり方について条約レベルで考えますが、まずＡ国とＢ国二国間の間についての捜査共助から進めることが重要であろうと思っております。

○安富参考人　お答えいたします。

クラウドコンピューティングの問題というのは、これからの重要な問題であろうかと思いますが、この法案との関係で申し上げますと、クラウドであっても、いわゆるリモートアクセスという仕組みの中で考えますと、同様な取り扱いで、差し押さえの対象となる電子計算機からということになりますので、この法案との関係では、同じような考え方で問題解決の道は可能ではないかというふうに私は考えております。

以上でございます。

○城内委員　ありがとうございました。

これで終わります。

○奥田委員長　これにて参考人に対する質疑は終了いたしました。

参考人の方々には、貴重な御意見をいただき、まことにありがとうございました。委員会を代表し、厚く御礼を申し上げます。（拍手）

どうぞ、御退席いただいて結構です。

○奥田委員長　この際、お諮りいたします。

本案審査のため、本日、政府参考人として警察庁生活安全局長樋口建史君、法務省刑事局長西川克行君、外務省大臣官房審議官武藤義哉君の出席を求め、説明を聴取したいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○奥田委員長　御異議なしと認めます。よって、そのように決しました。

○奥田委員長　質疑の申し出がありますので、順次これを許します。大口善徳君。

○大口委員　公明党の大口でございます。

参考人質疑を参考にして、ちょっと通告をしていないことも質問いたしたいと思います。

冒頭ですけれども、民主党の議員の方々も、この法案について、そんなに急ぐ必要はないのではないか、こういう意見があったり、慎重であるべきだ、こういう意見があるわけです。

大臣として、この法案は是が非でもこの国会で成立させなければならないという、その説得力ある、民主党の議員さんにも説得できる理由をまず答弁いただきたいと思います。

○江田国務大臣　いろいろな御意見はもちろんあることは承知をしておりますし、今の参考人質疑も外で聞かせていただきました。その中でも、時間をかけろという御意見もあるのも承知をしております。

しかし、サイバー条約は、これはもう締結をしてかなりの年月がたっておりますし、また、今コンピューターの世界というのは国際的にも広がっていて、私どもの日ごろの社会生活のインフラとしても欠かせないものになってきておりまして、その中で、コンピューターウイルスが犯しておりますいろいろな不都合、これは目に余るものもあるのでありまして、もう可及的速やかにこの法案はぜひ成立をさせていただきたいと思っております。

○大口委員　次に、フリーソフトウエアというものは、大臣、この前答弁されましたが、一般的には、ユーザーがその扱いを自由にできるソフトウエアのことで、我が国では、主として無償で利用できるという意味に使われております。

前回の質疑で私から、フリーソフトウエアを公開したところ、重大なバグがあるとユーザーからそういう声があった、それを無視してそのプログラムを公開し続けた場合は、それを知った時点で少なくとも未必の故意があって、提供罪が成立するという可能性があるのか、こういう質問に対して、大臣はあると回答されました。

この質疑は、その後、インターネットの中でかなり反響を呼んでおりまして、インターネットにおいて、フリーソフトを公開し、それに対して、バグについての報告を踏まえて何度も改訂して、徐々によりよいソフトウエアの完成を目指していくという文化があると言われているわけでありますが、すべて利用者の責任で使うことを条件に、自由なソフトウエア開発と自由な流通を促進することによってソフトウエアが発展してきた歴史的な経緯もある。ところが、その途中の段階で、バグがあるソフトを公開していることが提供罪として罰せられるということは、このような文化が阻害され、だれもフリーソフトを公開しなくなってしまうおそれがある、こういう危惧が出されております。

さかのぼって考えますと、そもそもバグが、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動

作をさせるべき不正な指令」に該当すると解釈されるように広い概念となっていることが原因だとも考えられますが、この点についてどうお考えでございましょうか。

○江田国務大臣　お答えの前に、先ほど、サイバー条約は署名でございまして、ちょっと言い間違えましたので訂正しておきます。

フリーソフトウエア上のバグの問題について、先般、大口委員の御質問で、私は、委員の御質問、可能性があるかと。可能性ということならば、それはあると簡単に一言答えましたが、これが多くの皆さんに心配を与えたということでございまして、申しわけなく思っております。

これも委員今御指摘のとおりで、私もこうしたことに詳しくありませんが、自分でコンピューターをいじっていて突然フリーズをするとかあるいは文字化けをするとか、いろいろ不都合が起きる、これはどうしてだと言ったら、いや、何かいろいろごみが詰まっているんですよというようなことで、そうしたものであって、フリーソフトウエアの場合にはそういうものがあることを、みんなある程度了解の上でいろいろやりとりをして、しかも、そうしたものがあればこれはなくするようにみんながいろいろな努力をしているので、こういう多くの皆さんの努力でいいものができ上がっているプロセスはあるし、そのことは非常に大切だと思っております。フリーでなくてもそういうことはあるわけです。したがって、そうしたバグの存在というのは、ある意味で許された危険ということがあるかもしれません。

ただ、そういうバグが非常に重大な影響を及ぼすようなものになっていて、しかもこれが、そういうものを知りながら、故意にあえてウイルスとしての機能を果たさせてやろうというような、そういう思いで行えば、これはそういう可能性がある、そういう限定的なことを一言で申し上げたので、そうした場合でも、その限界はどこかというのは、これはなかなか大変なことでございまして、捜査機関においてそのあたりは十分に慎重に捜査をして、間違いのない処理をしていくものと思っておりますので、無用な心配はぜひなくしていただきたいと思っております。

○大口委員　これにつきましては、やはりきちっとした形で、またこの構成要件の解釈について明確にこれからも法務省としても打ち出していただかないと、かなり現場は混乱していますので、よろしくお願いしたいと思います。

次に、通信履歴の保全要請の対象となる通信履歴について、これは刑訴法百九十七条で「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」と規定しています。「その他」に何が含まれるのか。

特に、今回も参考人質疑でもいろいろ話題になりましたが、電子メールの場合に、通常、ヘッダーの部分と本文があって、通信履歴というのはコンピューターが自動的に付与するもので、ヘッダーにある件名、サブジェクト部分は通信内容として理解されるべきと考えておりますけれども、そのような理解でよろしいんでしょうか。

○江田国務大臣　件名、サブジェクトというものでございますが、これは電子メールを送信する者が、件名のところに、先日はとかお礼とか、何かこう書き込んで、自分でつくるものでございまして、送信者が用いるメールソフトによって作成、記録されて送信されるということである以上、これは、通信履歴、つまり、通信事業者等が業務上記録しているもの、これには当たらないので、保全要請の対象とならない。つまり、通信の内容に当たるということでございます。

○大口委員　次に、今回の法案で、保全要請を受けたプロバイダー等の第三者に多くの負担、コストがかかるということが予想されております。

指宿参考人からも、小さなプロバイダーは大きな負担があるし、大きなプロバイダーは技術難度が高いということでコストアップにつながる、アメリカはその費用の請求ができる、また、場合によっては損害賠償の対象にもなる、ユーザーにも負担がかかる、こういうことでございました。

今回、保全する期間は九十日を、原則三十日で、例外として最大六十日と限定したわけでありますが、まだ負担は大きいと思います。民主党の修正案でも、「求めに応じた者は、同項の電磁的記録を消去しないようにするために必要な費用の支払又は償還を受けることができる。」という規定の提案をかつてしていたということもございます。

プロバイダー等の第三者の負担を軽減するためにそのようなことも検討しているのか、お伺いしたいと思います。

○江田国務大臣　これはもう委員、今おわかりと思いますけれども、通信履歴を新たに記録して保存することを求めるものではなくて、ただ消去しないように求める、期間についても御指摘のとおり、そして、必要性がある場合に限って保全要請を行うということでありまして、過度の負担を負わせることにはならないと考えておりまして、その費用は通信事業者等に負担いただけるものと考えております。

負担ができる限り小さくなるように事案に応じて配慮をしていこうと思っておりまして、それ以上のことを今考えているわけではございません。

○大口委員　それとも関連するわけでありますが、保全する期間について、原則三十日で、例外として最大六十日まで認められているわけでありますが、捜索・差し押さえ許可状は、申請者が即日か遅くとも翌日に令状発付されると考えられるわけです。保全する期間が長過ぎるようにも思われるわけですね。これほど長い期間が定められているのは、海外から日本に捜査共助が依頼されたような場合には、捜索・差し押さえ許可状に必要な疎明資料を海外から送付し、それを翻訳等して、疎明資料にするためにある程度の時間がかかるからであります。

日本国内だけで捜査する場合には、そんなに長い期間保全をする必要はない。保全要請してそんなに日数がたたないうちに差し押さえがなされるものと理解いたします。中には、例外的に確かに時間のかかるものもありますが、ほとんどは、保全要請してすぐ差し押さえといいますか、要するに、保全要請とその後の差し押さえの時間的間隔は極めて短いというふうに私どもは考えておりますし、そうあるべきだというふうにも考えます。

百九十七条の三項で、第二文ですか、「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。」という条文もそういう趣旨なんでしょうけれども、やはりこれから保全要請をするに当たっては、その後の差し押さえや記録命令つき差し押さえとの間隔をできるだけ短くすべきだと思いますが、いかがでございましょうか。

○江田国務大臣　これは委員御指摘のとおりだと思います。

差し押さえの必要があるときという要件があって、言ってみれば記録命令つき差し押さえの準備と位置づけられるものでございますから、今の、期間三十日、六十日というのはあくまで上限であって、実際には、捜査機関で、個別に、通信事業者等の負担も十分配慮して、具体的事情を踏まえて、より短い期間を適切に定めていくように努めるものと思っておりますし、また、捜査機関としては、これはもちろん、早期にこうした情報を入手したいと考えるのが当然でございまして、必要とされる令状を速やかに取得する、そういう運用になっていくものと思っておりますが、若干の期間が必要という場合も考えられますので、一応三十日、六十日ということにしておるということでございまして、速やかに運用していくというのは当然でございます。

○大口委員　次に、記録命令つき差し押さえについて、捜査機関が対応する場合は、海外、域外サーバーの場合、壁があるわけでありますけれども、第三者に命じてやる方式ですと、海外、域外サーバーにも差し押さえができるというふうに指宿参考人の文献にもあったわけでございますが、この第三者に命じて行わせる方式でこういう域外サーバーの主権の壁の問題を回避することが可能

か、お伺いしておきます。

○江田国務大臣　記録命令つき差し押さえは、もちろんこれは、我が国に所在する者に命じて行われるものでございます。その記録をする者が、仮に海外に記録媒体が所在しているとしても、そこへアクセスして、そして電磁的記録を記録するという複写の行為自体は、その命令を受けた者、国内にいる者が行うわけで、その者が自分の権限で行うものでございまして、主権の制約というものにはかからないと思っております。

○大口委員　時間が来ましたので、以上で終わります。

ありがとうございました。

○奥田委員長　次に、辻惠君。

○辻委員　民主党、辻惠でございます。

今回の法案、サイバー法案と従来言われておりましたけれども、コンピューターを扱う人々、また広い多くの方々から、コンピューター監視法案と呼ぶべきではないかという指摘があります。名は体をあらわすという言葉がありますが、コンピューターの監視につながるような危うい要素のある法案ではないかという指摘があるのは事実でありますので、それらの点について、捜査の権限が濫用されないように、運用いかんによって本当にそういうふうになるということをやはり懸念している方が多いわけですから、その歯どめをしっかり確認させていただきたいなというふうに私は思います。

まず、この審議の中で明らかになったことを幾つか確認したいと思います。

コンピューターウイルスによる攻撃が非常に大きい理由になっておりますけれども、例えば、この審議の中では、コンピューターウイルスに関する犯罪として検挙されたのは二〇〇三年から一〇年の間十三件、うち十件は不正アクセス禁止法で違反である、三件がその他の罪名で検挙に至っている、非常にいろいろ誇大に宣伝されるような立法事実があるわけでは必ずしもないのではないかということが事実として出たと思います。

また、作成罪については、これは提供以前の、対外的な実行行為以前の行為を処罰するものでありますから、捜査機関の濫用によって、実行行為以前の、ある意味では表現の自由、内心の自由を侵害される危険性が要素としてあるという事実も指摘されたところであります。

そして、正当な理由がないとか目的罪ということでありますから、主観的要素が非常に重要な要素となっておりまして、では、そもそも、これを客観的に証明できる、どんな材料によって捜査の端緒を得ることができるのかということについても非常にはっきりしないということもあります。ほかの件で捜索が行われたときに、たまたま現場で発見されて、そこから芋づる的に作成罪に広がっていくというような、それは捜査機関の権限の濫用につながるのではないかという指摘があるという事実もありました。

そして、本店のサーバーを差し押さえたところ、支店のデータの差し押さえにも及んでしまう。リモートアクセスについては、憲法三十五条一項の令状主義の趣旨にかんがみて、やはり慎重になされなければならないのではないかという指摘がありました。また、差し押さえを受ける側の負担の軽減について配慮する必要もあるのではないか。

さらに、通信履歴の電磁的記録の保全要請については、プロバイダー業者等について、これは事実上の保全をしなければいけないという強制になるのではないか。また、三十日、さらに三十日ということで保全しなければいけないというのは過重な負担にはならないか。差し押さえの必要性の現実的な、具体的な理由がないのに、事前に、それの要件をむしろ逸脱するような段階での保全要請ということがあり得る危険性も指摘されたと思います。

さらに、サイバー条約批准後、憲法二十一条二項との関係で、通信の秘密が憲法上保障されておりますけれども、通信履歴がさらに通信内容に及ぶようなことがあってはならないという懸念も示されておりますし、これが従来の共謀罪を含めた三法が一体となって提案されてきた経過を見れば、共謀罪の水先案内になってしまうのではないかという懸念も指摘されたところであります。

そこで、大臣に、これらの危険について、どのような歯どめが考えられるのかという点について御質問をさせていただきたいと思います。

まず、作成罪についてでありますけれども、恣意的な捜査や見込み捜査があってはならない。コンピューターウイルスによるコンピューターに対する切迫した具体的危険性が生じた場合に限って捜査が開始されるべきだと考えますが、いかがでしょうか。

○江田国務大臣　国家の刑罰権というのが間違っても濫用されて国民の基本的人権を侵害するようなことがあってはいけない、これはもう言わずもがなのことでございまして、辻委員初め多くの皆さんが、そうした観点から今回のこの法案についていろいろ疑義をただしていただいたことは大変ありがたいことだと思っております。

その上で、作成罪でございますが、今のコンピューター秩序というものの重要性を考えれば、コンピューターウイルスを作成する、これは具体的な行為でございまして、作成されたコンピューターウイルスというのが大変な害悪の根源になるという意味で、当罰性は十分認められる。

ただ、さはさりながら、これはコンピューターの中にまだ存在している段階でございますから、これを見込み捜査などで捜査をして、あっ、結果的になかったなどということが横行するようなことがあってはいけません。

そこで、コンピューターウイルスの作成に続く供用罪など、そうしたことによって、外形的に、どこかで作成されているに違いない、こうして捜査の端緒が開かれる場合というのが多いであろうと。そして、そういうようなところで入っていって、ここで作成がされているというところへたどり着きましたら、これは作成罪で検挙できる、そういうプロセスになっていくし、また、作成罪と供用罪、あるいは、その結果の器物損壊等の牽連犯あるいは観念的競合、そういった罪と罪との関係といったこともございますので、作成罪の摘発に当たっては、委員御指摘のような慎重な配慮というものは必要だと思っております。

○辻委員　次に、リモートアクセスに関連して伺います。

例えば、先ほど申し上げたように、本店、支店ということで、本店のサーバーの差し押さえをしたところ、支店に保管されているデータについて、いわば網打ち的な差し押さえに至る危険性があるのではないか、これは憲法三十五条一項で言う令状主義、捜索場所や物の特定という令状主義を逸脱することになるのではないかという指摘があるわけであります。

したがいまして、この差し押さえに当たっては、その対象ができるだけ特定されるように、捜査機関に運用の指示をすべきであろうというふうに考えますが、この点はいかがでしょう。

○江田国務大臣　今のコンピューターネットワークというものが、現に目の前にある電子計算機の中に電磁的記録が記録されている場合以外に、さまざまな記録媒体が、そのコンピューター外にあってそちらに記録されているというのがもう無数にある。今の状況はそういうことになっているわけで、したがって、目の前にある電子計算機にあるさまざまな電磁的記録に一定の強制を加えようとする場合に、リモートアクセスというものが避けられないということは事実で、ただ、リモートアクセスが野方図に広がってしまいますと、これは令状主義との関係でどうなるのかということは、もう委員おっしゃるような問題があるわけです。

したがって、令状に、電子計算機と、さらに、そこからアクセスの可能な記録媒体、そこにある記録の範囲、こうしたものを令状上に明示して運用すべしということでございまして、こうしたものが間違った運用にならないよう、これは捜査機関にも周知をしていきたいと思っております。

○辻委員　差し押さえを受ける者の負担を軽減するために、電磁的記録の差し押さえに当たっては、できる限りそれを他のディスク等へ複写等した上で当該ディスクの差し押さえを行うべきだというふうに考えますが、この点はいかがですか。

○江田国務大臣　記録媒体自体を押さえてしまうというよりも、複写をして電磁的記録を押さえるという方法の方が相手に余計な負担をかけないことになることは事実でございまして、なるべくそうした方法によるべきという委員の御指摘はそのとおりだと思います。

ただ、そうした協力が得られない場合は、これは記録媒体自体を押さえなきゃいけない場合があるし、さらに、記録媒体自体を押さえることによって、その記録媒体にありますさまざまな情報をしっかり解析することによって事案が明らかになっていくということもございますので、記録媒体の差し押さえということも、もちろんこれは排除するわけにはいかないということだと思います。

○辻委員　通信履歴の電磁的記録の保全要請に当たって、先ほど申し上げたように、非常にこれは業者に対する負担とかが生じる危険性がありますす。そういう意味で、差し押さえを行う必要が具体的に本当にあるという場合に、最低限、必要な期間に限定して保全要請は行うべきだし、また、保全要請の要請先についてはインターネットサービスプロバイダー等の通信事業者に基本的にやはり限定して要請するようにすべきだというふうに考えますが、簡潔に、この点はいかがでしょう。

○江田国務大臣　差し押さえの必要があるときは、これはもう条文上それを明記をしているわけで、おっしゃるとおりでございます。

相手方については、業者に限るということにはしておりませんが、濫用にわたらないように注意をしていきたいと思います。

○辻委員　私の前回の質疑の中で、サイバー条約が批准後、通信履歴にとどまらず通信内容に拡大するような、そんな法改正があってはならないということを申し上げて、江田大臣も、そういうことはないんだというふうに答弁をされたことをこの場で再確認させていただきたいと思います。

もう一点。過去、これが共謀罪と一体的に提案されてきたということで、本法が共謀罪制定に連動するものなのかというような懸念が指摘されているところであります。この点に関して、大臣は、前政権が出した共謀罪は断固反対であるということを言明された。そして現在、関係省庁としっかり協議をしており、与野党の皆さんの御意見もいただきながら、国内法を設けなくても批准できるという考え方もあるんだ、そういうことも念頭に置いて協議をしていくんだということをおっしゃられました。

そういう意味で、私は、この国連の組織犯罪防止条約の批准と国内法の整備ということについては、例えば、いろいろな、準備罪や予備罪や共謀共同正犯理論の定着化等によって、条約の三十四条が要求する国内の基本法制は、これは現に既に存在しているんだという理解は十分にあるというふうに考えますし、そういう意味で、あえて国内法を整備する必要がないという意見があるということを申し上げておきたいと思いますし、仮にその点が国際的に疑義が生ずるとしても、これは本来は締約国の間の交渉によって解決すべきだというのがこの国際犯罪条約の三十五条に規定されているところでありますし、国連がその批准を、国内法の整備なしに批准をしたからといって、それに対して疑義を言う、そんな筋合いではないんだというふうに考えます。

このような意見について、やはり基本的に尊重していただきたい、このように思います。いかがでしょう。

○江田国務大臣　国際組織犯罪防止条約、これの締結に当たっての国内法整備に関して、これまでの国会審議については、これはもう委員今御指摘のとおりで、私もそうした中で一定の役割を果たしてきたと思っておりますし、そのことが間違いであったとは、当然これは思っておりません。

ただ、この条約を、これはもう国会で承認もしていただいているわけでございますし、これをやはり締結していかなきゃならぬ、そのために何が必要かということについて今いろいろな協議をやっている最中で、これは何が必要なのか、あるいはこういうことは必要じゃないんじゃないか、そうしたことについてのいろいろな御意見がありますので、関係省庁ともしっかり協議をしながら検討を進めていく。その際に、今委員御指摘のようなことは十分踏まえてまいりたいと思います。

○辻委員　条約の批准に当たっては、条約を精査いたしましたが、既にそれに沿う国内法は十分整備をされている、新たな整備は必要がないという意見があるし、日弁連もそういう見解に立っているということを十分御考慮いただきたいということを最後に申し上げまして、私の質問を終わりたいと思います。

ありがとうございました。

○奥田委員長　次に、柴山昌彦君。

○柴山委員　自由民主党の柴山昌彦です。

今も少し出ましたけれども、今回の、コンピューターウイルス作成段階で処罰可能とする法案は、私たちが前政権で治安確保のため必要だと考えて一体として提出した法案のうち、組織的な犯罪の共謀を処罰可能とする部分を落としたものです。

ともに、現行法の処罰範囲を、実害発生以前の行為という点で拡大することを内容としながらも、国会で承認した条約に基づく法整備であって、一方の共謀罪はあれだけ強硬に反対だとしておきまして、一方のコンピューターウイルス作成罪は結構ですという方針に、民主党との調整はきちんと済んでいるんでしょうか。

○江田国務大臣　きちんと済んでいると理解をしております。

○柴山委員　済んでいたらいいんですけれども、前々回の質疑で橘委員から、民主党の法務部門会議では、相当これは異論であったり反対というものが相次いでいたのですが、何かいつの間にか結局決まってしまって、法案が提出をされてしまったんじゃないかといった印象を持つものでありますすというような御指摘もありますし、また、橘委員のブログでも、手続上の問題ということがある書かれているように思います。

さはさりながら、民主党の党内手続が仮に済んだといたしましょう。今御指摘のあった共謀罪については、これはどうなっているのかということについてぜひお伺いしたいと思います。

○江田国務大臣　前政権といいますか、一昨年の九月の政権交代以前の政権が提案をされておりました共謀罪、いわゆるつきですが、これについて民主党として反対という態度を決めているのは、これは事実でございますが、そのときに出されましたさまざまな問題点を踏まえて、条約締結のための国内整備にどういうものが必要であるか、可能であるか、これは党としても十分検討をこれからしていただけるものと思っております。

共謀罪というのは犯罪の実行に着手する前の段階の処罰、コンピューターウイルスは作成という実行行為が行われた場合の処罰でありまして、根本的に違うので、そこは、先ほど委員の御質問の冒頭にありました点はちょっと見解を異にするかなと思っております。

○柴山委員　ところが、これまで累次の共謀罪での質疑におきまして、例えば対象犯罪を絞り込むですとか、今、江田大臣がおっしゃったように、純粋たる共謀はやはり処罰の対象とするのはおかしいんじゃないかというような御指摘を受けて、明確な外部的行為というものを伴った形でやはり処罰をするというような、さまざまな限定の方向での修正ということも議論されてきたことも事実なんですね。

コンピューターウイルス作成罪についても、いろいろと濫用のおそれがないように修正をしているわけですから、これとしっかりと理論的な一貫性を貫くような形で共謀罪についてもぜひ検討していただきたいと思うんですけれども、江田大臣は、これに対して、新規立法が必要かどうかはいろいろ意見があるというようなことも、今お話が

あったように前回質疑でおっしゃっていますが、結局、いつまでにどうされるんですか。

○江田国務大臣　これは今、この委員会でもいろいろ御質疑があったところで、両方の意見もございますし、また関係省庁との協議も十分進めていかなければならないことでございまして、いつまでにという確定的な日時を今お答えする段階には至っていないと思っております。

○柴山委員　しかし、コンピューターウイルスに対する対応も喫緊の課題かもしれませんけれども、さまざまな組織犯罪だとか暴力団とかあるいはテロへの対処ということも、これもやはり国際的な喫緊の課題でもあります。

　前回の質疑で、組織犯罪防止条約の五条に定める共謀罪または参加罪の立法化などの措置がなければ結局条約上の義務を果たしたことにはならないと、同僚の稲田議員などの質問に対して外務省が明確に答弁をされていましたが、これについて再度確認をさせていただきたいと思います。

○武藤政府参考人　お答えいたします。

　国際組織犯罪防止条約、ＴＯＣ条約でございますけれども、この五条１、これは、重大な犯罪を行うことの合意または組織的な犯罪集団の活動に積極的に参加することの少なくとも一方を犯罪とするということを義務づけてございます。したがって、この条約を締結するに当たっては、上記行為のうちいずれか一つが犯罪とされている必要があると考えております。

　ＴＯＣ条約につきましては、平成十五年に国会承認をいただきまして、その国内担保法についての議論がなされてきたところでございますけれども、ＴＯＣ条約の締結に伴う法整備については、これを進めていく必要があると考えておりますが、条約に従っていかなる形で進めるのが適当かという点も含めて、関係省庁との間で協議をしながら検討を行っているところでございます。

○柴山委員　必要性はありますし、今お話があったように、やはり何らかの形で、どういう形をとったらいいのかということは協議をしなければいけないわけですから、くれぐれも立法不作為というようなそしりを免れないように、どういう検討が行われているかということも含めて、しっかりと……（発言する者あり）辻議員、ちょっとやじを飛ばさないでください。しっかりと議論の状況については委員会でも明らかにしていただくようにお願いしたいと思いますが、いかがですか。

○江田国務大臣　これは、今まさに関係省庁がしっかり議論をしていくべきことであって、その議論については、もちろん委員会での審査の対象になるものと思います。

○柴山委員　次の質問に移りますが、事前には通告をしていませんが、先ほどちょっと大臣の答弁をお伺いしていて気になる点がありましたので、一点確認をさせていただきたいと思います。

　フリーソフトウエアのバグの問題で、バグがあることを知りつつも、引き続きそれをインターネット上の提供状態に置いていた場合に、提供者にウイルス提供罪、ウイルス供用罪が成立するかどうかというところで、大臣は、成立する可能性はあるんだけれども、ただ、目的として、損害や誤作動を与えるというような積極的な目的を持っていなければこれを処罰できないというようなお話をされていたのかなと思うんですけれども、ただ、これは条文を見ると、目的はあくまでも「電子計算機における実行の用に供する目的」というように書かれておりますので、大臣がおっしゃったような目的を私は限定の材料にすることはできないんじゃないか。

　もちろん、利用者の推定的な承諾、推定的という言葉を使うかどうかはともかく、それは一つ根拠になります。あと、正当な理由なくといって、つまり、やはり一定のそういったバグがあっても、それを上回るさまざまな効用というものがあれば、これを提供し続ける正当な理由があるのかどうか。そういうようなところで縛りをかけるのはともかく、条文上、やはりこの目的のところで限定というものをすることはできないんじゃないかなというように思いますので、江田大臣、先ほどの御答弁を繰り返してください。

○江田国務大臣　条文の一つ一つの文言についての細かな解釈ということになりますと、私もよく吟味をしながらお答えをしなきゃならぬかと思いますが。

　全体にこれは故意犯で、そしてもちろん故意は積極的な故意だけじゃなくて未必の故意と言われるものもあるわけですけれども、やはりそういう故意犯であるということは一つの縛りになるし、さらに、フリーソフトウエアというものが持っている社会的な効用、フリーソフトの場合にいろいろなそういうフリーズなどのことが起きるということをあえて引き受けながら、しかし、フリーソフトの世界をより有効に、有用に社会的に活用していこう、そういう、ここへ参加をしてくる者の多くの認容というものはあるわけで、そういう意味では、ある程度のバグ的なものがあってもこれは許された危険ということになっていくのだと思いますし、そこはまた、もし時間がありましたら、この条文の一語一語について細かなコンメンタール的な解説というものは必要かと思います。

○柴山委員　今御指摘のように、許された危険というのは一つの考え方かと思います。

　続きまして、保全要請の問題について質問をさせていただきます。

　今回、通信履歴の電磁的記録の保全をプロバイダーなどに要請する制度を新設するに当たって、書面によることとするとともに、要請主体を検察官、検察事務官や司法警察員に絞りました。そしてまた、「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」に限定をいたしました。しかし、これらはいずれも捜査側の行為規制であって、濫用防止として不十分じゃないかという指摘もあるところです。

　そこで、大臣に伺うんですけれども、この保全要請の運用状況の国会報告など、外部の目を入れる制度について検討されていますか。

○江田国務大臣　濫用防止について、保全要請をする側にいろいろな縛りをかけるということで濫用にわたらないようにしようという努力をしてまいりまして、ここまで歯どめをかけますと、濫用ということは考えがたいと思っております。

　さはさりながら、やはりどの程度の件数、どういうものがあったか、そうしたことを把握して事後的に報告をする制度を設けてはどうだという御指摘については、そういう御指摘をいただいているところでございますが、なかなか、捜査現場の負担のことも考え、また、迅速かつ機動的な捜査に支障が起きるかといったことも考えていかなければいけませんので、そうしたことを総合勘案いたしますと、これが濫用にわたらないよう適正に運用されること、これの周知を十分していき、そして、それを踏まえた上で、運用を見守らせていただきたいと今のところ思っております。

○柴山委員　ちょっと今の御答弁には納得できません。というのは、今申し上げたとおり、書面によって要請するということを義務づけているわけですよ。紙が出ているわけなんです。紙の枚数を数えれば、すぐにそんなもの、事務作業なんかは必要なくわかるわけですよね。

　また、緊急性というふうにおっしゃいましたけれども、これは別に、捜査の途中に出せなんて私は言っているわけではありません。実際に捜査を遂げ、そして、要請の後に続く差し押さえなんかも終わった形で、その件数ですとかあるいは要請した理由、こういうものをただ統計的に報告させればいいということですから、これに例えば警察上の何か手間が過大にかかるということは全く考えられないと思うんですけれども、警察庁、いかがですか。

○樋口政府参考人　通信履歴の確保は、私ども、サイバー犯罪の捜査、検挙が非常に大きな課題になっていますけれども、それだけではございませんで、各種の犯罪捜査で、被疑者特定で欠かせない捜査事項でございます。

　現状におきましても、御承知のとおりでございまして、通信事業者の通常の保存期間の制約があるものですから、現状でも、捜査の進捗状況を踏

まえて、必要があると考えた場合には、関係の通信事業者に対しまして特定の通信履歴の保存をお願いいたしておるところであります。その際には、過度の負担にならないように、十分な配意をしながらやっておる。

ただ、件数的には、申し上げますと、サイバー犯罪に限らず、さまざまな犯罪捜査で必要があるものですから、サイバー犯罪の検挙だけでも、昨年、年間で約七千件ございます、等々勘案をいたしますと、保全要請の件数は相当多数になるものですから、仮にこの報告が求められるということになりますと、捜査現場にとりましては非常に大きな負担になるのではないかと危惧をいたしております。

○柴山委員　紙の枚数を集計して出すということに、そんなに私は、そんな十万件も二十万件もあるなら話は別ですよ、負担があるとは到底思えませんので、ぜひこれを国会報告の対象にしていただきたいということを、この法案とは別に強く要請させていただきまして、私の質問を終わらせていただきます。

ありがとうございました。

○奥田委員長　次に、城内実君。

○城内委員　城内実でございます。

けさの朝日新聞の記事がございまして、その中で、今、急速な普及を見せている多機能携帯電話、いわゆるスマートフォンというのがありますが、これをねらったコンピューターウイルスが急増している、そういう内容の記事でありました。セキュリティーソフト大手トレンドマイクロの調査によりますと、昨年、二〇一〇年中はたった五種類だったウイルスが、既に五十七種類にまでふえているということであります。

こうしたウイルスは、いわゆるアプリケーションに潜り込ませていることが多いそうですけれども、このアプリケーションをインストールするかどうか、まさに利用者個人の自己判断に任されているので、利用者の安全な使用とアプリの普及にとっては非常に大きな脅威となっておるわけであります。

今般の刑法等の改正により、こうしたウイルス拡散の犯罪行為を検挙するということは私は非常に大賛成でありますが、他方で、権力の濫用が一部で危惧されておりますし、こうしたことで、あるいは解釈があいまいな部分があるということもあって、さらに、捜査における裁量の余地が大きいことから、本来悪意のあるウイルスを作成、開発などしていないような一般の罪なきインターネット事業者、ソフトウエア開発者等が取り締まりの対象になる、そういう懸念が多く出ているわけでございます。

そこで、本案採決に当たり、こういった懸念を払拭し、今後、我が国の戦略産業であるインターネット事業者やソフトウエア開発者、そして総じてＩＴ産業に安心して事業に取り組んでもらうことが私は必要であると思います。そういった観点から、改めて、今回二度目ですけれども、大臣にこの問題について質問させていただきたいと思います。

まず、そもそも論として、不正指令電磁的記録という表現、あるいは条文の「意図に沿うべき動作」とか「意図に反する動作」という定義が非常にあいまいであって、私は前回大臣に、コンピューターウイルスという表現をしたらいいんじゃないかという話をしました。また、その対象となるもの、例えばアンチウイルスソフトは対象にならないというふうにお伺いしましたけれども、そこら辺の具体的なものが非常にあいまいもことしているんですが、この点について、大臣の御見解をお聞きしたいと思います。

○江田国務大臣　刑法関係の言葉の定義というものは、罪刑法定主義といった見地からも厳密に使われなければいけないというのは委員御指摘のとおりでございますが、さはさりながら、言葉だけで、内包、外延、一義的に明確だというのがなかなか困難なことはまた事実でございます。

しかし、可能な限りこれは明確にするようにし、さらに運用においての周知徹底を図るであるとか、あるいはさまざまな解説書等によっていろいろな周知をしていくとか、あるいは運用の中で疑問が生じた場合には、直ちにこれを裁判実務においても、あるいは法の改正などにおいても改めていくとか、そうしたことを繰り返しながらよりいいものに仕上げていかなきゃいけないということであって、今回、不正指令電磁的記録、これは、今委員おっしゃいましたような文言で定義をしているわけでございまして、この定義自体が、通常の判断能力を有する一般人に十分理解し得ないものにはなっていない、これでとりあえずスタートをしていきたいと思っております。

○城内委員　私は一般人には理解できないというふうに考えておりますけれども、そもそも、その定義のあいまいさが恣意的な運用を生むということもありますので、その点については十分注意していただきたいというふうに思います。

次の質問に移りますが、先ほど、たしか大口委員の質問に対する大臣の答弁ですが、通信履歴の保全についてかかったコストは、過度の負担にならないように配慮するが、通信事業者に負担していただきますと。たしか私はそういうふうにお伺いしました。

しかし、そうなりますと、小さな事業者にとっては、これは予算のかかる話でありますし、いろいろと手間暇かかって非常に業務が滞ってしまうんじゃないかと思うんです。この点について、やはりもうちょっと、負担にならないように配慮するが通信事業者に負担をしていただくというんじゃなくて、将来は負担も考えるという前向きな答弁を私はぜひしていただきたいんですが、どうでしょうか。

○江田国務大臣　これは、今私どもの考えているところですと、新たに記録して保存することを求めるのではなくて、消去しないように求めるだけで、しかも、期間の限定もありますし、必要な範囲内での要請といった限定もありますし、過度の負担にはならないと思っておりますが、もちろん負担ができる限り小さくなるように、事案に応じた配慮もしていくことを周知させたいと思いますし、また、現にこんな負担があったというようなことがございましたら、そういう場合にこれをまた検討していくという余地は当然あろうかと思います。

○城内委員　今大臣から、検討する余地があるという、やや前向きな御答弁をいただきましたので、実際運用してみて、いろいろ支障が出てきた場合には、ぜひ前向きに検討していただきたいというふうに思います。

次に、同じく通信履歴の保全要請あるいは差し押さえについてなんですが、通信履歴の定義なんですけれども、送信元であるとか送信先、通信日時ということもあると思うんですが、済みません、これはちょっと質問通告していませんでしたけれども、件名もそれに入るかどうかということが、先ほど参考人質疑で議論があったんです。

私は、もし例えば件名が入るとしたら、これは通信内容と密接不可分である場合が多々あるんですね。例えば、私が作成したウイルスについてという件名であれば、もうその中身がほとんど件名にあらわれているわけですから、どこで線を引くかというようなことをやはり厳密にやらないと、通信の内容に踏み込んでしまうんじゃないかと思うんですが、件名の扱いについてはどのようにお考えでしょうか。

○江田国務大臣　件名は、これは電子メールを送信する者が用いるメールソフトによって作成、記録されて送信されるものでございまして、通信事業者等が業務上記録している通信履歴には当たらない。したがって、単に御連絡というものであれ、あるいはウイルスをつくったのでお知らせというものであれ、その内容がどのようなものであれ、これは通信履歴には該当しないと考えております。

○城内委員　該当しないという考えでよろしいわけですね。わかりました。

次の質問に移りますけれども、何度も、先ほど大口委員、辻委員からも御指摘あったと思います

が、バグとウイルスの違いでございますけれども、大臣は先ほど、バグについては、重大な影響を及ぼす場合は、そしてあと、故意性がある場合は認められるというような話をされましたが、私は、バグとウイルスというのはやはりきちんと区別してやった方がいいんじゃないかなというふうに思っております。

と申しますのは、やはり、何度もこの委員会でも指摘があったように、よかれと思ってフリーのソフトウエアを提供して、それによって生じたいろいろな問題というのはありますけれども、重大な影響という、それ自体が非常に私はあいまいだと思っているので、悪意がなければ、いろいろなプログラム上のミスで多少支障が生じたとしても、これはいわゆる未必の故意も成立しないし、提供罪も成立しないということで一線を画すべきではないかと思うんですが、この点について、大臣、どうお考えでしょうか。

○江田国務大臣　これは、バグというものが通常はプログラム作成に付随して起きるものだと。したがって、コンピューターをいろいろいじっていると、とりわけフリーソフトウエアなんかの場合にはそういうものもあるものだということは、皆お互い了解済みでやっていることでございまして、そうしたものがコンピューターウイルスに当たるというようなことは、これはあり得ないと思っております。

ただ、一部に、もし仮に、そのバグというものが電子計算機の機能を麻痺させる、あるいはその作動が容易に回復しないような状態に至らしめるという重要なものであって、そのことを十分知りながら、故意犯としてそうしたものがついているソフトを提供するというようなことになりますと、これはちょっと見逃せないということも起こり得るという意味で、可能性があるということを申し上げただけでございまして、一般のコンピューターの利用者の皆さんが、そうしたことに特に意識をせずに、バグがあっても、もちろんバグをなくするような努力は当然いろいろやっていかなきゃならぬと思いますが、あってもコンピューターを大いに活用していただくことは何ら支障がないと思っております。

○城内委員　しかし、重大な障害を生じるということを十分知りながらとか、悪意を持ってと、これはなかなか証明するのは難しいので、おまえは悪意を持ってやったんだろうと言われちゃうと、それを否定してもそうなってしまう可能性もあるわけですから、そこら辺は本当に、運用上十分気をつけていただきたいなというふうに思います。

もう時間も余りないので終わりますが、最後に一つだけ、人権侵害救済機関の問題について質問させていただきたいと思います。

大臣は、五月十七日のこの委員会で、私の質問に対して、人権侵害救済機関の設置について、「どの程度の財政措置が必要かというのは、まだ言える段階には至っていない」という答弁をされました。ということは、まだ言える段階には至っていないということですが、いつになったら言える段階になるんでしょうか。

○江田国務大臣　これは本当にまだ言える段階に至っていないので、国の機関としてつくるのもどの程度のものにするのか、あるいは地方にまでそうしたものを手を広げるような機関にするのかどうかなど、今検討中でございまして、そうしたことが決まっていかないと、予算のこと、経費のことなどは全く決まらないんです。

この検討はいつごろまでにやるかということを言わなければ、いつごろになったら経費がどのくらいかということに答えをすることはできないんですが、それは、私ども、なるべく適切な時期にぜひ導入をしたいと思っておりますが、まだいつの段階というところまで言えるほど検討が煮詰まってきているわけではございません。

○城内委員　しかし、これはどれだけ財政的措置がかかるのかというのがわからないと判断のしようがないし、実際にどれだけその効果があるのかとか、私は基本的に反対の立場で、個別法をつくって、人権擁護局がしっかりと、日本全国にいらっしゃる人権擁護委員の方々と……（発言する者あり）

○奥田委員長　御静粛に。

○城内委員　連携をすればいいと思っていますが、いずれにしてもここははっきりさせていただきたいと思いますので、時間がないので私はここで質問を終わりますが、また次回質問させていただきます。

以上です。ありがとうございました。

○奥田委員長　これにて本案に対する質疑は終局いたしました。

○奥田委員長　これより討論に入るのでありますが、その申し出がありませんので、直ちに採決に入ります。

内閣提出、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案について採決いたします。

本案に賛成の諸君の起立を求めます。

〔賛成者起立〕

○奥田委員長　起立総員。よって、本案は原案のとおり可決すべきものと決しました。

お諮りいたします。

ただいま議決いたしました法律案に関する委員会報告書の作成につきましては、委員長に御一任願いたいと存じますが、御異議ありませんか。

〔「異議なし」と呼ぶ者あり〕

○奥田委員長　御異議なしと認めます。よって、そのように決しました。

〔報告書は附録に掲載〕

○奥田委員長　次回は、公報をもってお知らせすることとし、本日は、これにて散会いたします。

午前十一時四十八分散会

平成二十三年六月七日印刷
平成二十三年六月八日発行
衆議院事務局
印刷者　国立印刷局