第百四十五回国会

参議院法務委員会会議録第二十二号

平成十一年七月二十七日（火曜日）

午前十時開会

委員の異動

七月二十二日

辞任　補欠選任

佐々木知子君　井上　裕君

七月二十三日

辞任　補欠選任

亀井　郁夫君　有馬　朗人君

七月二十六日

辞任　補欠選任

有馬　朗人君　斉藤　滋宣君

井上　裕君　脇　雅史君

角田　義一君　内藤　正光君

出席者は左のとおり。

委員長　荒木　清寛君

理事　鈴木　正孝君

服部三男雄君

円　より子君

大森　礼子君

平野　貞夫君

委員　阿部　正俊君

斉藤　滋宣君

世耕　弘成君

竹山　裕君

仲道　俊哉君

脇　雅史君

海野　徹君

小川　敏夫君

千葉　景子君

内藤　正光君

橋本　敦君

福島　瑞穂君

中村　敦夫君

事務局側

常任委員会専門員　吉岡　恒男君

参考人

株式会社東京デジタルホン専務取締役技術本部長　桑折恭一郎君

東日本電信電話株式会社常務取締役技術部長　森下　俊三君

東京インターネット株式会社上級顧問　髙橋　徹君

ニフティ株式会社取締役サービス企画統括部長代理　本名　信雄君

本日の会議に付した案件

○参考人の出席要求に関する件

○組織的な犯罪の処罰及び犯罪収益の規制等に関する法律案（第百四十二回国会内閣提出、第百四十五回国会衆議院送付）

○犯罪捜査のための通信傍受に関する法律案（第百四十二回国会内閣提出、第百四十五回国会衆議院送付）

○刑事訴訟法の一部を改正する法律案（第百四十二回国会内閣提出、第百四十五回国会衆議院送付）

○委員長（荒木清寛君）　ただいまから法務委員会を開会いたします。

まず、委員の異動について御報告いたします。

去る二十二日、佐々木知子君が委員を辞任され、その補欠として井上裕君が選任されました。

また、去る二十三日、亀井郁夫君が委員を辞任され、その補欠として有馬朗人君が選任されました。

また、昨二十六日、有馬朗人君、井上裕君及び角田義一君が委員を辞任され、その補欠として斉藤滋宣君、脇雅史君及び内藤正光君が選任されました。

○委員長（荒木清寛君）　参考人の出席要求に関する件についてお諮りいたします。

組織的な犯罪の処罰及び犯罪収益の規制等に関する法律案、犯罪捜査のための通信傍受に関する法律案及び刑事訴訟法の一部を改正する法律案の審査のため、本日の委員会に参考人として株式会社東京デジタルホン専務取締役技術本部長桑折恭一郎君、東日本電信電話株式会社常務取締役技術部長森下俊三君、東京インターネット株式会社上級顧問髙橋徹君及びニフティ株式会社取締役サービス企画統括部長代理本名信雄君の出席を求め、その意見を聴取することにいたしたいと存じますが、御異議ございませんか。

〔「異議なし」と呼ぶ者あり〕

○委員長（荒木清寛君）　御異議ないと認め、さよう決定いたします。

○委員長（荒木清寛君）　組織的な犯罪の処罰及び犯罪収益の規制等に関する法律案、犯罪捜査のための通信傍受に関する法律案及び刑事訴訟法の一部を改正する法律案を議題といたします。

本日は、三案の審査のため、お手元に配付の名簿のとおり、四名の参考人から御意見を伺います。

まず、午前中御出席をいただいております参考人は、株式会社東京デジタルホン専務取締役技術本部長桑折恭一郎君及び東日本電信電話株式会社常務取締役技術部長森下俊三君でございます。

この際、両参考人に一言ごあいさつを申し上げます。

本日は、御多用のところ当委員会に御出席をいただきまして、まことにありがとうございます。

両参考人から忌憚のない御意見をお聞かせいただきまして、今後の審査の参考にいたしたいと存じますので、どうぞよろしくお願い申し上げます。

議事の進め方でございますが、まず桑折参考人、森下参考人の順にお一人二十分程度ずつ御意見をお述べいただきまして、その後、各委員からの質疑にお答えいただきたいと存じます。

なお、念のため申し添えますが、御発言の際は、その都度、委員長の許可を得ることとなっております。また、各委員の質疑時間が限られておりますので、御答弁は簡潔にお願いいたしたいと存じます。

なお、参考人の意見陳述、各委員からの質疑並びにこれに対する答弁とも着席のままで結構でございます。

それでは、桑折参考人からお願いいたします。桑折参考人。

○参考人（桑折恭一郎君）　東京デジタルホンの桑折でございます。よろしくお願いいたします。

それでは、お手元に「ＰＤＣ携帯電話の概要」という資料があるかと思いますが、その資料に沿って説明をさせていただきます。

御承知のとおり、携帯電話というのは世界的には幾つかの方式がございますが、ＰＤＣというのはその中で主としてドコモさんが中心として開発されました日本独自の方式でございます。日本の特徴を生かしておりまして、周波数の使用効率が非常にいいというところが特徴になってございます。それの概要を説明させていただきます。

まず第一ページでございますが、システム構成といたしましては、ここの図に書いてございますように、各基地局というのを都心でいきますと主としてビルの屋上等に設置しておりますが、郊外に行きますと、鉄塔を建ててそこに基地局がございます。それを伝送集約局というところまで有線でつなぎまして、あと私どものネットワークセンターというところまで結ばれております。こちらのネットワークセンターの中に、後ほど説明させていただきます交換機なりその他各システム等が入ってございます。

それでは、二ページ目をごらんいただきたいと思います。

ネットワーク構成でございますけれども、下の方から説明させていただきますと、移動機、これがいわゆる携帯電話と言われている電話機でございます。それからあと、基地局がありまして、基地局から先が有線で持ちまして、その上に書いてあります移動体用交換機という交換機につながれております。移動体用交換機と基地局の間は光ファイバーその他で結ばれております。

それから、その上にゲートウェイ交換機というのがございますが、直接そのゲートウェイ交換機には基地局は接続されておりませんで、ＮＴＴさんなりそれから他の携帯電話事業者さんとの間をＰＯＩという事業者間の接続点を経由いたしまして接続をしております。

あと、その右側にホームロケーションレジスタというのがございますが、これは各移動機の、東京デジタルホンでいきますと東京デジタルホンに加入されているすべてのお客様に対する電話機の情報が入っておる。特に、一番その情報の中でも重要なのが今各電話機がどの場所にいるのかということを特定するための情報等か入ってございます。

あと、その上に留守番電話センターというのがございますが、これは今東京デジタルホンの場合ですと、加入していただいたお客様につきましては、基本的にはすべて無料で、かけた相手の移動機につながらない場合に留守番電話にお客様のメッセージを入れるというサービスをしておりますが、そういったシステムでございます。

それからあと、最近、私どもは商品名でスカイウォーカーという名前で言っておりますが、いわゆるデータ系のメールサービス、それをとり行いますための文字通信センターというようなシステムでございますが、そういったものを持っております。

それから、三ページ目をごらんいただきたいと思います。

いわゆる移動体通信というのは、セルラーという会社名がございますけれども、この方式そのものかセルラー方式という名前で、これは総称の名前で言っております。ここの三ページ目の一番下に六角形の図が幾つか書いてあるかと思います。それで、こちらの基地局一つについて、私どもの会社でいきますと六角形の単位というもの三つを持つことを基本としております。この一つをセルという名前で呼んでおります。このセル単位にある数だけお客様が同時に通話できるというための無線機を持っております。

事業者さんによりましては、これが一つの基地局で三つではなくて六つのセルを持つという方式を使われているケースもございます。基本的に考え方としては同じものでございます。

それで、私どものＴＤＰの例でいきますと、これらの移動体通信を行うために十メガヘルツという帯域の電波を私どもは使わせていただいていまして、全部で三百九十八種類の周波数を使うことができます。この周波数一つ一つに無線機が一つつきまして、私どものシステムでは一つのセルに最大十五の無線機を積むことが可能になっております。すなわち、十五の周波数を使って十五の無線機を使うことができます。それで、一つの無線機では時分割多重といいまして、一つの無線機ではフルレートという音質のいい、伝送方式でいきますと三つの音声を同時に接続することが可能になります。それから、ハーフレートというのはその倍の容量を持っておりまして、音質は多少落ちますが、一つの無線装置で六チャンネルつくることが可能です。ですから、最大のセルの大きさでいきますと十五掛ける三の四十五チャンネルということになりますが、そのうちの最低一チャンネルは制御用として使いますので、一つのセルで同時に話ができるお客様の数というのは四十四人までが最高の場合でございます。郊外等に行きますとフル実装しておりませんので当然これより下がりますが、セルの最大のキャパシティーとしては四十四チャンネルというふうになってございます。

それでは、四ページ目をお願いしたいと思います。

移動体と固定電話の一番の違いは何かということでございますが、移動体の場合は一台一台の電話機というのが電話番号を持ってございますけれども、これは絶えずお客様が電話機を持って移動されるわけです。ですから、固定電話ですと、交換機から回線が出ておりますが、その先につながっている電話機というのは全部固定的につながれておりまして、交換機は交換機側の出回線の番号でもってその先につながれている電話番号というものをつかむことができるわけです。

ただ、移動体の場合ですと、交換機から出ておる出回線というのは、どの基地局のどのセルの何番目の無線機の、先ほど申し上げましたように、一台の無線機で三チャンネルあったとしますと何チャンネル目かと、それについては全部固定的にそこまでは線がつながれております。その先、どのお客様がそのチャンネルを使うかというのはその都度変わってきておりまして、固定的に電話番号と交換機の間の対応というのができないわけで、実際に通話する場合には電話機と交換機から出て最後に無線装置の出口のところに行く回線までを結びつけるという作業が必要になります。

その結びつける仕事のためにどういうことをやるかというと、まず位置の登録という仕事がございます。電話機を持って移動しますと、位置登録エリア、これは一般的に複数のセル、十とか二十とかというセルをまとめて一つの位置登録エリアとしておりますが、そこの中で今どこの位置登録エリアにいるのかということを各端末は中央側に登録するという作業が入ります。この図でいきますと、左側の位置登録エリアにいました移動機Ａが位置登録エリアのＡ'という方に移った場合には、そのタイミングで交換機に向かって位置登録要求というものをしまして、その位置登録要求の結果が先ほど申し上げましたホームロケーションレジスタというところに位置登録エリアのエリア番号というもので登録されます。これによって複数のセルのあるグループの中のどこに今この電話機がいるのかということをネットワークとして把握することができるわけです。これが一番最初に接続のためにやる仕事でございます。

それから、五ページ目をごらんいただきたいと思います。

電話機を持って移動した場合にどういうことが起きるかということでございますが、あるセルから隣のセルに移ってまいりますと、もとのセルの電波が距離が離れるに従ってだんだんと弱くなってまいります。逆に、隣のセルに近づいていくと隣のセルの電波がだんだん強くなっていく。それがある一定の差になりますと、電波の強い新しいセルにチャンネルを切りかえるという仕事が必要となってまいります。それが、ここに書いてありますように、ある左側のセルから右側の方のセルに移動した場合のチャンネルの切りかえという事柄でございます。これが起きた場合には、先ほど言いましたように、ホームロケーションレジスタに新しいエリアに移動したという情報が更新されるわけでございます。これは、俗にセルの間を移動する言葉としてハンドオーバーという用語を使っております。

それから、六ページ目の説明をさせていただきます。

まず、先ほど申し上げましたように、移動機というものが大体どこにいるのかということは、位

置登録要求ということでホームロケーションレジスタというところに登録されているわけですけれども、左側のAという端末からBという端末に通話をしようといったときにどういう制御の流れになるかというのがこの六ページ目の図でございます。これにつきましては、Aの端末は発信する側、それからBの端末はAの端末から呼ばれる受信側ということでございまして、発信側の制御と受信側の制御が若干違いますので、それぞれについて説明をさせていただきます。

発信側の方が一般的にはコントロールとしては簡単でございまして、端末から相手番号をセットしまして発信ボタンを押しますと、その端末から基地局に対して発信要求がなされるわけでございます。そうしますと、基地局はセルの中のあいているチャンネルというものを探しまして、それとAの端末機を結びつけます。それによって、基地局の何番目の無線機の何チャンネルの通話チャンネルがこの無線機で使われたのかということが初めて対応づけができまして、その情報は左側の移動機用交換機ーというところにも情報が通報されまして、このとき初めてこの交換機からの出線に対して〇九〇の何番という端末がつながっているということを移動機用交換機ーでつかむことが可能になっております。

それで、接続の問題でございますが、下の枠の①に「Aの認証」という言葉が書いてございます。これはどういうことかと申しますと、移動機の〇九〇の番号というのが仮に解約されたといった場合には、基本的に私どもは最低六カ月間の期間をもって同じ番号を再度使うということになります。そうしますと、また同じ番号が使えてしまうわけですけれども、もしそのときに前のお客様が持っていた端末で同じ番号だったといったときに使えてしまうと請求がおかしなことになってしまう。それから、もっと言いますと、クローン端末という同じ番号を持った端末をだれかがつくってしまうと、〇九〇の何番といいますともうほとんど番号はいっぱいになっていますので、大体どこかの番号に当たることができる。

そういうことができますと非常に不正のもとになりますので、新しいお客様に端末をお渡しするに当たりましては、電話機の番号とともに認証の番号というものを端末機とホームロケーションレジスタの両方にセットしておきます。ですから、接続の段階で、端末の電話番号だけでなくて認証番号も一致したときに初めてその電話機か使える状態になります。ですから、先ほども言いましたように、仮に六カ月前に持っていた同じ番号があった場合には、その認証番号が違いますのでその端末から発信しても接続はできない、不正の状態にはならないということでございます。これが発側の接続の問題でございます。

着側はどうかといいますと、先ほど申しましたように、Bの端末というのはあらかじめ位置登録というものをホームロケーションレジスタなり交換機の2というのに登録かされております。それで、Aの端末から着側の電話番号をホームロケーションレジスタに聞きに行きますと、これがどの交換機のどのロケーションエリアの中にあるのかということがわかりまして、該当する交換機に対して接続の要求を出します。それから後、基地局は複数のあるグループングされたセルに対して、この着側の番号かいたら応答しろという命令を一斉に出します。

違った電話機でもそれを受けますが、それは自分の番号と違うということがわかりますから、その電話番号は無視しますけれども、たまたま呼ばれた電話機だけがこれは自分の番号だということがわかりまして、基地局に対して今呼ばれた番号は自分の番号だという形の信号を返します。それを基地局から交換機の2の方に返しまして、それによって初めて電話機のAとBというものが接続されるという形になります。これが接続の概要でございます。

あと、最後の三枚は接続の問題ではなくて、音声というものがどういうふうに運ばれるのかということでございます。

一般的に、これは固定電話でもそうなんですが、電話というのは三・四キロヘルツという幅までのアナログ信号で行きますと人間の声を明瞭に聞くことができるということで、固定電話も全部これだけの帯域のアナログの信号をやりとりしているわけです。それをデジタル化する場合は、一応四キロという幅でもちまして、一秒間に六十四キロビットという信号に変換します。一般的な交換機は全部六十四キロビットで回線の交換をやるということでございます。

ところが、移動体通信の場合、その六十四キロビットで端末とやりとりをしようとしますと、音質的には非常にいいんですが、無線の波を非常にいっぱい使わないといけないということで、そのために六十四キロビットを聞き取れる範囲内で圧縮という形の処理をかけます。現在、PDCの場合ですとフルレートで六・七キロビット・パー・セカンドという形まで圧縮をかけます。それから、ハーフレートで行きますと三・四五キロビット・パー・セカンドに圧縮をかけます。それによって電波を非常に有効に利用しようということでございます。

この端末の中には、ですから、きょう時点でいきますと、フルレートの圧縮変換のソフトとハーフレートの圧縮変換のソフトの二つが入っております。移動機から交換機のところまではその信号でフルレートもしくはハーフレートで行きまして、これが例えばNTTさんの固定網なんかと接続する場合には、そこで六十四キロビットに変換する、それを、左方にコーディック変換と言いてありますが、それによって六十四キロビットに直してNTTさんの方に接続するという方式をとってございます。

それから、八ページ目でございますが、これは移動体事業者をまたがる場合でございますが、この場合は二つケースがございまして、先ほど言いましたように、例えばフルレートなりハーフレートなりがどちらも同じチャンネルをつかんだ場合には、この左側の音声圧縮方式Aという形でその信号を六十四キロビットに途中で直さずに、そのまま相手側の端末にまで六・七キロビットなり三・四五キロビットで移動機のところまで届けて、その移動機側で音声に変換するという方式をとります。これが圧縮方式が同じ場合でございます。

それから九ページ目の場合は、例えば片側がフルレートのチャンネルをつかんだ、それから片側がハーフレートのチャンネルをつかんだといった場合には、そのままで相手側の端末に届けることができませんので、左側の音声圧縮方式Aというのが仮にフルレートといたしますと、相手側はこれはフルレートの圧縮をしていないなということかわかりますと、移動体通信事業者Aのところで六十四キロビットという基本的なデジタル信号に一たん戻しまして、それからさらに移動体通信事業者C側の交換機で今度はハーフレートだということで三・四五キロビットにまた再度変換して移動機の方にハーフレートで出していくというような方式になります。

これらはいろいろな組み合わせがございますし、これはちょっと静的に書きましたけれども、先ほど言いましたように、移動機を持って移動した場合に、今までフルレートでつかめた場合は、隣のセルに行った途端にフルレートではなくてハーフレートしかなかったといった場合には、途中からフルレートからハーフレートに変えるというようなケースもございます。

いずれにしても、こういうことで発側から着側までの接続ということができますし、特に音声方式の圧縮というものは、これはフルレート、ハーフレートについては日本の場合、PDCでは全部統一されておりますので方式は同じでございますか、基地局から移動機の間につきましては圧縮した信号をさらにスクランブルという形で一般の人に盗聴が簡単にできないようなランダマイズをして送っておりますので、デジタルの場合は非常に盗聴等について信頼性が高いというところがここにあるわけでございます。

以上、ＰＤＣの原理というのを簡単に説明させていただきました。

○委員長（荒木清寛君）　ありがとうございました。

次に、森下参考人にお願いいたします。森下参考人。

○参考人（森下俊三君）　ただいま御紹介いただきました東日本電信電話株式会社の森下でございます。

本日は、通信傍受法案が成立した場合に通信傍受を行うことが可能なのはどこか、技術的にどういったところが可能なのかということを中心に御説明させていただきたいと思います。座って御説明いたします。

御承知のとおり、弊社ではいわゆる固定電話サービスを御提供いたしておりまして、そのためにさまざまな電気通信設備を設置しております。弊社の電気通信設備のうちで通信傍受を行うことが可能な場所、これは何カ所かに限定されますので、その部分につきまして技術的な側面から御説明を申し上げたいというふうに思っております。

お手元にあらかじめ「電話回線における通信傍受について」という一枚紙の資料をお配りしてございます。この資料は上段と下段に分かれておりますが、上段がアナログ回線、これは電気通信サービスのうちで従来の一般の電話サービスというものでありますが、資料上はアナログ回線と表現いたしております。下段は総合デジタル通信サービス、私どもがＩＳＤＮと称しているものでありますが、資料上はデジタル回線と表現いたしております。

この資料では、説明上、一般的な設備の形で表現してありますので、実際はお客様の建物の状況、一戸建て、マンションあるいはオフィスビル等によって若干形態が異なっております。ただ、原理的にはすべて同じでございますので、代表的なケースで御説明させていただくということをあらかじめ御承知おき願いたいというふうに思います。

まず、設備の状況でございますが、お客様宅のところに電話機がございまして、それから引き込み柱と書いてありますところ、これがＮＴＴのケーブルに接続する引き込み線と言われているものであります。引き込み柱から、電柱の絵がかいてありますが、これは架空のケーブルでありまして、それを経由いたしまして地下の太いケーブルの方へ接続されていく。最終的にはＮＴＴのビルのところで地下のケーブルがビルの中で立ち上がりまして、主配線盤というところでケーブルが全部終端される。ここは端子板がありまして、全部一本一本のケーブルがここで接続されるわけであります。片一方、ＮＴＴビルの中には交換機というのが設置してありますが、交換機の方から交換機の回線が同じようにこの主配線盤のところに全部終端されまして、ここを接続することによりまして電話機が交換機に接続されるということでございます。交換機から右側のところはＮＴＴ中継網とありますが、中継伝送路を経由いたしまして中継交換機に接続されていく、あるいは他事業者へと書いてありますところは、ここにＰＯＩ、他の事業者との接続場所、ポイント・オブ・インターフェースと言っておりますが、ＰＯＩを経由いたしまして他の電気通信事業者のネットワークにつながっていく、移動体ネットワーク等へつながるという形でございます。

それでは、まず初めに資料上段のアナログ回線の部分について御説明を申し上げます。

一つ目は、資料上で①の引き込み柱と書いたところであります。この引き込み柱と申しますのは、先ほど御説明いたしましたケーブルとお客様の家にあります電話機をつなぐところに設置してある電柱でございまして、引き込み線は二本の導線でもって接続されておるわけでありますが、引き込み柱のところにはケーブルと申しまして、平均的には百台の電話が接続されるケーブル、ですからこれは二百本の電線、導線が束になっておるわけでありますが、そういったものと接続する場所であります。

ここのところに黒く四角の記号がつけてありますが、これは端子函と申しております。これは何かと申しますと、先ほど御説明いたしましたように、このケーブルの方は二百本あるいは四百本という電線がずっと延びてきておりますので、その中からお客様のところへつなぐというために端子板で接続するようにしておりまして、その端子板を入れる函でございます。電柱の上に長方形の黒い函があるのをよくごらんになると思いますが、その部分でございます。

通信傍受を行う方法といたしましては、この端子函の中の通信傍受の対象となる回線の端子、これにクリップなどを用いまして物理的に捕捉するという方法がございます。しかしながら、この引き込み柱というのは一般的には道路の上にあったり、あるいはお客様の敷地内に設置されているということでございますので、そういったことを考慮いたしますと、本法案にございます通信傍受を行う箇所としてふさわしいかどうかという面では疑問であると考えております。

それから、先ほどの引き込み柱から電話ケーブルと書いてある部分、主配線盤までの部分につきましては、たくさんの電線が一本のケーブルにまとめてありますので、基本的には通信傍受を行うためにその当該の回線に割り込むということは極めて困難であるというように考えております。

二つ目の場所は、この図の②の主配線盤、ＭＤＦと記載してある部分でございます。このＭＤＦと書いてあります部分は、先ほど御説明いたしましたように、お客様のところからのケーブルが全部集まってまいりますので、普通の局ですとここに何万本あるいは何十万本の電話線が全部立ち上がってまいりまして、それが端子板で全部終端をいたします。一本一本の導線が全部そこに接続されるということでございます。そういったことで、この主配線盤におきましては一対一で電話と対応しておりますので、通信傍受の対象となる回線の端子を物理的に捕捉して通信傍受を行うことは可能でございます。後ほど御説明いたします

が、アナログ回線を対象とした通信傍受はこの②の主配線盤で行うのが妥当ではないかというふうに私どもは考えております。

三番目は、資料上の③、試験制御装置と記載してある箇所についてでございます。試験制御装置と申しますのは、電話を利用していただいておりますお客様から、利用している回線のぐあいがよくない、ダイヤルをしてもうまくつながらないとか、故障しているんではないか、そういったことでお申し出をいただいた場合に、故障調べということを行います。あるいはお客様から電話設置の御要望をいただいた場合に、その設置の工事を行った後で、ちゃんとその電話がきちんと使えるかどうかを試験するための装置でございます。

故障調べといいますのは、通常、お客様が故障のときには一一三番をダイヤルしていただきますと私どもの試験センターの方に接続されまして、そこでお客様の電話機が故障しているのか、電話機からＮＴＴのビルに入ってきている途中のケーブルのところで故障が起こっているのか、あるいはケーブルではなくてＮＴＴビルの中の交換機等が故障しているのか、それを切り分けることでありまして、そういった試験機能を持っているものがこの試験制御装置というものでございます。

資料上ではパソコンの図柄でかいてございますが、試験制御装置そのものは実は交換機と同じような装置になっておりまして、試験制御装置を操作するための端末がこのディスプレーのような絵でかいてあるということでございますので、そういうふうに御理解いただければ結構です。ちなみに、下段のデジタル回線のところの試験制御装置につきましても同じような装置のつくり方になってございます。

それでは、この試験制御装置を用いて通信傍受を行うことができるかどうかということの御説明をいたしますと、私どもでは、先ほど申しましたように、故障調べの場合に行う試験の方法として、これは幾つかの方法があるわけでありますが、お客様が一一三にお電話をしていただきまし

て、そこでその通話の状態がいいかどうかというのを見ないといけませんので、そういった意味で通話状態をモニターすることができるようになっています。

それはどうやってやるかといいますと、この端末装置から該当の回線に番号をダイヤルして割り込みますと、その状態でお客様の通話をモニターするということができるわけであります。もちろんこれは一一三をかけてきたときに試験いたしますが、一般にお客様が電話をしていただいているときに割り込むこともできるということでございます。

この方法をとって通話のモニターを行っておりますと、これは試験を行うことが目的でございますので、お客様が外部に電話をおかけになる、電話発信するということが可能になっております。そういう発信状態で試験をしないといけませんので、外部へ発信することが可能でございますが、その状態では逆に今度は当該回線にほかの方、第三者の方が電話をかけてきた場合にはこれは待ち受け状態ということですが、接続することができない仕組みになっております。これはもともと試験機能ということでそういうふうになっておりますので、あらかじめその回線に割り込んでおりますと、その回線には着信ができないということでございます。そういったことで、この資料の上の方に吹き出しで、「通話中に割込むことは可能。待ち受けは不可能」と書いてあるのはそういうことでございます。

したがいまして、参考までに申し上げますと、本法案にございます通信傍受を行うためにこの試験制御装置を利用するということは現実的ではないというふうに考えております。

次に、資料下段のデジタル回線の場合について御説明申し上げます。

まず、既に御案内のとおりでございますが、アナログ回線とデジタル回線では回線の中を流れる信号が全く異なっております。具体的に申し上げますと、デジタル回線の場合には、ＮＴＴの交換機のところからお客様宅内に設置してありますＤＳＵ、これは下に訳語が書いてありますが、デジタル回線終端装置というものでございますが、この間はすべてデジタル信号になっております。このため、この①の引き込み柱あるいは②の主配線盤といったところで通話のモニターを行いましても、アナログ回線のように音声として認識することはできません。デジタル信号ですので、傍受をしても一般にはブーンといった雑音のような音しか聞こえないということでございます。

したがいまして、資料下段の①の引き込み柱あるいは②の主配線盤と記載してある箇所で通信傍受を行うということは通常できないと考えております。

次に、③の試験制御装置というところでございますが、デジタル回線用の試験制御装置につきましては、デジタル信号を試験するということから、お客様が通話しているときに当該回線に割り込んで通話のモニターを行うことが可能であります。これはアナログと同じでございますが、さらに通話のモニターを行うために対象回線を捕捉している、あらかじめその回線を捕捉している状態でお客様が外部に発信することも可能でございますし、それから着信も可能になります。

アナログ回線の場合ですと、あらかじめ捕捉していると着信が不可能だという御説明をいたしましたが、デジタル回線の場合にはデジタル信号というのが、上り信号、あるいは下り信号といいますか受ける信号、こういった両方のデジタル信号を試験しないといけない。データが誤っているかどうかをチェックするということが必要になりますので、通話に影響しないようモニターしているため、発信、着信とも可能な形になっております。そういったことで、この資料上では吹き出しか書いてありますが、「通信中に割込むことは可能。待ち受けは可能」、こう書いてあるのはそういう意味でございます。

このようなことから、御参考までに申し上げますと、デジタル回線の通信傍受を行おうとする際にはこの試験制御装置を利用することが現実的であるというように考えております。

以上、アナログ回線とデジタル回線、それぞれにつきまして技術的側面から御説明申し上げました。これら以外に交換機など各種の電気通信設備がありますが、それにつきましてはすべてデジタル化されておりますので、個々の回線ごとに通信傍受を行うということは実質的に不可能であるということを申し添えさせていただきたいというように思います。

御説明は以上です。

どうもありがとうございました。

○委員長（荒木清寛君）　ありがとうございました。

以上で参考人の意見陳述は終わりました。

これより参考人に対する質疑を行います。

質疑のある方は順次御発言願います。

○世耕弘成君　自由民主党の世耕弘成でございます。

御指示でございますので、座ったまま発言をさせていただきます。

本日は、両参考人、本当に御多忙のところお運びをいただきまして、ありがとうございました。

前回、実は私はこの委員会で質疑に立ちまして、電話のネットワークですとかあるいはインターネットのネットワークの図を示しながら技術的な検証をこの委員会の中で行わせていただいて、そして技術的には傍受できる場所が相当限定されているんだということを明らかにさせていただきました。また、法務省の側も、当然技術的にできないところはもちろんのこと、法律的にも、通信傍受法の考え方の上でも、個人の電話番号やメールアドレスか特定されない限りは傍受を行わないということを言明された。これが私の前回の質疑のやりとりでございました。

そういうことから、技術的あるいは通信傍受法上的に傍受というものは極めて限定的に行われるということを私は前回の質疑で相当明快に整理したつもりであります。また、本日のＮＴＴ東日本の森下参考人の陳述によっても私の整理は間違っていなかったんだなということが明らかになったのではないかというふうに思っております。

また、桑折参考人の意見を聞かせていただきますと、携帯電話、特にデジタル化されている携帯電話の仕組みの複雑さというのが私はよく理解できました。これは後で質問をしていきたいと思いますけれども、傍受ができる範囲、これも移動体の場合も相当限られているんではないかなという感触を今持たせていただきました。

さて、先日の私の質疑をいろいろ技術の専門家の方ですとか地元のこういう問題に関心を持っている人たちに、今インターネットで参議院の審議は中継されていますので、見てもらいました。よくわかったという反応も非常に多かったですけれども、一方で、一部の私の発言に対する他の委員のコメントについて、皆さんから、参議院の議論というのはそんなに言いっ放しでかみ合わないまま行われているのかと。中には、世耕さん、このまま黙っていていいのかというような声もございました。きょうは技術の専門家もおいでですから、あえてそこを取り上げさせていただきます。

その箇所というのは、この間資料も配らせていただきましたけれども、五月三十日付の朝日新聞記事について私が言及した部分であります。

この記事をもう一回要約しますと、見出しはＮＴＴの外でも電話傍受が可能という記事でございます。趣旨としては、ＰＴＴという装置を用いて、きょうの森下参考人の絵の中にも出てきます試験制御装置にアクセスをすれば、ＮＴＴの外、場合によっては警察署の中でも通信の傍受ができるという趣旨の記事でございました。

この記事に関して私は私なりにいろいろ調査検証をして、前回の質疑の中で、そもそもこのＰＴＴというシステムがどういう背景で導入されたのかという理由を説明して、決してＮＴＴのビルの外で聞くことを目的にしたものではないということを明らかにさせていただきました。

さらに、これは記事中にも述べられていますけ

れども、大前提としてＮＴＴが全面的に協力しなければならないけれども、そんなことをＮＴＴは絶対にやるわけがないということも指摘をさせていただきました。

そして、さらにさらにその上で、ここは非常に重要ですので私はビデオから起こした発言のとおり読みますけれども、こう私は申し上げました。

技術的にもこの記事は致命的なんです。というのは、先ほど申し上げましたように、試験制御装置というのはアナログ電話の場合は待ち受けて聞くことはできないんです。既にできている通話を聞くことしかできないんです。ずっと待っていたら話し中になっちゃうんです。このＰＴＴというのは試験制御装置を延長して出ている無人交換局でチェックするための装置ですから、これを幾らつないだって技術的にそもそも傍受そのものができないということで、この記事は前提が大きく間違っているということを一つここで指摘させておいていただきたいと思います、こういうふうに私は申し上げました。

それに対して、後で質問に立たれたほかの議員の方、具体的には中村敦夫議員ですけれども、御自分の質疑の中で、これも重要なところですのでビデオから起こした原稿どおりに読みますけれども、これまでの政府答弁では通信傍受基地は通信事業者等の場所に限ると言明してきました。しかし一方では、やろうと思えば通信事業者の機能がある以外の別の場所でも傍受基地を設定することができるという技術的環境があるわけなんですね。先ほど世耕さんから例にも引かれました五月三十日の朝日新聞朝刊の問題ですが、これはノートパソコン型ポータブル試験端末、ＰＴＴを設置すれば通信事業者の場所の外でも盗聴できるではないかという趣旨の疑問か出ました。それに対して、法務省談話として、そういう方法は聞いたことがないし、警察署で聞けるというのは全然考えていない。令状は実際に傍受する場所を書くのであって、電話局しかあり得ない。まあ、この電話局とは広い意味で通信事業者等の場所だというふうに理解しますね。世耕さんからいろいろとＮＴＴ内部の運営事情などの説明もありましたが、結局のところですね、技術的な問題としてはＮＴＴの協力さえあれば可能だという証言になっていたわけだと私は受け取っていますと、こういう形がありました。

もう一度重要なところだけ繰り返しますが、私は、このＰＴＴというのは試験制御装置を延長して出している無人交換局でチェックするための装置ですから、これを幾らつないだって技術的にそもそも傍受そのものができない。こう発言をしているのに対して、世耕さんからいろいろとＮＴＴ内部の運営事情などの説明もありましたが、結局のところですね、技術的な問題としてはＮＴＴの協力さえあれば可能だという証言になっていたわけだと私は受け取っておる。こういうふうな発言をされました。

皆さん、よく今聞いていただければわかっていただけるように、私の言っていることとは百八十度違う整理をされています。これでは、私が貴重な自分の質疑の時間を割いて何のためにこの朝日新聞の記事に言及したのかわからなくなる、そう思っております。

通信傍受法案には賛成、反対意見、いろいろあると思います。私も反対の立場に立つ方の御心配の点というのも非常に理解できる部分がありますから、私の質疑の中では、運用上の配慮が必要だと思う部分もあることから、相当厳しく法務省をただして、傍受できる範囲なんかを限定したつもりであります。やはり相手の言ったことにも耳を傾けて討論を進めていくのが民主的なやり方ではないかと思います。

前回質疑したところを焼き直すのは余りやりたくはないんですけれども、本日は技術の専門家も見えておりますので、再整理をするいい機会だと思います。

またさらに、この記事が非常に重要なのは、前々回の質疑で福島瑞穂議員がこの記事を一つのよりどころとして通信傍受法に問題ありという指摘をされているわけです。朝日新聞というのは購読者も非常に多い、影響力のある新聞であります。また、その後、訂正記事が載せられたということも全然ございません。誤解をされたまま審議が進むと私はまずいと思いますので、この記事が正しいのか誤っているのかというのは審議を進めていく上で非常に重要だと思います。

この記事では匿名のＮＴＴ職員なる人物が出てきて証言をしておりますけれども、本日まさにＮＴＴの技術部門の最高幹部がお見えになっているわけですから、その辺をきっちり整理しておくいいチャンスだと思っております。

まず、森下参考人にお伺いいたしますけれども、アナログの試験制御装置でそもそも待ち受けができなくなっている理由は何なんでしょうか。

○参考人（森下俊三君）　お答えさせていただきます。

先ほどのＰＴＴと試験制御装置というのと二つあるわけでありますが、試験制御装置もＰＴＴも物理的に加入者のお客様の線がどうなっているか、この絵でいきますと、基本的には②の配線盤のところからお客様の電話機のところまで二本の線が延びていっているわけですけれども、その線が劣化して故障しているかどうか、あるいは電話機が故障してダイヤルがちゃんと出ないのかどうかとか、それを試験するための装置なんです、もともとは。

ですから、試験をしようと思ったときに、たまたまその回線に割り込んだときにもし通話中ですと通話の邪魔になりますからじっとそれを待っていて、通話が終わったら試験をすると。試験するのは当然お客様の線の方で、反対側の方は試験する必要がありませんから、そこを全部切り離してしまうわけですね。ですから、必ずその試験する線の方しかつながらないようになっているということなんです。

ただし、その電話機のダイヤルかいいか悪いかというのはダイヤルをしてみないとわかりません。それを試験装置でもってその電話機のダイヤル信号がきちんとつながるかどうかを受信する試験装置があるわけですから、そういう試験のときにもお客様の方からは発信できるようにしておかないと試験ができません。ですから、先ほどお話ししましたように、発信の試験ができるような機能は持っています、ですけれども着信ができないというのは、もともとこの装置はそういうように試験用の装置でありますから、相手側は切り離してあるということです。

それから、ＰＴＴといいますのは、基本的にこういう工事を行う、お客様から注文を受けて工事を行うときにその工事をする場所まで出かけていかないといけません。通常、試験をする場所というのはかなり集約してありますので、場所は限定されているわけでありますが、こういった交換機を置いてありますＮＴＴビルというのはたくさんあるわけでありまして、実際そこで工事を行わないといけませんので、工事をする人はそこへ行って、そこで工事の結果がちゃんとできているかどうかを試験する、そのためのものがこのＰＴＴでございますので、ＰＴＴというのはもう本来試験機能しかないということなんですね。ですから、今の試験制御装置よりももっと機能が限定されたものがＰＴＴでありますので、デジタル電話も全く通話はわかりませんし、アナログの場合も全く発着信はできない。もう単にそこに割り込んで、通話が終われば試験をするという機能しかないということですので、そこのところがこの記事には相当誤解があるのではないか。

ですから、たまたま通話しているところにぱっと入れば通話がモニターできるということは機能としてはありますので、そういう一部のところを非常に拡大して、そこだけをあたかも誤解を与えるかのように書かれているのではないかというのが私どもの解釈でございまして、基本的にはこれはもう試験機能しかありませんので、そういった意味では非常に誤解を与える記事だというふうに理解しております。

○**世耕弘成君**　非常に明快な整理で、よくわかりました。そもそも試験制御装置もＰＴＴも目的は全然違うし、そういう通信を待ち受けて傍受する機能そのものを全然持っていないということが前提になると思います。

　このＰＴＴ端末で試験制御装置へのアクセスというのは、これは当然電話回線を使ってやっておられるという理解でよろしいですね。

○**参考人（森下俊三君）**　はい。

○**世耕弘成君**　ということは、電話回線ということは、ある意味でだれでも電話でとりあえずアクセスはすることができる。要するに、これはハッカーですとかあるいはセキュリティーシステム上、非常に脆弱な部分もあるんじゃないかという心配があると思うんですけれども、そういうことにならないためにＮＴＴとしてどういう対策を打たれているんでしょうか。

○**参考人（森下俊三君）**　基本的には、こういう試験装置につきましては、操作できる人のパスワードもありますが、それ以上に、その端末等がすべて登録されているとか、あるいはコールバック方式と言っておりますが、一遍つないだ後で試験装置の方から決まった電話機にしかつなげないという機能を持たせること、それからもともとこのＮＴＴのビルにつきましては、ビルの入退室の管理、これはすべてシステムで管理しておりますので、ビルのセキュリティーを含めてそういう試験装置のアクセスにつきましても相当の範囲でセキュリティーの機能を持たせているというふうに考えております。

○**世耕弘成君**　今の御発言ですと、まずパスワード、さらに端末のパスワードを知らなきゃいけない、さらに端末が登録されていなきゃいけない、そしてさらに電話回線も試験装置の方からかけ直すわけですから、もう極めて指定された、限定された電話回線からしかアクセスができない、そういうことだと思うんです。

　ということは、この記事にも書いてありますか、ＮＴＴが警察に協力をしない限りはまず絶対にＴＷＳに、試験制御装置にＰＴＴ端末でアクセスすることはできないということになると思うんですけれども、ＮＴＴが警察に協力をする、パスワードを教え警察の端末を登録し、警察の電話回線に対してコールバックするような設定をする、そういうような可能性はあるんでしょうか。

○**参考人（森下俊三君）**　基本的には、私どももともと通信の秘密を守るということが使命でありますし、社員にもそういうことは教育を徹底してきております。

　それから、特定の社員が万が一そういうことをやったといたしましても、多分それはシステムの方でチェックをしておりますし、それからシステムの管理も特定の人間だけでやっているわけではございませんので、複数の組織でいろんなチェックがかかるようにしております。ですから、特定の状態で、先ほどお話しになったようなことはまず起こり得ないというように考えております。

○**世耕弘成君**　このお配りの絵では、上段がアナログ、下段がデジタルという形になっておりますが、今このアナログとデジタルの比率というのは大体どれぐらいになるんでしょうか。

○**参考人（森下俊三君）**　現状では、毎年二百数十万のＩＳＤＮのお客様がふえておりますが、十年度末ではアナログが大体九三％ぐらい、デジタルが七％ぐらいのお客様ということでございます。

○**世耕弘成君**　もう一度今の森下参考人のお話を整理しますと、試験制御装置へのアクセスに関しては非常に厳重なセキュリティーシステムをとっておって、ＮＴＴが協力しない限りシステム自体にアクセスすることは不可能、そしてＮＴＴが協力することはあり得ない、そして電話の九三％を占めるアナログ電話についてはそもそも技術的に傍受そのものができないという整理になると思います。

　ということで、この五月三十日付の朝日新聞の記事は、今、森下参考人の御答弁の中にもありましたけれども、非常に誤解に基づいた記事だということを、これ実は前回明確にしたのでもう一回やるのは非常に残念なんですけれども、もう一度明確にさせておいていただきたい、そういうふうに思います。

　それでは、今度は桑折参考人の方にお伺いをしたいと思います。

　先ほどの携帯電話のつながる仕組みというのは、私も余り詳しくない部分ではあるんですけれども、御説明を聞いて非常に明快に整理をされたと思います。端的にお伺いいたしますが、携帯電話の中で通信を傍受するとした場合に、一体このネットワーク構成の中のどこで傍受をすることになるんでしょうか。

○**参考人（桑折恭一郎君）**　お答えさせていただきます。

　先ほど申し上げましたように、携帯電話の場合に、発側の移動機、それから着側の移動機がある基地局の通話チャンネルとつながって初めて通話が成立するわけですけれども、それがどこかということをあらかじめ特定するというのはちょっとできない。その都度その都度非常にもうあいているところを次々とつながっていくという問題が一つと、それから先ほど申し上げましたように、通話中にも場所が移動するなり、同じ場所でも非常に微妙な場合ですと隣のセルに移動してしまうというようなケースがございまして、その場合にはまた回線を全部再設定し直してしまうというようなケースがございます。

　ですから、一番の問題点は、このネットワークの中のどこでその目的とする通話が流れているのかということを知ることが非常に難しいというところにあるかと思います。

　以上でございます。

○**世耕弘成君**　そうすると、その難しい中で、そもそも傍受ができるんでしょうか、できないんでしょうか。

○**参考人（桑折恭一郎君）**　基本的には、全くできないかどうかということは別としまして、まず、ある発側からある着側の呼というのが出た場合に、それを私どものネットワークの中でどの基地局の何番目の回線かということをまず知るという手段だけはございます。それを知った後、初めてその回線かフルレートなのかハーフレートなのかということを調べて、それからそれに対してのモニターをかけるということはございますけれども、その場合も、それでやったときに果たしてそのまま同じ通話がその回線上に乗っているかという保証は非常に難しいということで、現実的には、まず回線の特定からモニターを入れるまでということが非常に時間的にかかるということと、それからやってみたらまた別の回線設定に変わっていたというような可能性も非常にあるということで、現実的には非常に難しい問題だと考えております。

○**世耕弘成君**　残念なから時間がなくなってきましたので、最後にもう一度、五月三十日の朝日新聞の記事については、私の発言内容を一方的に誤った形で解釈し発言されたことについて、本日発言の時間をお持ちのようですから何らかの誠意ある御発言があるのではないかなと信じたいということを申し上げて、質問を締めくくらせていただきます。

　ありがとうございました。

○**内藤正光君**　民主党の内藤正光でございます。

　両参考人におかれましては、本日お忙しい中、こうしてお越しをいただきまして、本当にありがとうございます。

　まず、通信手段として何が考えられるか大別をいたしますと、従来の一般電話、これが一つ、二つ目としてインターネット、そして三つ目として携帯電話などが考えられるんではないかと思います。

　ところが、犯罪目的の使用を考えた場合、それぞれの通信手段はどうなんだろうか。まず、従来の一般電話というのはやはり足がつきやすいんであろう。そしてまた、インターネットというものもまさに証拠そのものをネット上に残すわけで、果たして犯罪に多用するだろうか。こんな疑問を私は持ちます。犯罪目的ということを考えた場

合、携帯電話を使うというふうに考えるのが妥当なんだろうと私は思います。

ところが、残念なことに、この携帯電話について今まで余り審議されてきませんでした。私は、携帯電話について、本法案、通信傍受法案の実効性を検討するのはそういった意味では大変重要な意味を持つものだろうと思います。

そこで、私は、携帯電話について、専ら技術的な項目について質問をさせていただきたいと思います。

参考に私もこのように皆様のところへシステム構成図をお配りさせていただきましたので、こちらを使いながらいろいろ議論をさせていただきたいと思います。

まず、端末と基地局との間は無線でやりとりが行われております。桑折参考人にお伺いしますが、この無線を傍受することで特定の通話をモニターすることは可能なんでしょうか。不可能であればなぜなのか御説明いただけますでしょうか。

○参考人（桑折恭一郎君）　お答えさせていただきます。

無線区間で傍受することにつきましては、私としては全く不可能だと考えております。その理由としては二点ございまして、一つは先ほど申し上げましたように、一つのセルに対してある電話機がつかむチャンネルの最大数というのは四十四回線、ハーフレートですとその倍ぐらいございますけれども、そのうちのどの回線をつかむのかというのかそのときそのときで変わってしまう。

それともう一つは、同じ端末から同じ発信をしたとしても、フルレートかハーフレートかということはそのときそのときで違ってしまうという形で、そこのところの特定がまずできないということが一つ。

それともう一つの点は、アナログの携帯電話と根本的に違うところは、アナログの場合ですと音声を基本的にはある特定のキャリアという周波数で変調して、それをエアの部分に出しているわけですけれども、デジタルの場合は、先ほど言った特殊な圧縮方式を使っているということと、それの解読が難しいことと、さらにエア部分につきましては、傍受されないセキュリティーを保つという逆の面の目的からスクランブルというものをかけておりまして、一般的にエアの部分でそれを解くということはできないようになっております。

そういったことで、この無線区間で特定の回線をつかむことが難しいことと、つかんだとしてもその中身の声がどうなのかということを解読することについては全く不可能だというふうに考えております。

○内藤正光君　アナログの時代はそれこそ秋葉原に行って受信機を買ってモニターできたかと思いますけれども、念を押してお伺いするんですが、デジタルの場合はそんなぐあいにはいかないというふうに理解してよろしいんですね。

○参考人（桑折恭一郎君）　はい、そのように考えております。

○内藤正光君　次に、携帯電話のつながるプロセスなんですが、先ほどの桑折さんの御説明でよくわかりました。

私は携帯電話と一般電話というのはやはりちゃんと分けて考えるべきなんだろうと思います。一般電話の場合は、それこそ加入者回線といって電話局から各家庭へ延びている回線と電話番号とはくくりつけ、一対一の関係にあるわけです。だから、これが容疑者の電話につながる回線なんだということで最初から事前に目星をつけて待ち受けることが可能なわけです。ところが、携帯電話の場合は通話のたびごとに、こちらの図にもありますように、交換局から基地局との回線並びに無線が割り当てられる。つまり、事前にこれが容疑者の回線だということで特定をして待ち受けることができないわけですね。

そこで質問なんですが、着信の場合と発信の場合とに分けて質問をさせていただきたいと思います。

まず、着信の場合です。六ページの図を参考にさせていただいておりますが、右側、着信の場合、これはどの回線が割り当てられたのかというのはシステム上で管理されているんですか。

○参考人（桑折恭一郎君）　着信につきましては、ある電話番号がどの回線に割り当てられるかということについてはあらかじめこの回線だということは特定できませんけれども、接続された後に、今この何番目の無線機の何チャンネルにこの電話機がつながっているということを知る手段だけはございます。

○内藤正光君　では、発信の場合についてはいかがでしょうか。

○参考人（桑折恭一郎君）　発信につきましては、たまたまこれは私どものシステムの問題かもしれませんけれども、今言ったような事柄を、あらかじめこの番号がという形で見た上で、それを知るという手段については、きょう時点のシステムではできておりません。

○内藤正光君　それは、そういう機能はお客様にサービスを提供する上では何ら必要のないものということだからなんですね。

○参考人（桑折恭一郎君）　基本的には今おっしゃったとおりでございます。

○内藤正光君　では、私の図の右上のところに監視センターがございますが、監視センターから特定の通話をモニターすることは可能なんでしょうか。

○参考人（桑折恭一郎君）　先ほど申し上げましたように、ある着信の番号に対しまして交換機がどのように回線設定されたかということがわかった上で、その回線設定をしたところにモニターをつくるということをやりますと可能です。

ただし、先ほど言いましたように、その間に発側も着側も移動していた場合にはその作業は全くむだになってしまうということでございまして、現実的には非常に時間もかかりますし、それに対する信頼性といいますか、そういったものについては非常に疑問な点はあるかと思います。

○内藤正光君　では、通話モニターが可能な条件をちょっとここで整理させていただきますと、まず、通話者のうちの少なくとも一方、これは実質的には容疑者が御社のデジタルホンの端末を持っていることが最低条件としてあるわけですね。そしてその次に、かつ容疑者が他の人から着信を受ける場合でなければならないということですね。

逆に言えば、幾ら御社の端末を使っていても、容疑者が発信をした場合は全く通話モニターできる可能性はないというふうに考えてよろしいですね。

○参考人（桑折恭一郎君）　今おっしゃったとおりでございまして、発信をした場合に今すぐモニターをするという機能は今の私どものシステムでは持っておりません。ということは、不可能だというふうに考えていただければいいかと思います。

○内藤正光君　同じような質問になるかと思いますが、念押しさせていただきます。

つまり、御社の現行システムでは、通信傍受の捜査協力をするにはかなり限界があるというふうに考えてよろしいわけですね。

○参考人（桑折恭一郎君）　今おっしゃったとおりで、傍受を始める条件というのが今言った着信側であるということが一つと、それから傍受をし始めるまでの時間が非常にかかるという問題が第二点でございます。それからもう一つは、仮にそれをモニターで聞き始めた段階で移動その他が起きた場合には処理そのものがむだになってしまうということで、確実性というものについては非常に難しい問題があると考えております。

○内藤正光君　着信の場合であってもかなり時間がかかるということなんですか、具体的にはどういうプロセスを経てどれぐらいの時間がかかるというふうに考えればよろしいんでしょうか。

○参考人（桑折恭一郎君）　まず、センターの方でどこの場所にいるかということがわからないというところから事が始まるわけです。ですから、仮に東京デジタルホンの管内にいるということがまず第一の条件でございまして、これが他社のところに行ったときにはうちのシステムでつかむこと

はまず不可能だということが第一点ございます。

それから、私どもとしては、基地局で使用している交換機というのは現在九台ございますし、これからまたかなり数がふえてまいりますけれども、その中のどの基地局の交換機に入るのかということをまず知らないといけない。それがわかった上で、基地局交換機から各基地局の、先ほど言いました何番目の無線機の何チャンネルかということを特定するという調査がかなりかかります。それがわかった段階でフルレートかハーフレートかということを確かめまして、それに必要なモニターをするということで、時間的にはかなりかかると思いますし、今までそういったものの具体的な処理をやった実例がございませんので、どの程度でできるのかということもちょっと今のところははっきりしないという状況でございます。

○**内藤正光君**　ちなみに私が調べたところでは、シェアの六割近くを握るＮＴＴドコモさんに関しても事情は同じだというふうに聞いております。

簡単に説明をさせていただきますと、通話か開始したことは事前設定しておけはわかる。しかし、固定電話ならは通話が開始したということでこの回線だということがわかるわけですが、回線特定は数百本単位でしか特定できない。つまり、この交換機から出ている回線のいずれかか容疑者の使われている回線なんだと、だからそこから一本一本回線探索が始まる。正確な時間はやったことがないということで教えてもらえなかったんですが、仮に一本当たり十秒かかったとして百本目に当たったとしても一千秒、およそ二十分近くかかるわけです。この手の通信傍受の対象になるような通話はそんな二十分も長話しているとは到底考えられない。一分近くで探索ができなければ実行上通話モニターは不可能であるというふうに言えるのではないかなと思います。

では、最後の質問をさせていただきたいと思います。

さきの郵政省と法務省の取り決めが新聞に出まして、システム開発は通信事業者が負うべき協力事項には含まれないというふうになっていました。しかし、御社の場合、仮に発信の場合にも通話モニターができるような仕様設計、仕様変更をしてくださいと言われた場合、それにかかるコストはいかほどか教えていただけますか、本当にざっくりで結構でございますので。

○**参考人（桑折恭一郎君）**　大変申しわけないんですけれども、交換機のソフトというのは一般のシステムのソフトウエアに比べまして時間とコストが非常にかかるということでございまして、今のお話を実現するためには、まずどのような仕様でどのような条件のときにどういう交換機のソフトを直すのかという検討から始めていかないといけないわけですけれども、その検討を詰めるまでにもかなり時間を要するのではなかろうかというふうに思っています。

一般的に、交換機のソフトだけで解決するかどうかというのも今後の検討でございますけれども、仮にうまくいったとしましても、交換機のソフトだけで見ますとやっぱり何億というオーダーには最低限でもなろうかと思います。

○**内藤正光君**　今回の通信傍受法案は携帯電話についてその実効性が今までほとんど審議されてきませんでした。ところが、今私がこうやって専門家の方々にその実効性についてお尋ねしたところ、かなりの問題かある、実行上不可能であるということがわかったわけでございます。

そこで、一つ質問をさせていただきたいと思いますが、例えば着信の際、その回線探索を始めるわけですけれども、この回線探索というプロセスの中で不特定多数の他人の通話も聞かざるを得ないということですね。

○**参考人（桑折恭一郎君）**　まだ具体的に対策の方法の細部というのは詰めておりませんのではっきり申し上げられませんけれども、先ほど申し上げましたように、回線を一つ一つ見るという中では当然そういう事態が起こるおそれもありますし、それから仮に目的の回線にぶつかった場合でも、果たしてそれが正しい発信、着信の会話であるかということ自体の特定も非常に難しい問題があろうかと考えております。

○**内藤正光君**　これで私の質問を終えますが、この通信傍受法案を審議するに当たって、携帯端末が全くと言っていいほど今まで審議されてきませんでした。私はこれは大変大きな問題ではないだろうかと思っております。私は、携帯端末で通信傍受ができなければ、この通信傍受法案を何のためにつくるんだろうか甚だ疑問を感じざるを得ません。そのことを一言申し上げまして、私の質問を終えさせていただきます。

○**大森礼子君**　参考人の方、きょうは大変にありがとうございます。

今、携帯電話の複雑な仕組みを御説明いただいたのですが、携帯電話については、傍受の実効性と言ったらいいんですか、これは不可能であるというふうに結論づけられたわけなのですが、桑折参考人の結論はそのようになっていたのでしょうか。携帯電話については通信傍受ということは不可能に近い、そういうお考えをお持ちなのでしょうか。

○**参考人（桑折恭一郎君）**　先ほど幾つか御説明申し上げましたように、非常に難しいという点が一つと、それを仮にやったとしましても、通話中にもまた回線の設定が変わってしまうとかいろんなダイナミックに移動する要素というのが入っておりまして、それでもってこの会話の傍受であると保証することが非常に難しいというふうに御理解いただきたいと思います。

○**大森礼子君**　技術的な問題点というのはあろうかと思います。それから、固定電話の場合と携帯電話と同様に考えることができない。携帯電話の方が非常に技術的に複雑といいますか、ですから難しいだろうというのはわかりました。

ただ、今、桑折参考人もおっしゃったんですが、例えば一つの問題点として、どこにいるのかわからない、つまりその携帯を持った人がどこにいるのかわからない。例えば、管内にいるのであれば非常に捕捉しやすいが、非常に移動するわけですから、その持っている本人はどこにいるかをつかむことが困難であるとおっしゃいました。逆に言いますと、大体ここら辺のこのあたりにいるだろうということがわかれば、これは非常に捕捉しやすくなるとも言えると思うのですが、そのように考えてよろしいでしょうか。

○**参考人（桑折恭一郎君）**　今までの御質問というのは、傍受ということで会話の中身はどうなのかという御質問を受けていたと理解しておりまして、それについては先ほど申し上げましたように非常に難しいということがございます。

大体どの辺にいるかどうかという事柄につきましては、先ほどの複数のセル、これは半径何キロぐらいになるかわかりませんけれども、そういった中のどの辺にいるかということについては、会話の傍受ということに要する時間なり信頼性に比べれば、比較的場所の特定だけはしやすい。ただ、郊外に行けば行くほどセルの半径というのは大きくなっておりまして、それがまた一つのセルに特定できませんので、そういったことで、ある程度その目的は達成されるのかどうかということについてはちょっと私としてもわからないところであります。

ある程度の場所にいる、例えば東京都にいるのか何とか県にいるのかという程度のことであれば、傍受という観点よりは比較的つかみやすいというふうに考えております。

○**大森礼子君**　わかりました。場所とかにつきましては特定する方法もあるし、またいろんな情報もあるだろうと思います。

いずれにしましても、大事なことは、この通信傍受法というのがなぜ必要となったかといいますと、電気通信分野における技術が非常に速いスピードで発展を遂げていきますと非常に通信手段が便利になります。そして、国民にとって非常に便利な通信手段が生まれますと、他方でその便利な手段を犯罪の用にも供するということで、犯罪捜査の面から見ますと便利さというのは常に悪用

の危険も伴っております。例えばクレジットカードというのができたときに、ああ、これは詐欺がふえるなと思ったらもうクレジットカード詐欺がふえる、こういう形になっていると思うのです。

ですから、現在非常に困難な部分があるからといって、では携帯電話だけは除きますということになりますと、みんな携帯電話を使うわけでございます。これは一つの課題としてこれから研究、検討していかなくてはいけないと思いますし、また捜査側の方と通信事業者の方ともいろんな検討をしていただくことになるだろうというふうに考えます。

それから、先ほど世耕委員がもう既に聞かれたのですが、五月三十日付の朝日新聞の記事ですね。「電話傍受　NTTの外でも可能」、これをNTTの職員が指摘ということで、これ私も読みました。

それで、いろんな議論をする中でやはり正しいところに到達しないといけないわけであって、こっちはああ言い、こっちはこう言いということではいつまでたっても結論がつかない。きょうは一つの結論を出していただいたのかなという気がいたします。

それで、例えば警察の方がパスワードをよこせと言ったら、世耕委員がそういうPTT端末を使っての傍受についてNTT側は協力することなんかはあり得ないと言いましたら、どこかで協力義務が書いてあるじゃないかというふうに声が飛んだわけですけれども、この協力義務は「通信事業者等は、正当な理由がないのに、これを拒んではならない。」というわけでありますから、正当な理由があれは拒んでもいいわけでありまして、まさにこれは正当な理由に当たるだろうと私は思いますし、また裁判官がNTTの建物の外でやれなんという令状を書くこともないのではないかなという気もします。

私はこの記事を読んだときに、この記事は警察がパスワードをよこせと言ったらどうなるんだ、危険なことになるんだと、こういうような書き方をしているわけですが、私は逆に、変なことをする人は警察だけとは限りませんで、先ほど世耕委員もセキュリティーの問題をおっしゃいましたけれども、実はこの前、電話番号情報が漏れたというのがありましたので、そんなこともあって、私人による悪用とか乱用とかも同時に我々は危機感を持って考えなきゃいけないことではないかなと思うわけです。

それで、いろんな情報というのが多く蓄積される、それから非常に有効な機能を持ってくるということになりますと、その情報というのは一つの財産にもなるわけですから、必ずこれを悪用する人がいるのではないか。そして、一人だれか変な人がいますと組織全体がおかしいという言い方をよくするんですが、私はそうは思わないんです。一定の人数がいれば必ずその一定の割合で変な人はいると思うわけです。

こういったことから、通信事業者内部ではセキュリティーの問題についてどのようにお考えか、両参考人に簡単で結構ですからお答えいただきたいと思います。

○参考人（森下俊三君）　まず基本的には、私どもは電気通信のサービスを提供するということですので、通信の秘密を守ることが第一だということは社員に対して教育しておりますし、それから就業規則、社員の規則等でも規定しております。

そのほか、例えばこのシステムにつきましては、先ほどお話ししましたように、パスワードの管理、あるいはシステム上でサーバーから登録されている電話しかつながらないようにするとか、あるいはそのサーバーの管理はまた別の組織で管理している。要するに、一人の人がすべてのことができるようにはなっていないということなんです。だから、そういうように組織的に幾つかの組織で管理をしているということですから、特定の人が何かをやろうとしてもどこかで必ずそれが牽制できるというように考えております。

それからもう一つ、傍受ということになりますと、たまたま今通話しているものにぱっと割り込んでしまうということは、それは先ほどのPTTでも可能になるわけですけれども、ただ、今それが通話しているかどうかをどうやって知るかという問題があるわけであります。あらかじめずっと監視しているということになりますと、社員もずっとそこの席にいるわけじゃありませんし、勤務時間も交代いたします。そういった意味で、特定の人がそういうことを同じ職場の中でやっているということは、基本的にはほかの社員の目もありますので、まずそういうことも実行的にはあり得ないのではないかというように考えております。

○参考人（桑折恭一郎君）　私どもとしても、第一種通信事業者として、今のお話と同様にまず通信の秘密というものの重要性ということについては十分認識して、また社員に徹底しているつもりでございます。

具体的に申しますと、一つはネットワークの観点から、それからもう一つは社員のモラルというかそういった面、あとシステム的な裏づけとに分けられるかと思います。

まず、ネットワーク上PDCというものは、先ほどもちょっと申し上げたかと思いますけれども、やはりアナログに比べての大きなねらいの一つに、簡単に他人が通話内容を聞けないようにする、そのためにデジタルで特殊なコード変換をしたにもかかわらずさらにそれにスクランブルをかける、そういうことで万全を期すというシステムにしておりまして、今の段階では少なくとも第三者が無線区間でもって通話の中身を知るということは全く皆無であるというふうに私は考えております。それだけのシステムをつくってあるというふうに認識しております。

それから、第二点の社内のモラルその他についてでございますけれども、これももう開業以来、社員の教育の中で、十分通信の秘密というものがどういうものなのかということは再三にわたって講習なり文書なりで指導しておりますし、それからシステムに対する端末も当然パスワードというものの管理その他については万全を期しているということでございまして、その辺についても今までのところは私どもの会社として特に問題を起こしたケースはないというふうに思っております。ただ、これは今後また新しい社員が入ってくるとかそういう形でいろいろ問題もあるかと思いますが、今後も継続して念には念を入れながら徹底していくつもりでございます。

○大森礼子君　プライバシーの侵害というのは、それが権力者によってなされようが私人によってなされようがもしかしたら余り差がないものかもしれないという気がいたしますので、ぜひセキュリティーの面でも十分考えていっていただきたいと思います。

それから、通信事業者の方の協力義務で立ち会いというのを定めてございます。それで、通信事業者みずからの施設とか機器の保守管理が必要である上に、利用者の通信の秘密を預かりこれを守るべき立場にもあることから、立会人としてその傍受の実施場所において常時立ち会っていただくということになっております、場合によっては地方公共団体の職員となっておりますけれども。

この立会人としての役割につきましては、この修正案では、原案もそうですけれども、外形的な事柄についてのチェックとか記録の封印と考えておるのですが、通信事業者のお立場から見て立会人としての役割についてどのようにお考えでしょうか。桑折参考人、それから森下参考人の順でお尋ねいたします。それで、もしよろしければ切断権云々という問題も。例えば立会人が通信の内容を聞くということについてはどのようなお考えを持たれているか、これを順次お尋ねいたします。

○参考人（桑折恭一郎君）　先ほどから申し上げておりますように、傍受という問題につきましては、携帯電話の特殊性から見ての難しさということを御説明させていただきまして、それはある程度御理解いただけたかと思います。ただ、やはり今回の法案そのものについての重要性なり、それから決定がされた上での通信事業者の役割という

ことにつきましては、そちらも私としては尊重しなければいけない問題だと考えております。

ただ、立ち会いの具体的な形とか、それからまた切断権というお話が今ございましたけれども、この辺につきましてはまだ私どもはそれ以前の段階の技術的な問題をどういうふうに考えていくべきかという段階でございまして、正直なところまだ社内でも余り細かい議論にまで至っておりませんので、この辺がはっきりして、またいろいろ御指導いただいた中で私どもの会社としての考え方というものをまとめていきたいと考えております。

○**参考人（森下俊三君）**　今回の法案におきましては、電気通信事業者に対する義務といいますのは傍受のための機器類の接続など主に技術的な協力であると理解しております。

また、立ち会いに関しましては、直接的には電気通信事業者ではなくて捜査機関に義務を課しているものでありまして、通信事業者の社員等の立ち会いが困難な場合には地方公共団体の職員に立ち会っていただくようになるものと理解しております。ですから、電気通信事業者の社員が立ち会う場合におきましても、立会人は傍受すべき通信の該当性の判断だとか内容に立ち入って関与するという立場にはないというように理解しております。また、通信傍受の際に立ち会うということは、通信事業者の立場からいたしますと、みずからの設備を保全するという目的にもかなうということもありますので、そういう面では立ち会うということでございますが、基本的には内容には立ち入らない。

なお、そういった場合でも、運用の問題といたしましては、電気通信事業者にコスト面とか稼働面で過度な負担がかからないように運用ではお願いしたいというように考えております。

○**大森礼子君**　通信傍受法に基づく通信傍受を円滑、適正に実施するためには、この法律が成立した後、捜査機関と通信事業者との間で事前に協議を行うことが大事ではないか。これは実施前にも必要だと思いますし、また実施後も技術の進歩等によりましていろいろ協議が必要であろうと思います。

それから、立ち会い等につきましても、民間会社の方に、やっぱり社員がいるということはコストもかかっているわけですから、余り過度な負担をかけてはいけないという、いろんな問題があると思います。

ですから、通信傍受の具体的な実施方法とか標準的な実施手順等について捜査機関とあらかじめ協議をしておいて、そういうことを定めておくことが望ましいのではないかと考えるんですけれども、通信事業者のお立場としてそのような協議を捜査側と行うことについてはどのようにお考えでしょうか。桑折参考人、森下参考人に順次お尋ねいたします。

○**参考人（桑折恭一郎君）**　今おっしゃったように、私どもとの協議という問題でございますけれども、これにつきましては、私としても、法案の趣旨にのっとって正しい判断を事業者としてもやりたいというふうに考えておりまして、協議といいますか、いろいろ御指導いただく絶好のチャンスでもあろうかというふうに考えておりますので、前向きにそういった形の場が持てればというふうには考えております。

○**参考人（森下俊三君）**　法案が成立いたしましたら、明確になりましたルールにのっとった対応を行わないといけないと思っておりますが、その際には関係方面と具体的な運用のやり方等については協議をさせていただきたいというように思っております。

○**大森礼子君**　終わります。

ありがとうございました。

○**橘本敦君**　携帯電話間の通信の傍受、いわゆる盗聴の問題ですが、これは大変困難だというお話は桑折さんからも伺いました。しかし、困難という事情はあるけれども、傍受はそれ自体不可能ではないということは、一面で、やり方によって、あるいは新しい技術の開発によって傍受自体、盗聴すること自体が可能になるということは言えるのではないでしょうか。その点はいかがお考えですか。

○**参考人（桑折恭一郎君）**　今回の法案自体の状況につきましては、会社の中でもこれが実際に成立した場合にどういう形でいくべきかという議論は既に始めておりまして、その場合に、当然、法案の趣旨にのっとった対策なり技術的な問題での解決ということについて積極的に検討していくという気持ちだけは十分あるつもりでございます。

ただ、まだ検討段階として非常に初期段階の議論になっておりまして、考えれば考えるほどいろいろあっちこっちに難しい問題があるなというようなことがございます。きょう時点で大体詰まったからこれで大丈夫だということの技術的な面でのまだ詰めも終わった段階ではございませんので、今後また引き続き私どもとしてはどういう形で解決策があるのかということについては検討していく用意はございます。

○**橘本敦君**　衆議院の法務委員会でもその問題が議論されました。携帯電話を聞くというのは技術的にどうなのかという議論がなされまして、それに関して郵政省の天野政府委員は、お尋ねの問題については、携帯電話を聞くということについてはかなり困難であるとおっしゃっておるんですね。

しかし、今後は機能としてオペレーションセンターなどの監視制御の問題を含めて、不特定の通話を通信信号としてモニターするということは可能であるにしても、その通信信号を音声として聞くためには特別な新たな装置を準備しなければならないということも一方でおっしゃっているんですね。

ですから、現状では直ちに聞くのは困難だとはいうものの、将来そういった技術の開発があれば可能になるのではないかという意見も当然この中には含まれていると思うんですね。だから、そういう意味で携帯電話同士の傍受が絶対に不可能だとは言えない、今後の課題としてあるというように私は見ざるを得ないと思うんですね。そうしませんと、この通信傍受法ができても、それこそ犯罪者グループは携帯電話同士でやればいいんだということになれば、せっかく法をつくっても意味を持たないことになりますからね。

そういう問題であるわけですが、一面でまた、この携帯電話同士の傍受を可能にする方法として、先ほどおっしゃいました問題に対して法務省の一部の考え方としては、事前にその特定した携帯電話を持った被疑者の立ち回り先を調べておいて、そして複数の交換局を傍受場所に指定して交換局ごとに傍受令状を請求するという方法もあるではないか、そういう意見が刑事局の中にあるという報道もあるんですね。そういうように押さえていけば、これはできるということになりますか。

○**参考人（桑折恭一郎君）**　私どもの例を申し上げますと、交換機の設置箇所というのは二カ所しかございませんで、その交換機の場所を押さえるというところについては、その二カ所の交換機のところで対応するということまでは可能でございます。

私どもが一番懸念しておりますのは、先ほどから申し上げますように、果たしてそれが正しい、本当に今回の目的に合った通話なのかどうかを特定することに非常に手間がかかるということと、それから一たんそれが目的の通話だったと仮にいたしましたときに、またそれが絶えず交換機の中で移動してしまう。あるルートでやっと回線構成がされた場合に、それが通話が始まってから終わるまで同じ回線構成でずっと続くという保証はなくて、ここまでできますと申し上げたときに、途中でまた別の通話になってしまうとか途中で会話が切れてしまうとか、そういう可能性があるので、どこまでこれが携帯として可能であると申し上げていいのかというのに非常に難しい問題があるということでございます。

○**橘本敦君**　そういう難しい問題を解決するということのためにいろんな手を打って網を広げてい

くということが捜査の方法として考えられる、このことがむしろ通信の秘密を侵す可能性が広まる問題として私は心配をしているんです。

その問題について、ＮＴＴドコモ関係のお話が載っている新聞で拝見をしたんですけれども、現在の通信事業者がお持ちになっている設備ではなるほど難しいと。しかし、そういう傍受ができるようにするために新たな開発ということになりますと、これは投資も要るし技術も要るし資金も要る、こうなってくるだろう。そういったことに対して、この法律ができてから以後、協力を要請されるということになって、政府からぜひそういう部門についての開発も検討してほしいというような要請があれば、それはどうなさるのかということが一つあるんですね。

その問題について桑折さんあるいは森下さんはどういうようにお考えなのか、ちょっとお伺いしたいと思います。

○参考人（桑折恭一郎君）　この法案成立後に移動体事業者としてここまでやるべきであるということの御指導をいただいた段階で、それに向けて私どもとしての技術検討を積極的にやっていく必要は事業者の義務として当然あるというふうに考えております。

ただ、先ほど申し上げましたように、まず技術的にどこまで可能なのかというようなこととか、それに対する問題点というのを関係の方とよく議論して、お互いに理解していただいた上で初めて、どういう設備でやった場合にこの目的が達成されるのかという結論まで行くと思います。そのために、私どもの中で一方的にこの程度でいいだろうというような形のものがきょう時点でまだつくれているわけではないということで、引き続きそういった法案の趣旨なり私どもの技術的な問題をお互いに理解し合いながら、そちらの方向に進んでいくということが必要かと思います。

それと、それに対する費用の問題がどの程度かということも、ある程度結論が出ない限りはちょっと算定自体が非常に難しいという面もございます。私どもとしても、片方ではできるだけお客様に安いサービスを提供したいという気持ちもございますので、その辺との兼ね合いでどういう形で御理解いただけるのかというのを今後考えていく必要があろうかと思っております。

○参考人（森下俊三君）　固定電話の場合は、先ほど御説明いたしましたように、アナログ電話の場合はＭＤＦでやるのが一番きちんとした傍受ができる、それからＩＳＤＮ、デジタル回線につきましては試験制御装置でそれが可能になるということですので、それを使っていただけば余計な開発等は不必要だと思っておりまして、関係機関にはぜひそれを使っていただきたいというように私どもはお願いしたいと思っております。

なお、今後どんどん技術が進歩してまいりまして新しいサービスが入ってまいりますと、そのときには当然また検討しないといけないかもわかりませんが、現状ではアナログ電話の場合はＭＤＦ、ＩＳＤＮの場合は試験制御装置で試験すれば大体目的は達成できるのではないかというのが私どもの考えでございます。

○橋本敦君　そうしますと、ＮＴＴとしては、お話がありましたいわゆるアナログ回線、それからデジタル回線、いずれについても新しい開発というようなことなしに通信傍受、つまり盗聴を令状によってやる場合は、今はそれ自体は可能になっているというお話ですね。

○参考人（森下俊三君）　そのとおりです。

○橋本敦君　そうしますと、もう一つの問題として、先ほど桑折さんから、法案ができてから後の協力義務の関係ではいろいろ検討しなくちゃならぬというお話がございましたが、その場合、先ほどもお話がありましたけれども、通信事業者として通信の秘密を守るという国民的な要請、憲法上の要請がございます。それと、政府からこの法案の実効性を確保するために新たなソフトの開発あるいは技術の開発の要請があった場合どう対応するかということで、これは非常に難しい問題になるんではないかと思うんです。そこらあたり、もう一遍お考えを聞かせていただけますか。

○参考人（桑折恭一郎君）　今お話がございましたように、少なくともきょうまでの第一種通信事業者としての私の立場から言わせていただきますと、やはり通信の秘密の重要性ということが私としては一番重要な問題でございまして、これは先ほどの社員のモラルの問題だけではなくて、システム的な面、ネットワーク的な面から、まず今まで一番検討の重要性を置いてきたのはその点でございます。

ただ、それと今回の法案との関係がどうなのかということでございますけれども、いずれにしましてもこの法案が具体的な段階に入った段階では私どもとしても尊重する義務があるかと思いますので、その辺は確かに通信の秘密との関係がどうなんだということについては、きょう時点、私としては本当にどちらを重要視するのか、それとも両方ある程度満足する解があるのかということについては非常に難しい問題だと考えております。

これにつきましても、具体的に私どもの事情、お話を聞いていただくなり、また法案の趣旨なり、それから通信の秘密との関係なりの御指導をいただきながら最善の解を見つけていくしかないというふうに考えております。

○橋本敦君　お立場はよくわかりました。ですから、この法案ができた以後どう対応するかは難しい問題だ、一概に政府の要請があってそれを拒否できるかというと、それはやっぱり検討しなきゃならぬということも考えざるを得ない、こういうことですね。

そういう意味で、今後この法案ができた以後、携帯電話間の通信傍受を一層可能にするためのシステムなり、あるいは技術的な開発なりという問題で政府から要請があった場合の事業者の皆さんの御負担というものについて私も実際は心配をしているわけです。

その点について、郵政省と法務省が交わした覚書が資料として出されているんですが、その中では、新たな投資やシステムの開発が必要となるものについては協力義務には含まれないという確認があるんですね。協力義務には含まれないけれども、しかし政府の方は協力の要請はできるという立場のようなんです。だから、協力義務には含まれないと書いていますが、協力は要請する。そうすると、任意に協力するということになってくると実際はこの覚書は生きてこない、こういうことになりますので、そういう意味で通信業者なりＮＴＴさんなりのこれからの立場というのは非常に大事じゃないか、私はこう思うんです。

それから、私は新聞で見たんですけれども、福島委員とも話し合っていたんですが、衛星携帯電話というのがあるんですね。この衛星携帯電話については通信傍受が困難だというふうに報道されているんですが、そうなりますと、この法案が通れば悪い連中はみんな衛星携帯電話を使うということも可能になってくるわけでしょう。これも技術的に困難だということは新聞に書いてあるんですが、これは技術的に通信傍受が可能になる技術の開発もこれまた可能ではないかと私は思うんですけれども、技術的な面としての御意見はいかがでしょうか。

○参考人（桑折恭一郎君）　衛星のシステムにつきましては、大変申しわけないんですけれども、私自身ほとんど知識を持ち合わせておりませんので、その辺の可能性の可否ということについては何とも申しかねるという点でございます。

○橋本敦君　森下参考人にお伺いしたいんですけれども、今、ＮＴＴでお役目をなさっているんですが、以前には電電公社にいらっしゃったということでございますか。

○参考人（森下俊三君）　はい、そのとおりです。

○橋本敦君　一九六四年に「通信の秘密」と題する文書がつくられておりまして、これはＮＴＴになってからも引き継がれておると思うんですが、この電電公社時代の文書によりますと、通信の秘密を守るということの立場から、現行犯逮捕に対する協力要請及び捜査機関等からの照会に対する措置として、そういう照会に応ずる場合には、一

つは、通信の当事者の同意がある場合のほか、被害者の生命、身体、自由に重大な危害が迫っておって、他の方法ではこれを救うことが困難であると認められ、かつ通信の一方の当事者の同意がある場合は照会に応じる、こういう規定があるんですね。非常に厳しく制限をしている。そういう意味で、捜査の要請があっても通信の秘密はもうぎりぎりのところまで守りますよという建前が貫かれているんですね。

私はこれ自体はいいことだと思うんですが、こういう立場が今も貫かれているのか。それからまた、今度は通信傍受法、いわゆる盗聴法ができた場合にはこの覚書はいわゆる協力義務ということで大きく変わってこざるを得ないのではないか、守り切れないのではないかというように考えておるんですけれども、そこらの点について参考人の御意見はどうですか。

○参考人（森下俊三君）　先ほどの「通信の秘密」につきましては、特に逆探知等で厳しい条件のもとでしか行っていないということだと思いますが、これにつきましては現行ＮＴＴになりましても現在でも同様でございます。ですから、運用につきましては、そういった意味では手続もかなり厳しく行ってきておるところであります。

今回の通信傍受法案が成立いたしました場合でも、これは成立後、関係機関と十分運用の方法については協議、お話し合いをさせていただくということになると思いますが、運用上は通信の秘密をきちんと守れるようにかなり厳しい手続をすることになるのではないかというように思っております。いずれにいたしましても、これは法案成立後、関係機関とお話をさせていただこうというように思っております。

○橘本敦君　今おっしゃったように、法案が成立すれば、せっかく電電公社時代に通信の秘密を守るということで自主的におつくりになった原則、今言ったように片方の当事者の同意がなければ緊急の場合でも捜査の照会で協力できないよとか、あるいは両当事者の合意かない場合は通信の照会に応じられないよと、こういう大事な原則は今度の法案でなくなっちゃうわけですよ。当事者の了解とか当事者の同意なしに通信傍受をする、いわゆる盗聴するというのがこの法案ですから。だから、そういう意味では基本的に今まで電電公社として通信の秘密を守るという立場で守ってこられた、そういうことが実際はこの法律によってできなくなる、そういう重大な問題でありますよということも私は指摘を申し上げて御意見を聞いたわけですけれども、その点、御意見があれば。

○参考人（森下俊三君）　本日は技術的な説明ということで参っておりますので、法律の解釈についてはちょっと御勘弁願いたいんですが、基本的には私どもは今回の通信傍受法案が成立いたしましてもそのあたりの条件は変わらないというように理解しております。

なお、法案の解釈につきましてはちょっと今回は御遠慮させていただきたいと思っております。

○橘本敦君　わかりました。変わらないというお考えは御意見としてはわかりましたが、法律は変えてしまうという重大な問題であるということを指摘して、質問を終わります。

ありがとうございました。

○委員長（荒木清寛君）　速記をとめてください。

〔速記中止〕

○委員長（荒木清寛君）　速記を起こしてください。

○福島瑞穂君　社民党の福島瑞穂です。

どうもお待たせして済みませんでした。

森下参考人にお聞きいたします。

先ほどアナログ回線、デジタル回線の比率をおっしゃいましたけれども、例えば来年あるいは三年後、五年後、十年後、この回線の割合はどういうふうになる予定でしょうか。

○参考人（森下俊三君）　基本的に言えば、これは私どもだけでサービスをやっているわけではありません、今後はＣＡＴＶ事業者の方のお客様もふえる、あるいはＴＴＮｅｔ等の事業者もふえてまいりますので、五年後、十年後どうなるのかというのは予測がつかないところがありますが、現状では、先ほど御説明いたしましたように、アナログからＩＳＤＮに毎年五千万のうちで大体二百数十万というお客様が移ってきているということですから、比率はかなり上がっていくだろうと思います。

それから、今後マルチメディア等のいろんなサービスがふえてまいりますし、インターネットがふえてまいりますので、かなり早い時期にＩＳＤＮのお客様がアナログの数を上回る時期が来るのではないかというふうな予想はしておりますが、いずれにいたしましてもこれはもうこれからの市場の状況によりますので何とも言えないところであります。

○福島瑞穂君　衆議院の法務委員に対してＮＴＴが「電話及びＩＳＤＮ回線における通信傍受」という資料をＮＴＴの見学のときに提示していらっしゃいます。

その中の電話回線、それからＩＳＤＮ回線のところに、傍受ポイントｃとしまして、電話回線のところは「試験制御装置の操作を行い、交換機の回線対応部に割り込み接続し、傍受用機器により通信内容まで識別可能。（但し、通話切断後は割り込んだ回線からの発信は不可）」、それからＩＳＤＮ回線のところも「試験制御装置や測定器の操作を行い、交換機の回線対応部に割り込み接続し、傍受用機器により通信内容まで識別可能。（割り込み中も発信可）」というふうになっております。

これは私たち参議院の調査室がつくってくださった資料にも入っているものですが、先ほど世耕委員の質問にお答えがありましたけれども、電話回線、ＩＳＤＮ回線において試験制御装置の操作を行い盗聴するということをＮＴＴ自身が提示していらっしゃるんです。

ですから、例えば電話回線の方がＩＳＤＮ回線よりも難しいところもあるかもしれませんけれども、電話回線、ＩＳＤＮ回線ともに盗聴が可能であると考えますが、いかがでしょうか。

○参考人（森下俊三君）　先ほど御説明しましたように、アナログ電話の場合は試験制御装置から故障のときに割り込むということであります。ですから、たまたま故障で割り込んだときにお話し中かもわからない、試験するわけですから。ですから、その割り込んだときにお客様が電話中ですと、モニターをしておりまして、それが終わってから試験をする。あるいはその試験のときにちゃんと通話できるかどうかがありますから、特別の機能を操作すればアナログの場合も発信だけはモニターしながらできます、だけれども着信はできませんということで、これはいずれも基本的に試験のためにそういうものを設けているということでございます。

それから、デジタルは基本的にどちらもできるようにしてありますが、これは先ほど御説明しましたように、デジタル信号がちゃんと通っているかを見るためにやるわけですから、どちらもできるということでございまして、盗聴云々という話がありましたが、基本的に私どもは電気通信のサービスを扱っている限りは、その作業の中で当然結果的に通信を聞くということは生じるわけであります。ですから、それは従業員規則等でそういう業務上で知ったものについてはきちんと通信の秘密を守りなさいという規則があるわけでありまして、先ほど言いました工事を行うあるいは故障作業を行うといったときに偶然知ってしまうということはあり得るということです。

今回の通信傍受法案につきましては、ですからこの法案が通りましたら、その機能を使っていただければ傍受ができますということをお話ししているところでございます。

○福島瑞穂君　でも、結局、試験制御装置の操作を行って盗聴することはできるわけですし、盗聴する場合にこの試験制御装置の操作を行うということも傍受としてＮＴＴは出していらっしゃるわけです。ということは、今回この盗聴法が実現した場合にはこの制御装置の操作を行って盗聴するということになると思いますけれども。

○参考人（森下俊三君）　先ほどお話ししましたように、試験をするということは私どもは盗聴とは考えておりません、盗聴というのは盗み聞くわけですから。基本的に試験をする、お客様からこの回線は故障ではないかということがありますから、そのために割り込んで試験をする。たまたまそれが電話中であれば電話をモニターする。その電話がちゃんと声が聞こえているかどうかも試験の範囲であるわけでありますから、あくまでも試験の範囲だというように考えております。

○福島瑞穂君　技術的に可能かどうかという問題と、これは試験の制度であるから盗聴法が実現しても使わないという問題がちょっと混同されているというふうに思うんです。技術的にこれは可能です。

それから、フラッシュの記事に石川県のＮＴＴが警察に協力して逆探知をしたというケースが載っておりますけれども、あれはＰＴＴを使って盗聴し逆探知もしたというケースなんですね。現に今、試験制御装置やその捜査を行っているわけです。

私たちが聞きたいのは、そういうことに使うかどうか、使えるかどうかということなんですけれども。

○参考人（森下俊三君）　先ほど御説明しましたように、ＰＴＴで待ち受けはできません。ですから、ＰＴＴをセットして待ち受けすると発着信が不可能になりますので、それで傍受はできないということをお話ししているわけです。だから、アナログの場合に、この試験制御装置というのをセットいたしますと、試験制御装置とＰＴＴは別ですから、発信はできても着信はできませんから、ですから傍受はできませんよということを先ほどお話ししたはずです。

○福島瑞穂君　ただ、電話回線とＩＳＤＮ回線の場合は、難度の違いはあるけれども盗聴は可能なのではないんですか。

○参考人（森下俊三君）　何度もお話ししていますが、今の装置にはそういう機能はありませんということを言っております。

デジタルの場合はなぜそういうことが必要かといいますと、中を通っているデータが高速のデータになっていますから、データがビット誤りを起こしているかどうかということは調べないといけません。ですから、そういうことを調べるために、上りのデータとか下りのデータが全部見れるようにしてあるということです。

アナログの場合はそういう必要性がありませんので、物理的なものを試験するようになっていますから、アナログの試験装置でやりますと着信はできなくなる。

それから、ＰＴＴの場合はあらかじめセットしておきますと発信も着信もできません。これはもともとそういう機能は必要ありませんから、工事用の試験用装置としてつくってありますので、ですから基本的にそういったものであらかじめセットして傍受するということは不可能であります。

○福島瑞穂君　確認ですが、デジタル回線の場合はこの試験制御装置を使って盗聴することは技術的には何ら問題はないんですね。

○参考人（森下俊三君）　先ほど御説明しましたように、この番号にセットいたしますと、発信、着信、両方とも傍受はできます。

○福島瑞穂君　それが確認できれば結構です。

次に、法務省は内線電話を使った盗聴についてホテルなどを例にとって説明をされております。例えばホテルと外部を結ぶ線は不特定多数の通信が行われるので盗聴はできない、そのためホテル内の交換機で盗聴するというふうにおっしゃっているんですが、内線用の交換機で盗聴は可能なんでしょうか。数千室もあるホテルの場合ではなくて、数十室のような小規模なホテルで使用される交換機でも盗聴は可能なのでしょうか。

○参考人（森下俊三君）　ＰＢＸの場合ですと、先ほどの絵でいきますと、お客様宅のところに電話機がたくさんあるわけです。ですから、ＮＴＴから行っている回線が例えば十本、十回線あるとしますと、そのホテルですとそこには百回線だった百回線電話がある。先ほど御説明しました引き込み線の一だとか二のところで私どもが見れるというのは、その十本の線しかわかりません。それから、そこはＰＢＸから発信しますとどの回線をつかむかはわからないわけです。ですから、内線のどの番号が私どもで言う私どものケーブルのどの線を捕捉したのかはわかりませんので、そういった意味ではＮＴＴのビルの方では傍受はできないということです。

ですから、今度はお客様宅のところ、要するにＰＢＸのところに同じように今度は配線盤というのがありまして、そこから電話線がずっと電話機のところまで延びていっておりますから、そこのＰＢＸの内線の配線盤のところで多分傍受をするのではないかというように思います。

○福島瑞穂君　一般企業の場合、ビジネスホンなどがたくさんありますけれども、容疑者がどの電話を使用するかわからない場合、交換機でどのように特定して盗聴するのでしょうか。

○参考人（森下俊三君）　ビジネスホンでも、私どもの線が一回線しかなくてお客様のところに何台かの電話機があった場合はすべて私どもの一回線に入ってきますから、そこを傍受することになります。ですから、どの電話から発信しているかはすべてこの一本の線で見てしまうというか、そういうことになるわけです。

それから、ここの線が複数回線ある、三回線とか四回線あって、しかもお客様のところにビジネスホンが十台とか二十台あった場合には、先ほどのＰＢＸと同様でございまして、どの回線をつかむかというのは代表を組んであったりしますと変わりますので、ですからＮＴＴ側の線、これは局線と言っていますが、その線を指定しただけではどの電話ということは決まらないということです。

○福島瑞穂君　そうしますと、同じ番号をみんなが使っているというような場合にはどれかわからないわけですね。そうしますと、結局、全部聞いてしまうことになるんですか。全部聞かないとわからないんでしょうか。

○参考人（森下俊三君）　基本的にはその線を指定していただくということ以外はできないと思います。

○福島瑞穂君　どうやって指定をするんですか。

○参考人（森下俊三君）　一応、代表電話が組んである場合でも、十本の線だったら十本の線に電話番号がついているわけです。ですから、その番号を指定していただく、そこを指定するということしかできない。だから、内線電話につきましては、あるいはビジネスホンでも、先ほどお話ししましたように内線はどの線をつかむかはわかりませんから、自動的に発信しますので、お客様のところの端子盤なり接続しているところで見ないとわからないということです。

○福島瑞穂君　しつこくて済みませんか、ビジネスホンだと、結局、複数をみんなが使っているわけですね。そうしますと、容疑者がこれを使うという特定はできないわけですね。その人は気分によって十番を押すかもしれないし八番を押すかもしれない。ほかの人の通話が同時に進行しているわけです。とすれば、どうやって特定するのか。いかがですか。

○参考人（森下俊三君）　先ほどお話ししましたように、複数の電話機、内線電話機をお使いになりますから特定できないということになります、それは。

○福島瑞穂君　ビジネスホンなどの場合は特定できないということを確認させていただきました。

先ほど協力義務のことで、パスワードなどを渡さない、世耕委員の質問に対してパスワードを渡さないと。もし誤読、ミスリードだったらごめんなさい。十一条の通信事業者等の協力義務に関してパスワードなどを渡さないという旨発言されたような気がするんですけれども、その協力義務の中身で、法務省と郵政省の覚書の中に「法案第十一条について」というのがあるのですが、パスワードを渡さないとかそういうことは一切盛られていないんですね。ですから、ＮＴＴは現在十一

条の協力義務についてどういう理解に立っているか教えてください。

○参考人（森下俊三君）　先ほど私はパスワードを渡さないという発言はいたしておりません。

それからもう一つは、先ほどの件につきましては、この新聞記事にありますようにＰＴＴを張り出してみても傍受はできないわけです。ですから、こういう不完全なものをやるということ自身は、もし関係当局が御要望された場合には、これは傍受は不完全だし、基本的には私どものビルの中でやっていただきたいということと、先ほどお話ししましたように、まずＭＤＦでやっていただけばそれできちんとできるわけですから、もともと不完全なものをもしお使いになるということであれば、それについては私どもはそういうことですよということをお話しさせていただこうというようには思っております。ですから、渡す、渡さないという議論は一切しておりません。

○福島瑞穂君　仮定の話で申しわけありませんが、もし警察の側がこれを使ってぜひ協力をしてくれと言った場合はどうなりますか。

○参考人（森下俊三君）　仮定の話は難しいんですけれども、先ほどお話ししましたように、これは傍受ができない装置ですから、たまたま割り込んだときに通話しておればモニターできますけれども、それ以外はできませんので、そこら辺を十分御説明して、何のためにお使いになるのか、むしろ傍受のためであればＭＤＦでやっていただければそれは私どもとしては協力をするわけでございますので、そういうお話をさせていただくつもりです。

○福島瑞穂君　デジタル回線の場合は試験制御装置を使って傍受をすることは可能なわけですね。それで、それに対して警察がＮＴＴに協力をしてくれと言うことは十分あり得ると思います。そして、協力義務の中では、こういうことは協力しないということの中には今まで出てきておりませんので、ＮＴＴ側は盗聴に関して全面的に協力をしてくれと言われた場合に拒否できる理由になるのかどうかという点についてはいかがですか。

○参考人（森下俊三君）　先ほど御説明いたしましたように、アナログの場合はＭＤＦでやっていただけば傍受の目的は達成できます、デジタルの場合は試験制御装置を使っていただけば傍受はできますというお話をしております。ですから、デジタルの場合はそれを使っていただくということになると思いますが、運用につきましては基本的には私どものビルの中でやっていただくということで関係機関には御相談をしたいというように思っております。

○福島瑞穂君　令状が出た場合はどうですか。

○参考人（森下俊三君）　先ほどお話ししましたように、目的は何かということであれば、私どものビルの中にある装置を、私どもの装置を傍受に利用していただいているということでございますから、そういった意味では私どものビルの中で使っていただくというのが原則でございます。ですから、そういうことを関係機関にお話をさせていただくということで私は関係機関の理解が得られるものだというふうに思っております。こういったものは外へ持ち出すものではないというのが私どもの解釈でございます。

○福島瑞穂君　条文上は傍受場所については特に限定はつけていないのですが、ちょっと時間がなくなりましたので、最後に御両者にお聞きしたいのは、立会人の問題です。

立会人が常時必要であるとなった場合に、アメリカの場合は例えばワイヤータップ・レポートによりますと一件について七百五十万ぐらいかかったというデータもあります。ですから、立会人をつけるという場合の費用などがどうなるのか。常時となりますと三交代になるのか、どうするのか。立会人についての御意見を御両者から、簡単で結構ですので、お聞かせ願えればと思います。

○参考人（森下俊三君）　この立ち会いにつきましては、運用の問題といたしまして、結構長時間になる場合もあると思いますし、件数がどの程度になるかもわかりません。場所的にも、先ほど御説明いたしましたように、ＭＤＦということになりますと、ビルがたくさんありまして無人の場所だとかそういったこともありますので、そういった意味で立ち会いにつきましては、コスト面、それから稼働面で当然負担が出てくるだろうと思っております。

ですから、これはどういう状況になるか今はわかりませんが、電気通信事業者にとりましてコスト面や稼働面で過度の負担にならないような運営をしていただくように、法案が成立いたしましたら関係機関にお願いしたいというように思っております。

○参考人（桑折恭一郎君）　先ほどから移動体の事柄について申し上げておりますけれども、私どもとしては、まず今回の法案が成立した段階でその趣旨にこたえる技術的な問題がどういう形で解が出るのかということをまず検討するということが第一だと考えておりまして、立ち会いというのはある程度その辺のめどがついた上での事柄だと思っております。

正直申し上げまして、きょう時点では立ち会いに関してどういう見解かというところまではまだ私どもとしては考える段階になっていないというふうに考えております。

○福島瑞穂君　どうもありがとうございました。

○中村敦夫君　中村敦夫でございます。

参考人に質問する前に、先ほど世耕議員から、先日の法務委員会で述べた私の発言及び朝日新聞の記事が間違いであるから世耕議員に対するあいさつが一言欲しい、そういう御発言がありましたので、御希望どおりあいさつします。

世耕議員の先日の発言の内容を考えますと、まず一つは、アナログ回線の場合は実際上ＰＴＴは難しいということを言っているんですね。これは困難だということを言っています。実施するにしてもＮＴＴの全面協力が必要だと。しかも、そういう場合ＮＴＴの協力はあり得ないんだというふうな文脈のお話だったと私は受け取っています。

ということは、私は道義的な問題ということを言っているのではなくて、やる気になれば技術的にそれが可能かどうかという問題を言っていたわけです。困難である、不可能であるということとはまた違うわけでございます。そういう意味では、ＮＴＴ自身が法務委員会に提出した「電話及びＩＳＤＮ回線における通信傍受」というところで技術的には可能だということをはっきり言っていますし、今の福島議員の質問に対しても、純技術的には可能だけれどもさまざまな事情とか困難さでできないというふうにお答えになっているんだと私は思います。ですから、問題のとらえ方が違うというふうに私は感じております。これがごあいさつです。

それで、早速質問に移りますが、お二人に同じ質問をしたいと思います。

さきの法務委員会で、私の質問に対して、法務省は警察施設での盗聴は法的にはできないんだというふうに答えておるわけですね。一〇〇％できないというふうな答えなんですね。ですから、わかりました、これは法的にはできないとして、また純粋に技術的なことをお聞きしたいと思うんです。

協力義務が法案の第十一条にありますけれども、そういう形で全面協力するという、例えばそういう形になった場合の技術協力の面についてなんですけれども、通信事業者の施設と外部の施設などをケーブルなどの専用回線でつなぐというケースですね。そうした場合、施設の外部から電気通信設備をモニタリングするということは技術的に可能なんでしょうか。専用回線の場合をお答えいただきたいんですか。

○参考人（森下俊三君）　先ほど御説明いたしましたが、アナログ電話の場合は、この試験制御装置を専用線で引っ張り出しても、要するにモニター状態にいたしますと着信ができない、技術的にできないということをお話ししております。

それから、先ほどごあいさつのときにありましたが、朝日新聞の記事にＰＴＴと書いてありますが、これは技術的にできないということであります

して、全面的協力が得られればできるということは全くの誤解だというように思います。技術的にＰＴＴそのものがモニターできないのでありまして、そこはこの書いてある内容が間違っているということを言っているわけです。

ただし、ごく例外で、たまたまそのＰＴＴから割り込んだときに通話をしておればモニターできる。だけれども、それは偶然割り込んだときに、通話していない限りはモニターできない。あらかじめセットしておいて待ち受けても通話はもうかからないということを何度も言っているわけです。基本的に何回やるといっても、それはどうやってやるのかということです。要するに、もう交換機の方でここは使っているという状態になっているわけですから接続できないわけです。

○中村敦夫君　そうなりますと、この法務委員会に提出した資料、これはなぜ識別可能というふうに断言しているんですか。

○参考人（森下俊三君）　いや、間違っておりません。そこはよく読んでいただくと、デジタルの場合とアナログと分けてあると思います。アナログは発信はできますけれども着信はできませんと書いてあるはずです。ＰＴＴのことではないんです、それは。試験制御装置のことです。

○中村敦夫君　はい、わかりました。

Ｊフォンの場合は今の質問はいかがですか、専用回線という。

○参考人（桑折恭一郎君）　今の法案にのっとって、どういう形での傍受が技術的に可能かということかある程度詰まった段階で、それがまたうまくシステム上、こういう形でやればできるという回答かできた段階では基本的に専用線でやるという解はあるかもしれませんけれども、私どもとしては、まずそれ以前の段階として、どういう形でそういう情報がとれるかということと、その情報が本当に目的とされる情報であるかどうかということをどこまで私どものネットワークとして保証できるのかということの面で非常に難しさがあるかと思います。

それと、先ほど言いましたように、数百回線の中から特定していくという作業自体は、これは私どもの専門家でも本当にうまくできるのかどうかという非常に不確定要素もございますので、専用線をやったことですぐ目的に沿うような形のものができるかどうかということについては非常に疑問な点があるかと思います。

○中村敦夫君　それでは、同じようなケースですが、通信事業者の施設と外部の施設などをケーブルなどではなくて携帯電話でつなぎ、施設の外部から電気通信設備をモニタリングするということは技術的に可能なんでしょうか。お二人にお聞きしたいんですけれども。

○参考人（森下俊三君）　ちょっとイメージがわかないんですが、今の御質問は試験制御装置の内容を無線回線といいますか携帯電話の回線につないで携帯電話で受けるというお話でよろしいんでしょうか。

○中村敦夫君　はい、ケーブルじゃなくて携帯電話で。

○参考人（森下俊三君）　原理的に考えますと、その回線を携帯電話の回線に乗せてやるということは可能だとは思います。原理的には可能だと思います。

○参考人（桑折恭一郎君）　もし専用線で結んで意味のあるまたは技術的にも問題ないということがある程度答えとして出た段階では、携帯か専用線かということについては技術的には全く差異はないと考えておりますので、そういう形ができたとした場合には携帯でデータ伝送をやるという方式も専用線と同様だと考えていただいていいかと思います。

○中村敦夫君　そうすると、純技術的には可能性があるというお話だと受け取ります。

森下参考人にお聞きしますけれども、けさの日経新聞なんかでも、日本でもやっとインターネット銀行を開始するという趣旨の記事が出ておりました。こういう状況の中で、ＮＴＴでは、例えば暗号技術に関して捜査のために必要であれば当局にすべての開発情報を提供するというふうな形になるとお考えでしょうか。

○参考人（森下俊三君）　先ほどＩＳＤＮの回線でお話ししましたが、傍受をするところでデジタルの信号ですからブーンという音しか聞こえないというお話をいたしました。基本的には今回の傍受という意味での協力は私どもはそこまでだろうと思っておりまして、中身は私どもの義務には入っていないというように解釈しておりますので、どういう信号、中身なのかは私どもは関与しておりませんし、それを解明するようなものを私どもがつくるという考えも今のところはございません。

○中村敦夫君　そうすると、例えば暗号技術に関しては協力を求められてもできないということなんでしょうか。

○参考人（森下俊三君）　ちょっとよくわからないところがあるんですが、暗号技術そのものはいろんな暗号技術があって、ＮＴＴが開発したものについてはこういったものだという技術的な説明はできると思うんですが、ただ実際の回線でどういう形でそれが使われるか。実際は暗号といいましても暗号は多分その発信した一つの通話ごとに変わっていくわけでしょうから、そういった意味では原理はわかってもそれをどうやって傍受するか、傍受したものを暗号解読するかということは、またそういうものを開発しないといけないということになると思いますので、そういった意味では私どもの傍受というのはそこまで含まれていないというふうに理解しております。

○中村敦夫君　質問を終わります。

○委員長（荒木清寛君）　以上で午前の参考人に対する質疑は終了いたしました。

両参考人に一言御礼のごあいさつを申し上げます。

本日は、御多用のところ貴重な御意見をお述べいただきまして、まことにありがとうございました。当委員会を代表いたしまして厚く御礼申し上げます。（拍手）

午前の審査はこの程度にとどめ、午後二時まで休憩いたします。

午後零時四十分休憩

午後二時開会

○委員長（荒木清寛君）　ただいまから法務委員会を再開いたします。

休憩前に引き続き、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律案、犯罪捜査のための通信傍受に関する法律案及び刑事訴訟法の一部を改正する法律案を議題とし、参考人から御意見を伺います。

午後御出席をいただいております参考人は、東京インターネット株式会社上級顧問髙橋徹君及びニフティ株式会社取締役サービス企画統括部長代理本名信雄君でございます。

この際、両参考人に一言ごあいさつを申し上げます。

本日は、御多用のところ当委員会に御出席をいただきまして、まことにありがとうございます。

両参考人から忌憚のない御意見をお聞かせいただきまして、今後の審査の参考にいたしたいと存じますので、どうぞよろしくお願い申し上げます。

議事の進め方でございますが、まず髙橋参考人、本名参考人の順にお一人二十分程度ずつ御意見をお述べいただきまして、その後、各委員からの質疑にお答えいただきたいと存じます。

なお、念のため申し添えますが、御発言の際は、その都度、委員長の許可を得ることとなっております。また、各委員の質疑時間が限られておりますので、御答弁は簡潔にお願いいたしたいと存じます。

なお、参考人の意見陳述、各委員からの質疑並びにこれに対する答弁とも着席のままで結構でございます。

それでは、髙橋参考人からお願いいたします。

○参考人（高橋徹君）　高橋でございます。

それでは、私は、インターネットから見た通信傍受法の問題ということをお話しさせていただきたいと思います。

私自身のことを申し上げますと、十五年前からインターネットのユーザーでございまして、一九八七年、十二年前には日本で最初のインターネットのための機器を扱うようなビジネスをしてございます。

それから、インターネットの調査研究をずっと年ごとに行ってまいりまして、その結果を通産省に提供したりしておりますが、九四年には東京インターネットという会社を設立しまして、これが大手のプロバイダーになった、インターネットサービスの提供者として、特に専用線のユーザー、企業ユーザーに対するサービス提供会社としては最大のものになったことがございます。その資格としてございますのは、特別第二種の電気通信事業者という資格でございます。

その間、ずっとインターネットの普及発展に貢献してまいりまして、九七年に日本インターネット協会の会長を務め、現在でもそれを務めておりますが、九八年にはアジア・パシフィックのネットワークインフォメーションセンターの議長を務めております。そのほか、国際のさまざまな役割を負っているという状態です。

改めてインターネットとはということを申し上げますと、世界じゅうのコンピューターネットワークがたくさんございますが、これが相互に接続された世界大、要するにグローバルスケールのネットワークとしては唯一のものである。ア・ネットワーク・オブ・ネットワークスというふうに言いならされております。

相互に接続されたという意味合いは、それぞれの単位のネットワークというのがございまして、それぞれが接続の責任を負うという形で、自律統治、セルフガバナンスというのがインターネットの成り立つための原則となっております。あくまでもインターネットはセルフガバナンスということによって成り立つものであるというのが原則的な考え方としてございまして、そのためには、世界じゅうで共通の通信手順を使う、これをＴＣＰ／ＩＰというふうに言っております。

ちょうど三十年前、一九六九年に米国の国防総省のお金をつけたプロジェクトで学術研究用のネットワークが始まりまして、それから三十年たちました。その間、学術用から商用への展開というのがございまして、商用のインターネットというのが米国では十年間の歴史を持っているわけです。日本ではまだ、九二年の末から商用のインターネットが始まったということで、それでも七年になるということになります。

インターネットの技術といいますのは、情報を小包、パケットにして送受信するコンピューター制御の技術というふうに言ってしまえば非常に単純ですが、これをパケット通信技術というふうに呼んでおります。情報を蓄積するコンピューターをサーバーと言いまして、サーバーにユーザー側のコンピューター、これをクライアントというふうに言ったりしますが、ユーザー側のコンピューターからサーバーにある情報をアクセスして情報の送受信を行うということになります。

住所、氏名がないと送ったり受け取ったりはできないわけで、住所がアドレスという番号になっておりますし、氏名の方はドメイン名ということで、これははっきり名前をつけるということになっております。住所、氏名をつけることによってインターネットも初めて情報の送受信ができるということになります。

送受信のための通信回線というのはもともと専用線、つまり電話線ではない、インターネットのためだけに使われる、データ通信のためだけに使われる専用線というのが主でありまして、それがなかなか高い、それによってなかなか普及が阻まれているということがあるために、電話線が補助として使われているというのがもともとの考え方です。インターネットの発展というのは専用線をベースにして発展してまいりました。個人ユーザーは大体電話線を使って成り立っているというのが現状です。

そういう中で、セキュリティー技術というのが非常に発達してきまして、これは軍事技術としてのセキュリティー技術も含めまして、特に商用化の発展する中でセキュリティー技術がそれぞれの企業に必要になったということで非常に発達を遂げてきております。

インターネットのメディア特性ということを申し上げますと、今申し上げたサーバー・クライアント型といいますか、大きなコンピューターとそれにアクセスするユーザー側のコンピューター、その対応関係が世界じゅうに散らばっているんだということで、サーバー・クライアントの自律分散環境というふうに申しております。

そういう中で、クライアントとクライアント、つまりエンドユーザーとエンドユーザーが相互に通信できるということを保証しているのがインターネットの仕組みでございます。これがグローバル、つまり世界大という形で発展しているわけなので、どうしても国権の範囲を越えるような越境する性格というのがあります。ボーダーレスの世界というのがそこで生まれてまいります。そうすると、さまざまな問題がそこで出てまいりますが、国権の範囲を越える国際協調というのが非常に重要な問題になってまいります。

それから、一対一だけでなくて、特定多数への通信が同時に可能になっております。これをマルチキャスティングというふうな言葉で呼んでおりますが、一対一の通信だけにとどまるものではないということです。そういう意味では、インターネットプロトコル、ＩＰというふうに言っておりますが、この上で音声、動画、静止画を扱えるようなマルチメディア通信が可能であるというふうになっております。今後、このマルチメディア通信がどんどんインターネット上で発展するものだというふうに考えられております。

それで、インターネットのシステム管理というものの特性を申し上げますと、サーバーの管理者の権限が非常に大きい。これをルート、一番根っこという意味でルートというふうに言っております。ルートの管理者になりますと、ユーザーに関する情報がある程度まで把握できる。これは、暗号化などがかかっていないような場合には細かな情報までほとんど見ようと思えば見られるようなぐあいになっています。ですから、非常に責任が重たいのがサーバーの管理者ということになります。

こういうネットワークの運用管理者というのは、現在、日本ネットワークインフォメーションセンター、ＪＰＮＩＣという社団法人のもとで管理されておりますが、ネットワークの運用管理者は必ずＪＰＮＩＣのデータベースに登録しなければならないということになっております。そういう意味では、運用管理者相互の協力というのが発達せざるを得ない。ますますインターネットが発展するのに対して、運用のための技術者というのが不足してまいります。大手のネットワーク企業の技術者というのはほぼどこにだれがいるかということはわかっているわけです。だから、ますます相互協力が発達するということになります。

それから、インターネットカルチャーということを申し上げますと、非常に特徴がございますのは、多数決原理で物事を進めていくわけではない。つまり、どの技術がすぐれているかということを多数決で決めたりはしないということがあります。技術を多数決で決めるなんというようなことは考えられもしないことですが、まず実質を重視するということです。

それから、ラフコンセンサス・アンド・ランニングコードという考え方がありまして、要するにラフな、大ざっぱなコンセンサスがあればあとは現場でもってどんどん詰めていくべきであるというふうな考え方です。それから、ランニングコードというのは、現実に動いているプログラムを重視しましょう、こうあるべきだ、あああるべきだという議論が重要なんじゃなくて、実際に動くものが必要なんだと。実際に動いて役に立つものと

いうことです。細部まで決めないで実態に即した考え方というのがインターネットの考え方になります。

さらに、オープンシステム、オープンリソースということを言っておりまして、一企業がつくり出したものに取り囲まれるということが全く必要ない。どの企業もみんな同じシステムを持っていて、それが相互に運用できるような、そういうものとして存在するというのがオープンシステムですが、そういうオープンシステムの原理というものを守っておりまして、それからオープンリソースという一番もとになるプログラムであるとかソフトウエアというものをどんどん公開していくという考え方があります。よいものはみんなが使っていけばもっとよいものになっていくというそういう考え方です。

この辺が、非常に新しい文化、カルチャーの問題を出していると思いますが、さらに、トップダウンよりもボトムアップか主流であるということになります。

それから、分散環境、さまざまなところにあるネットワークがそれぞれの危険負担というものをやらなければならない。そういう分散環境のもとで危険負担を行うために、それぞれのリスクというのは非常に少なくて済む、人に迷惑をかけないで済むようにしようというのが一番の考え方です。

それから、最近、インターネットソサエティーの方は、インターネットコミュニティーの標語としまして「インターネットは万人のために」、インターネット・イズ・フォー・エブリワンということを言っております。エブリワンということを言うと、老若男女あるいはディスエーブルの方々やいろんな人たちにインターネットは使えるようにならなければならないというそういう考え方が非常に強く押し出されてまいりまして、現在二億人のユーザーがいる世界のインターネットが、本当に六十億のみんなの手に渡るということを目標としております。

片や、商用インターネットというのがどんどん発達してきまして、郵政省の発表ですと国内で千七百万人がユーザーになったということでありますが、一九九四年からの発展が非常に急激です。これは本当に急激過ぎるほどの発展を遂げていまして、その中で、学術用途や商業用途というふうなことを限定しない、何でも使っていいんだというふうなことがどんどん言われて、そういうビジネスが発達してまいりました。そういう中では、誤用、悪用、アビューズというふうに言ったりしますが、そういうものも生まれてきております。

それから、その悪用の中には、この世に存在するさまざまな犯罪の要素がインターネット上に入ってくるということもございます。商用のインターネットは非常に急激なスケールの拡大を必要としておりまして、ネットワークのスケールも拡大しているし、トラフィックもどんどん伸びているということに対して対応しなければならないという、いつも追いかけられている状態です。

それから、商用のインターネットの時代になって初めて自律統治をさらに拡大しなければならないというインターネット全体の管理組織の問題が非常に大きく浮かび上がってまいりました。現在、国際インターネットの世界ではＩＣＡＮＮ、インターネット・コーポレーション・フォー・アサインド・ネームズ・アンド・ナンバーズという非営利の民間の組織、これをインターネットの管理組織として成立すべきであるという議論がこの三年間ほどずっと続いてまいりまして、ことしの秋にはこれが成り立つということになってまいります。日本の政府からもここには代表が出ていたり、日本全体の代表というのもボードメンバーに入っております。そういうことをつくっていく過程に現在我々は直面しているという状況があります。

さて、インターネットの犯罪というのも、これもいろいろございますが、これに対する対応というのをインターネットのコミュニティーはずっとやってきております。

まず、不正アクセスに対応するということというのは、不正アクセス防止法というのも検討していただいておりますけれども、要するに迷惑な通信を防止しようということから始まっております。スパムメールであるとかメール爆弾であるとか、いろいろ悪さを仕掛けてくるようなことがありますが、そういうことをまず防止しよう。

そのときに我々はどういうふうにやるかといいますと、まず通信の経路、どういう道筋をたどって通信がやってくるのか。それと、あて名、差出人というものを調べます。また、通信の経歴というのがサーバーに保存されている場合がございますので、通信の経歴を記録したものを調べる。その結果、この不正なアクセスがどこから来たかということを管理運用の担当者の間でもって連絡をとり合って、おたくのユーザーにこういうのはいないだろうかということを打診していって相手を特定することがあるいは可能になるということがあります。

そういうことを自律的に常時行っておりますが、それがはっきりした場合にはユーザーに警告をする。もともとインターネットのプロバイダーとユーザーとの間には、公序良俗に反することを犯したようなユーザーに対しては使用停止処分を加えるというふうなことが最初の約款に明記されております。その約款に従ってそういうことを排除していくということをやってきています。

この間、商用のインターネットがどんどん発展して以来、この五年間にわたって警察には随分協力をしてきておりまして、その結果、非常に高い検挙率であるということか語られております。

さて、現在問題の大規模組織犯罪となりますと様相は多少違っておりまして、犯罪組織がインターネットを使うということになりますと、これはもうはっきり意図した形で名前を偽ったり匿名性ということを駆使したり、それからさらには暗号化を駆使するということが考えられます。そうなりますと、一般の傍受では解けないメッセージがふえてくるだろう。これを防止するためには非常に高度な技術力を要することになります。それからさらに、ＯＥＣＤやＧ７などで議論されているような形で国際協力が必須になってまいります。

現在の法案の問題点というのを簡単に申し上げますと、一般に現在の電気通信事業者としてインターネットのサービスを提供している者にとっては、通信の秘密を保持しなければ事業が成り立ちません。これがユーザーとプロバイダーとの間の契約の関係になっているわけです。それは、電気通信事業法によって絶対的な前提としてこれを与えられている。

これを覆すということになりますと、電気通信事業法の建前というものが全く違ってしまうんじゃなかろうか。通信の秘密を保持しなければならないということを非常に強く、これは憲法でも電気通信事業法でも言われておりますが、その前提を覆すということがどういう影響を与えていくのかということがよく見えない。その前提を覆すおそれというのがあるということです。

それから、ユーザーのプライバシーを侵すというおそれがあります。これは、特定の犯罪組織が特定のメールアドレスでもって電子メールのやりとりをしているということが確定していれば、そのファイルだけを抜き出すということは可能かもしれませんが、リアルタイムあるいはそれに近いような形でもってファイルを見ていくということは非常に難しい。そのほかのユーザーに対する迷惑が非常にかかりやすい形になります。迷惑がかかるということは、要するにほかのユーザーのプライバシーを侵すおそれがある。

犯罪者同士の通信ということを確定することは難しいわけですから、ほかの人たちのプライバシーを侵すような形で相互の通信を見ないとこれはわからない。その結果としてユーザーとの信頼関係を損ねるおそれがありますし、一たん信頼関係を損ねた場合にどういうふうにしてこれを修復できるのかという、修復の保証をだれもしてくれないんじゃないかということがあります。

それから、プロバイダーが立ち会うということにも問題がありまして、技術者が機密事項に関与せざるを得なくなってまいります。これは技術の人たちが一番嫌っている、技術者のカルチャーにとって一番嫌なことだということがよく言われます。

それから、三年ほど前にテレコムサービス協会から大規模組織犯罪の防止についての傍受について意見を求められまして意見書を出しておりますが、これがうまく今回の場合に反映されているんだろうかということが改めて問題になります。

その三年前の時点と今の時点というのは、また運用技術のレベルが上がってきておりまして、通信の傍受ということをする上での運用技術の発展というのが、傍受のための運用技術じゃなくて運用技術一般の発展があって、そのことを十分に検討しなければ通信の傍受ということもなかなか難しいんじゃなかろうかと思います。

今までいろんな形でプロバイダーとかインターネットコミュニティー全体が犯罪捜査に協力してきているというふうに私は考えておりますが、現在の運用技術のレベルから見て十分な検討がないままに進めるということがなぜ行えるのか、これが非常に疑問でございます。

警察の捜査技術というのは、そういう意味では信頼し得るものでないといけない。信頼し得るものではないということを言うインターネットコミュニティーの人々も多々ございます。それが信頼し得るものであるためには、インターネットコミュニティーと捜査技術に関する協議機関というのが必須ではなかろうか。外国ではＣＥＲＴ、コンピューター・エマージェンシー・レスポンス・チームとか、それからＦＩＲＳＴ、ＦＩＲＳＴというのはフェデレーション・オブ何とかという、いろんな産業界、いわゆる各企業と学術、それから政府の機関も入ったようなそういうコンピューターネットワーク上の事件に対する協議機関というのがあります。そういうことが既に持たれている国々というのがあるのに対して、現在の日本には何もございません。一度、ネット上の犯罪の未然防止のための技術フォーラムというのを警察庁が二年間ぐらいにわたって開いてくれたわけですが、それは現在はもう存在していないということかあります。

本当にその技術検討をやらないままに進んでいきますといろんな間違いが起きそうな感じがしますので、ここで十分な御検討をいたきたいというのが私たちの願いでございます。

以上、私の見解です。

○委員長（荒木清寛君）　ありがとうございました。

次に、本名参考人にお願いいたします。本名参考人。

○参考人（本名信雄君）　ニフティの本名と申します。

それでは、通信傍受に関する法律について、私ども商用プロバイダーとしての対顧客に対する役務の提供ということを大前提とした形でもって、今回の傍受法の施行についての問題ということで述べさせていただきます。

私ども、商用サービスというのは、あくまでも利用者が日々使うサービスを円滑に、またトラブルなく提供する環境を第一の役務として考えております。こういった観点から、こういった法律が施行されて、実際、傍受という形でもってそれが実行されるときに起こり得る問題点という形でもって、まず最初に通信傍受のための機器の接続等に協力することによって我々が提供しているサービスのパフォーマンスの低下、それからあってはならない障害が発生する、こういったことは絶対許されない。特に、大規模なデータの流れの中から送信あるいは受信されるメール等の通信内容をリアルタイムに取り出して、それをチェックするということ自体は現在の技術からすると非常に非現実的と言わざるを得ません。

傍受というその行為自体をリアルタイムモニタリングという形でとらえるならば、実際こういった電子メールサービスと記録通信、蓄積された文書をある時点でもってほかへ流す、こういった形でのサービスの中では、傍受という概念よりも、従来その文書ないしはそのサーバー自体を差し押さえるといった形での運用の方が現実的ではないかというふうに思われます。

今言ったリアルタイムモニタリングというのは、システム的な負荷が非常にかかりまして、その対象となるものをスポット的に取り出すというのが非常に難しくて、そのサーバーに流れ込んでくるすべての通信をくまなくウオッチしなければいけない、それは人間の目では到底できるようなことではありませんので、当然何らかのプログラムを組み込んだ形でもってそこを抽出しなければならない、そういったような構成が考えられます。そうすると、必然的にその作業をするためのべつ幕なしにそのプログラムが動いているというところでもって、実際サービスを展開していくサーバーなのかモニタリングをするサーバーなのか、本末転倒という形になってしまいます。

こういった流れの中でもって、プロバイダーといえども大きなものから小さなものまで、極端に言いますとインターネットプロバイダーのビジネスというのはそれこそ数人規模で行える事業です。そういった大小のプロバイダーの格差、そういったものと、それから捜査対象範囲、こういったものを勘案しながら実行しないと、私ども大規模なプロバイダーほどそれに庄力する部分が大きくなってきて、それでもって必要以上の費用、それから必要以上の労力の負担をしなければならない可能性が出てくるというふうに考えます。

それから二番目に、この法律の目的、趣旨を逸脱した通信傍受が行われた場合のことなんですが、利用者の通信の秘密及びプライバシーの侵害のみならず、インターネット自体、一くくりに言うとコンピューター通信、データ通信という流れの中でもって行われている行為なんですが、単なる通信という手段だけではなくて、インターネットの中ではこういったデータ通信という方法を通じて個々の表現ないしは思想をその中でもって主張していく、そういった傾向が非常に強くなっております。

こういった環境の中でもって、いろいろ使っていただいている利用者にとってインターネットが非常に住みにくくなる環境になるような、こういったことはぜひとも避けなければならない。インターネットの健全な発展が阻害されるおそれのあるような運用自体は望ましくないというふうに言えます。

次に、実際、傍受という作業をやるに際しての運用上の要望事項ということでもって、プロバイダーとしての意見を述べさせていただきます。

従来、インターネットのみならず、こういった電気通信、パソコン通信という形でもってデータ通信を提供している中で、さまざまな形でもって犯罪の捜査に絡むようなケースがございました。それを通じて見ますと、特に被害者が出たところが基本的にその捜査の窓口という形でもって、私どもプロバイダー事業を東京でもって展開しておりますが、全国からそういった捜査照会という形での照会がございます。今回のこの傍受という行為の施行に関してもさまざまな地域からそういった要請が出てくると思いますが、その際についても、全国で均一的な運用方針というものをぜひ確立していただいて、でき得れば運用マニュアル的なところをきちんと策定していただいた上で、それにのっとった形でもって運用していく。

それから、実際プロバイダーでいろいろな形でもって電気通信のサービスを行っておりますが、基本的にはインターネットというスタンダードの世界でもってその技術をベースにして行われているケースが多いのですが、個々のプロバイダーによってはいろいろな形でもってそれをアレンジしているケースがございます。そういった個々の事情を勘案した上でもし傍受という行為をするのであれば、事前に技術的な可能性とそれに対する手順について十分詰めた上でその実施が必要になってくると思います。

それから、実際、傍受に関連する捜査員の方

が、極端に言うとこういったサービス運用ないしはメールサーバーの運用に熟知しているとは到底思えません。そういった方々がどういう形でもって我々サイドに関与してくるかというのが全く今見えていない状況です。我々は、一体だれを相手にしてこういった技術的なディスカッションをすればいいのか、そういったところの組織的な受け皿というものがぜひ必要ではないかというふうに思っております。

それから、警察や検察サイドと同じように、実際、傍受を許可する裁判所の運用方針についても、徹底してそれをマニュアル化していく必要があるのではないかというふうに思っております。

それから、先ほども申しましたように、傍受の対象はデータ通信の中ではいろいろございますが、例えばリアルタイムに会話を交わすチャットというサービスもございますし、電子メールのように一たん蓄積されてからおのおののメールボックスないしは次のメールサーバーへ転送するようなそういったサービスもございます。ですから、そういったサービスの特徴をとらえて、何に対して傍受をするのか、その辺はきちんと押さえていただく必要があると思います。

傍受という行為自体がなじまないものに対しても傍受法案を適用すること自体が妥当かどうか。その辺は、従来やっている差し押さえによる捜査が可能な事案については極力差し押さえという形でもって対応していただいて、余分なシステム負荷をかけないような形での協力というのを我々としては望むところでございます。

それから、三点目にプロバイダーの協力義務についてなんですが、実際、傍受に対して協力を要請された場合、どういう協力まで踏み込んでやらなきゃいけないのかというのがよくわからないところでございます。

現段階で伺っている情報の中では、通信傍受用のソフトウエアの開発ないしはそれに必要な新たな設備投資はその協力義務のうちに含まないということですが、実際その傍受が可能かどうかは、使おうとしているソフトウエアがその中において適切に稼働できるかどうかの確認をしなければなりません。これは先ほども申しましたように、各プロバイダーごとにそういったサービスの提供形式というのは違っておりますので、汎用的な形でもって傍受に必要なソフトウエアをたとえつくったとしても、それが一〇〇％稼働する保証はございません。

したがって、プロバイダーにとってそういったソフトウエアが仮に傍受に必要な形でもってそこに設置されなければいけないという状況であるならば、やろうとしているそのソフトウエアがどういう性質を持っているものなのか、どういう環境で動くものなのか、それをちゃんと事前にその仕様を公開して、それに対応できるかどうかの判断が下せるような情報を与えてもらわなければいけないというふうに思います。

それから、実際それを我々のシステムの中に組み込む場合なんですが、そのソフトウエアを組み込むために、組み込むための権利を傍受者側、この場合は捜査側に与えることはできないというふうに考えております。

これは先ほど高橋さんの説明の中でも、そういったシステム設定をできる権限というのは、逆に言えばそのシステム全体をクラッシュさせることもできる権限というふうにとられます。ですから、そういった技術が伴わない捜査側にこういった権限を与えること自体、私どものサービスを継続していく上で非常にリスキーな形になっております。したがって、仮にこの傍受という形でもって捜査協力を依頼された場合には、必然的に我々プロバイダーの技術者サイドがこれに関与していかなければならないというふうに考えます。

こういったプロバイダーとして傍受に協力するための設定行為やその他運用に関する形での協力行為が、先ほど申されたように、電気通信事業法に照らし合わせてちゃんとその免責が担保されるような形での表記が望ましいというふうに考えております。

それから、仮に捜査当局が持ち込んだソフトウエアを私どものシステムにインストールしてそれを動作させた場合、それが原因でもってサービス等に重大な影響が出た場合、その補償についてどういうふうに国家が負担するのか、その点も明確にしてほしいというふうに思っております。

以上、私どもの陳述でございます。

○委員長（荒木清寛君）　ありがとうございました。

以上で参考人の意見陳述は終わりました。

これより参考人に対する質疑を行います。

質疑のある方は順次御発言願います。

○仲道俊哉君　自由民主党の仲道でございます。

参考人のお二人にはお忙しい中御出席いただきまして、大変ありがとうございました。また、直接関係のあります通信事業者の立場から専門的な立場で問題点等も指摘をしていただき、そしてまた非常に前向きな考え方の御発言をいただきましたことに、まず冒頭感謝を申し上げたいというふうに思います。

御承知のように、今回の組織的犯罪対策三法案は、これまで随分この場でも審議をし、約三十時間を超える審議をしているわけでございますが、この審議の中で明確になったのは、通信傍受法についての問題をどうとらえるかということ。

一つには、この通信傍受法案は盗聴法であるということで、通信の秘密が侵害されるんだという立場で最初から反対をされておるいろいろな意見の方もあるわけでございますが、今の発言のように、絶対に通信の秘密は守らなければならない、侵害されてはいけないんだという立場で、では、どのような方法なり、またどのように実際に通信事業者の皆様方との話し合いをするのかということで、私はきょうの参考人の先生方の意見は大変参考になったと思うわけでございます。

これまでの問題点の中で大体はっきりしてきたことは、通信の秘密は侵害されてはならないけれども、一つには憲法第十二条及び十三条に公共の福祉による制約を規定していることから、通信の秘密の保障も絶対に無制限ではないという、ここのところをどのようにとらえるか。すなわち、公共の福祉の要請に基づく場合には必要最小限の範囲でその制約は許されるのではないかという意見も今回の通信傍受法の中には大きなウエートを占めておるというように私は思うわけでございます。

ただし、この意見の前提は、警察官や立会人や裁判官等、この法案に関係する人たちをどう信用するかという、まずその前提に立っておるというふうに私は思います。過去の事例から、日本の警察官に対しては信用できないんだ、立会人が信用を置けないという前提に立てば、何一つこの法案は成立をしないわけでございます。

そういうことで、問題はどう信用するかということでございます。これは余談でございますけれども、警察官に対して一般的な人たちとしては余りいい感情を持っておる人はいないと思いますし、特に交通違反なんかを起こして切符を切られた人たちはこのやろうというような感情を持っておる人も多いわけでございますが、しかし私は、そういう個人的な感情でなくて、今この世の中の治安をどう守ってくれるのか、日本の警察組織の信頼感というのと個人的な感情とは別であるというように思うわけでございます。

いま一つ、基本的な人権、今このことを叫び、通信の秘密を守り基本的な人権が侵害されてはならないんだと言う人たち、そういう人たちも組織暴力や世の中の治安のためにすべて人権が優先するとは考えていないと思います。ここが今度のこの法案を考える場合に非常に大事なところです。

その証拠には、例えば今問題になっておりますオウムの問題です。オウム関連での地域住民の反対運動や、または麻原彰晃の子供が学校に転入する、この問題については実際には私はこれほど人権を侵しておることはないと思う。しかし、そういう人権の問題に対しても、やはり社会秩序を守り、そしてどう世の中の治安を守っていくかということについては、そういう人たちも今は目をつ

ぶり社会の治安を優先すべきであるということで、この問題を余り大きく取り上げていない点が見られるわけでございます。

そういう点では、やはり今度の通信傍受法案についても、世の中の治安と組織的な暴力、そしてこの通信の問題、また人権の問題についての、私はそこのところが大きな接点であるだろうと。そこのところをどういうふうに置くか、その接点の置きところかそれぞれ賛成、反対の人の考え方に分かれるんじゃないか、そういうふうに思います。

そういうことから、きょうせっかく通信事業者のお二人においでいただきましたので、コンピューター通信に関する傍受について数点お尋ねをいたしたいと思います。

まず一点は、先ほどからいろいろ御意見をいただきましたが、通信傍受法案による通信傍受の対象から以前インターネットやコンピューター通信を除外すべきであるという意見も一時ありました。これを除いてしまうと、このような通信が犯罪に用いられることを広く許してしまうことになりますし、このような通信手段の健全な発展にとっても決して好ましいことじゃないというように私は思うわけでございますけれども、お二人の御意見は、この基本的な考えについていかがでございましょうか。高橋参考人の方からひとつ。

○参考人（高橋徹君）　インターネットというのは現在の通信の一番基礎になってきておりますので、これによって社会全体のインフラが成り立ってくるという過程が進んでいるわけです。それを通信傍受法の対象から外すとなりますと、もともとの法案の意味というのはほとんどなくなってしまうんじゃないか。電話だけでやってくださいということであれば非常に私どもは楽ですけれども、多分これから先はインターネット電話というのが出てまいりますが、インターネット電話が現在のアナログの電話をはるかに超えるという形になっていきます。そういうことも含めて、インターネット及びデータ通信というのは対象になって当然だろうというふうに思いますが、ただ、現在の方法でもって対象にしても余り意味はないという考え方です。

○参考人（本名信雄君）　今、高橋さんからもお話があったんですけれども、電気通信全体を見ていると、データ通信と要するに通話と言われる従来音声でもって話しているこういった部分のトラフィックの比率がほぼ五〇、五〇の段階に来ておる状況です。少なくともこの二年ぐらいの間には、データ通信部分のトラフィックというのが全体の電気通信のトラフィックの中で六〇％、七〇％という形でもって比率的には逆転していくだろう。その中で傍受対象という形でもってこの部分を除外すると大きな穴をあけるというふうな認識がございます。

ただ、従来の通話を傍受するという、特にアナログ電話、現在ＩＳＤＮ、このレベルの傍受とインターネットの世界の中でもっての傍受という行為は全く異質だというふうに考えてほしいと思います。よく言われるスポットモニタリングというのは、このインターネットの世界においては全く非現実的な手法です。ですから、そういった技術的な背景を十分審議された上で個々の傍受に対する運用というのを、その方法を確立していただくことが必要じゃないか。現在の何ら私どもにとっては技術的な検討という側面が全く見えない状況でもってただやりますと言われても、ただ協力してくださいと言われても、では我々は一体何をするのといったのが正直な感想です。

それから、例えば電子メールの世界、とりあえず傍受というのは日本国内を念頭に置いてですが、先ほど高橋さんの方からインターネットの世界というのはボーダーレス、要するに国境のない世界だというふうなお話がございました。ですから、例えばメールサービスをアメリカのドメインで受けたらどうするの。イギリスのドメインで受けたらどうするの。オーストラリアのドメインで受けたらどうするの。それから、実質サーバーはどこか違うところにあるんですけれども、例えばトンガという国のドメインで受けた場合、ではその捜査に対する権限はだれが持つんですか。こういったメール一つをとっても、ドメインという概念を導入した場合、傍受の場所というのが一体どこにあるんですかというふうな素朴な疑問というのも出てきます。こういったような環境はインターネットの世界至るところにございます。

ですから、そういった環境それから技術的な背景を十分認識した上で、この傍受という作業を実際行うのであれば、そこを十分そしゃくした上で行っていただきたいというふうに思います。

○仲道俊哉君　大変参考になる御意見ありがとうございました。

実際にニフティや東京インターネットが一日当たりに扱うメールの数というのは大体何通ぐらいでしょうか。

○参考人（本名信雄君）　私ども、ニフティが取り扱っている一日当たりのメールの通数なんですけれども、会員の間でもって、要するに会員クローズの中でもって出すメールと、それから広くインターネット世界との間でもって行き来する、この二つの種類があるんですけれども、例えば会員間でやる場合には一日当たり約九十万通のメールがやりとりされています。それから、会員と外のインターネットの世界という観点で見ますと、発信する通数が大体五十万通、受信する通数が一日百七十万通、このぐらいの規模で実際に今運用しているところでございます。

○仲道俊哉君　東京インターネットの方はいかがでしょうか。

○参考人（高橋徹君）　最近、私は運用の方に携わっていませんので細かいことはわかりません。ただし、例えば流量として考えるわけです。今のニフティさんのようなメールの数というんじゃなくて、トラフィックの流量というふうに考えますと、東京インターネットが現在経験している流量というのは百六十メガというのがずっと一日じゅう流れているというふうに考えられます。百六十メガというのが平均値でもってずっと一日じゅう流れているというふうに考えれば、その流量を一メール当たりの量でもって割ったのが数として出てくるわけですが、ちょっと今計算できません。

○仲道俊哉君　そのメールの情報量は実際に何バイトになるのか、膨大な量であろうと思うんですが、聞いている素人にわかりやすく、例えばフロッピーディスクでは何枚分とか、また新聞では何日分というような形でもしわかれば教えていただきますと大変参考になると思うんですが。

○参考人（本名信雄君）　私どもが取り扱っている非会員と会員との間の流れ、例えば一日百七十万通のメッセージを現在ストアしていく容量としては、大体十七・八ギガバイトの容量が必要になっています。これをフロッピーに換算しますと、ちょっと私計算違いするかもわかりませんけれども、大体一日に一万七千枚ぐらいのフロッピーが必要になってくるというふうに思います。一万七千枚のフロッピーをパソコンでしこしこかけても一日ではとても処理できません。

○仲道俊哉君　そうしますと、個別のメールアドレス別になっているＰＯＰのサーバー以外の場所において特定の人物でのメールをピックアップすることは技術的には可能でしょうか。

○政府委員（本名信雄君）　現在、私どもが持っている技術で、例えばリアルタイムで飛び込んでくるメールを引っこ抜いてほかに蓄積するということ自体はできません。もしやろうとすると、一日のトラフィックのメールを、例えばここでありますと一日十七・八ギガバイト、これを全部一たんどこかのサーバーに蓄積して、その中から該当する部分をプログラムを組んでぶんぶん回して引き出すといった作業になってきます。それも来るか来ないかわからないようなメールを毎日毎日これをやるというようなことになります。

○参考人（高橋徹君）　今、本名さんがおっしゃったような形で、相当大きなサーバーを用意して、それを特定するための専用の機械として置いて、あちこちのメールサーバーの通過するものを全部検索するというふうなことをやるくらいの力があ

ればできるでしょう。それは恐らく、これは余りあれですが、中国政府がインターネットに対する規制を強めたりしていることはたまたまありますが、そういうときに考えている手法というのは、特定の単語が流れていくのをキャッチするということで大規模なサーバーを用意するというふうなことを言っているわけです。それと同じような手法は考えられないことはないです。ただ、それをだれのお金で用意してだれがやるのかということになると、全く当てがないということだと思います。

○仲道俊哉君　ありがとうございました。

おたくのサーバーを利用してわいせつな画像を提供する者が検挙されるということがありますが、どういうスタンスで捜査に協力するのか、また憲法が保障する表現の自由との関係はどう整理されておるのか、会社としてのスタンスをお伺いしたいと思うんですが、いかがでしょうか。

○参考人（高橋徹君）　先ほどもちょっと申し上げましたが、ユーザーとプロバイダーの間にはサービス約款というのが存在します。サービス約款の中にはどのプロバイダーも必ず、これは文言は違いますけれども、公序良俗に反した行為をユーザーが行った場合に、その使用権利を停止する、あるいは全く使用させないようなことを通告するということもあるというふうに書いてあります。

公序良俗ということがその場合に問題になりますが、これは解釈はさまざまで、いろんなプロバイダーの中では、たまたまアダルトコンテンツというのをたくさん持っているサイトではこれは緩いわけです。

それから、私が社長をやっていた東京インターネットの場合は、内容についてお客さんから相談を受けるようにしました。お客さんというのは、アダルトコンテンツを置きたいというお客さんに対しては、その中身をチェックして最初は見ましたけれども、後はそのお客さんの方がどんどん変えていけるわけです。どういうふうに変えたかということまではとてもフォローできません。そんなことはやっていられない。そうすると、最初に見て警告をするということはできるし、それからほかのユーザーからあそこに見苦しいものがあるというふうに言ってこられたときに、それも複数言ってきたときに初めて我々がキャッチしてその中身を見て、それで警告を発する。それでも何もしなければ、それは切りますよということを通告していくという話になります。そういう形でやっています。

○仲道俊哉君　おたくのサーバーを用いてもし薬物犯罪等が実行されている、そういう場合には捜査に対して積極的に協力をいたしますか。どうでしょうか、基本的な姿勢として。

○参考人（高橋徹君）　基本的にそれは日常的にやっています。警察から要請があるたびにそれに対応して、対応する人間がそこに存在しております。

○仲道俊哉君　ニフティに対してちょっとお聞きいたしたいんですが、おたくが提供している掲示板でわいせつ情報の提供や個人に対する誹謗中傷が行われた場合、おたくの場合は削除や会員資格停止等の断固たる処置をとっておられますね。その観点から、おたくのインターネットサービスを活用して組織犯罪を行う等の行為があった場合にはどういう対処をなされますか。

○参考人（本名信雄君）　基本的には高橋さんのところで運用されている基準と同等の処置をいたします。基本的に私どもは、役務提供の中でもって公序良俗に反しないということを前提にしてサービスの提供というのをうたっておりますので、これに反するようなものが発見された場合、それは私どもも、その部分の削除とか最終的には会員資格の剝奪とか、そういった形でもって対処しております。

○仲道俊哉君　私は、きょうのお二人の御意見をお聞きしまして、本当に大変参考になりました。基本的にはそういう通信事業者が公共の福祉または秩序のために崇高な精神を持って当たられるということが基本であろうと思いますが、我々といたしましても、ハード面で、先ほど意見も出ましたが、それに見合う対策がぜひ必要であるなということを十分感じたわけでございます。

きょうは大変ありがとうございました。

○海野徹君　参考人のお二人、大変ありがとうございます。民主党の海野です。

私は、インターネットと暗号についてお聞かせいただきたいわけなんですが、その前に、この通信傍受法案を理解するということで、現実問題としてどういうふうに理解したらいいのかなということで悩んでいる部分があります。

一つは、新聞等にも発表されておりますが、アメリカのEコマース、これは対前年比二・五倍、三百六十億ドルにもなっているという話がありました。日本でも二〇〇三年ほどに七十兆円を超えるのではないかという数字があります。確かにアメリカの産業政策というのはずっと変わってきております。一九六〇年からドルが非常に揺らいできたときからアメリカの産業政策は変わってきて、とにかくある意味では今金融技術とインターネット、通信技術を融合させてそれの覇権を握ろうというようなそういう戦略があるのではないかなと思います。

もう一つは、これは要人とか経済人を対象にしていると思われるんですが、エシュロンという存在があります。これはアメリカの国家安全保障局の下部組織というか協力機関といいますか、至るところでいろんなデータが盗聴され、解析され、分析され、非常に問題になっております。それで、アメリカ側から、ロシアあるいは中国へもこの協力要請があった。日本へも同じような協力要請があったんではないかなという前提がございます。

しからば、日本はどうするかといったら、日本はやはり物づくりとIT技術、情報技術を融合させてこれから二十一世紀経済はやっていかなくちゃいけない。そういう中で、インターネットの発展が阻害されてはならないということがあるものですから、その観点に立ってお伺いしたいわけなんです。

インターネット上の注意点というのは、やはり情報が勝手にコピーされたりリンクされたり、そういうことをしないことだと思っております。そこでお伺いします。

まず、技術的な問題をお伺いしたいんですが、電子メールのコピーをほかの場所へ転送することは可能ですね。お二人に聞きたいと思います。

○参考人（高橋徹君）　可能です。ほかの場所というのは、特定の場所に送ることは可能です。

○海野徹君　だから、転送先を例えば警察のメールアドレスに設定する、切りかえたけでユーザーが気がつかないうちに警察へ転送するというのは、これは可能ということですね。

○参考人（高橋徹君）　それは、その電子メールを把握できた人、まず途中でもって受け取ったということがないとこっちに持っていけないわけです。要するに、自動的にそれを設定してそっちへ持っていくということをやるためには、最初の設定のときにはまずこれがこうであるということを確定しないとできないわけです。それはできます。それを設定すればできます。

○海野徹君　わかりました。

それでは、インターネットへ接続するプロバイダーからの専用線を通信傍受するということは、これも可能ですね。

○参考人（高橋徹君）　専用線というのは、エンドユーザーとプロバイダーとの間の専用線ということをおっしゃるわけですか。

○海野徹君　いや、違います。インターネットとインターネットサービスプロバイダーとの専用線です。

○参考人（高橋徹君）　その場合には非常に難しいと思います。これは先般、法務省の方にも伺った話ですが、アクセスラインを越えたバックボーンのところで専用線を使っているのが普通ですから、そこのところで傍受するということはまず考えないというふうなお話を伺いましたが、それはもう本当に全く困難だと思います。バックボーン

のところで流れてくる情報の量というのは大きいわけですから、それはさっきの話にもつながるようなことで、よっぽど大きなサーバーというか管理するためのマシンがなければとてもできない話です。

○海野徹君　同じ質問なんですけれども。

○参考人（本名信雄君）　今、高橋さんからもあったんですが、上流へ行けば行くほどどんどんパイプが太くなって、そこを流れていく情報量というのは級数的にふえていきます。そこの部分をモニタリングすること自体が非常に技術的に難しい状況であります。たとえとれたとしても、ほんの断片的なものしかとれないんじゃないか。全体的な量からして断片的なものしかとれないような状況になるんではないかというふうに考えます。

○海野徹君　それでは高橋参考人にお伺いしますか、今大変大きな施設が整備されればという話だったんですが、私どもがいろいろ勉強させていただくと、予算があれば、数千万から大きければ数億という話なんですが、それさえあれば十分可能であるというような教えをいただいたんですが、その辺はどうでしょうか。

○参考人（高橋徹君）　それは実際にアメリカで行っておるのはそのくらいの規模の話だと思います。そういう意味では、できないことはないと思いますが、それが全部を覆うということはまず不可能です。ですから、特定したものについて場所を限定してやることはできないことはないと思いますけれども、すべてのトラフィックに対して調査をするということは、これは不可能だと思います。

つけ加えますと、トラフィックというのは今、年に少なくとも三倍に膨れ上がっています。そうすると、多分、去年のサーバーが今動かなくなってしまいます。そんなにスピードが速いわけですから、毎年毎年それにどんどんプロバイダーはお金をかけていますが、調査をする方がそれ以上のことをやらないととても間に合わないということだと思います。

○海野徹君　それでは、暗号についてお聞きしますが、まず質問の前提として、警察が暗号解析用の設備としてスーパーコンピューターや専用線など大規模な設備が用意されている、そういうことを仮定してみます。ある意味では予算を使って暗号解読用の設備を整えた環境であるということを前提として質問をさせていただきます。

お二人にお聞かせいただきたいんですが、メールを暗号化した場合、解読は技術的に可能ですか。

○参考人（高橋徹君）　一般に答えることは難しいわけです。どのアルゴリズムで暗号化したかということによって随分違いますし、それから暗号のアルゴリズム、暗号の論理、暗号をつくるための論理というのはどんどん技術が発展して変わっていきます。ですから、これは今あるものを今のレベルで共通にみんなかぎを持っているからそれは解読ができるというふうなことがあったとしても、現在のレベルでも既にさまざまなものが存在しています。そこには共通性は全くない。

ですから、何かのかぎを持っているからといってみんなを共通に読めるなんということは一切あり得ないわけですから、それぞれに独自なかぎが必要であるというのが現在の問題です。

○参考人（本名信雄君）　今も話があったんですけれども、暗号のアルゴリズムというのは非常に多岐にわたって存在しておりまして、商用ベースで運用されているもの自体もアメリカでは代表的な五つ、それから日本でもＮＴＴ初め各メーカーさんが独自の暗号のアルゴリズムを発表されています。

まず、暗号を解析する上の前提というのが、その暗号自体がどのアルゴリズムにのっとって暗号化されたものなのか、これを特定しなければいけないというその作業から入らなければいけません。

それから、暗号の解読競争みたいなもの、インターネットの世界の中においては頻繁にやられている一つのイベントみたいなものがあります。至近の例では、アメリカのＲＳＡという組織が暗号解読コンテストというのを最近やりまして、これは五十六ビットでもって暗号化した、要するにＤＥＳという手法でもって暗号化した暗号を解読してください、そういった暗号のアルゴリズムを提供した上でその解読競争というのがなされました。最近ではこの五十六ビットの暗号解析に五十六時間という記録が出ております。これはこのＤＥＳという暗号解析用に特化したコンピューターを使っての結果というところです。

多くの暗号アルゴリズムが、例えばこの五十六ビットは破られた、ではその上に暗号化するためのビットをどんどんふやしていきます。現在商用化でやられているケースとしてはほとんど百二十八ビットという形でもって暗号化されているケースが多い、ないしは百二十八ビットを売り物にして商品化されているものが多いといった現実を踏まえますと、まず解読は難しいでしょうというふうに考えます。

○海野徹君　それでは、もう少し一般的な例でお伺いしますけれども、ＰＧＰというのがございます。ＰＧＰをマニュアルどおりに使用して暗号化した場合、その場合のメールの解読というのは可能でしょうか。お二人にお聞かせいただきたいんですが。

○参考人（本名信雄君）　私はＰＧＰの提供者側ではないので何とも言えないんですけれども、現実、そのＰＧＰで暗号化された暗号メールはまだ破られていないというふうな実績になっています。ＰＧＰ自体は四つの暗号手法がありまして、四つか五つかちょっとはっきりしませんが、複数の暗号手法がありまして、そのうちのどの暗号手法を使ってやるにしろ、先ほど言いました百二十八ビットでもって暗号化するといった形になっております。

ですから、現実的な形での暗号解読というのは、理論上は可能であるかもわかりませんけれども、現実的にはほぼ不可能と見ていいのではないかと思います。

○参考人（高橋徹君）　ＰＧＰはプリティー・グッド・プライバシーという言葉の略ですが、これをつくった人たちはフリーソフトウエアのグループなわけです。フリーソフトウエアということを主張しているグループで、そのコミュニティーが中心になってＰＧＰというのを使ってきています。

そのコミュニティーの中で今、本名さんがおっしゃったように幾つかのパターンがあって、このパターンでもって私は使うぞと言って相手にかぎを渡しておけば、お互いに解ける関係というものを設定した上での通信ということが可能になるわけです。それを第三者が見て解けるかといったら、それは全く解けないというのが普通であって、それよりももっとＰＧＰが役に立っているのは、むしろ自分が自分であるということを証明するためのサインとしてＰＧＰが使われているということが一般的な使い方です。

ですから、商用として発達するというよりも、むしろコミュニティーの中のものとしてどんどん広がってきたというのがあるものですから、そのコミュニティーの中で使われる一対一の関係の中ではかぎは当然授受できるものだというふうに考えられております。第三者がそれを見てもわからない。

○海野徹君　私は、七月十三日の法務委員会で政府側に暗号技術の規制をするのかという質問をしました。そうしたら、刑事局長は、現在のところ規制は考えておりませんという話だったんです。しかしながら、その後いろいろな動きを聞いてみますと、ある省では暗号化を規制しようというような、あるいはそういう商品を開発させないというような動きをしているという情報が入ってきたわけであります。

答弁の方針がそのままずっと未来永劫に続くということは当然考えられませんから、政府による暗号の規制がされたようなときにインターネット上でどんな問題点が発生するのか。あるいはＥコマースの中でそれがどういうような影響を及ぼしていくとお考えですか。お二人にお聞かせいただ

きたいんです。

○参考人（高橋徹君）　難しい質問ですが、エレクトロニックコマースが発展する中で、どうしても企業のいわゆる機密の情報というのがやりとりされるわけです。特に、金額のやりとりをしているわけですから、それを書きかえられたりしたらたまったものじゃない。これは絶対に暗号化が必要であるというふうに現在なってきています。どういう意味合いでも、第三者にかぎを渡すということはまず考えられないというのがユーザーとしての実感だと思います。エレクトロニックコマースが伸びるためには、ユーザーが自分を守るための道具を極めて十分に持つことが必要である。それを助長することによってエレクトロニックコマースというのは発展するし、エレクトロニックコマースを筆頭としたインターネットビジネスというのがどんどん広がっていって、新しい世界経済の基盤になるのは目に見えている。

それに対して、暗号の規制をかけるということになりますと、まず暗号が第三者によって見られているかもしれないというのが規制という意味合いです。というふうに私は受けとめます。そして、第三者に見られているかもしれない、第三者が解けるかもしれないということを考えながら暗号化をどんどん進めるような人は世の中に存在し得ないと思います。その暗号のシステム自体を捨てなくちゃいけない。アルゴリズムを捨てて別のものを採用するということにどんどんなっていきます。そういうことが保障されなければ今のエレクトロニックコマースが伸びる余地は失われてしまいます。それこそ、技術の進歩に対して十分な保障を与えていくことが必要な話だと思います。

○参考人（本名信雄君）　暗号規制なんですが、アメリカでは一九九三年ぐらいでしたか、チップに埋め込んでそれをすべてのネットワーク機器に入れなきゃいけないなんという、クリッパーをベースにした暗号規制みたいな法案が出たんですけれども、袋だたきに遭って引っ込めたということで、現在、私は、最終的にどういう決着をしたのかわかりませんけれども、かなり規制的には緩くなって、キーリカバリーという方式でもって暗号化を規制しようといった法案がアメリカの中で動いているというふうに認識しています。

このキーリカバリーというのは、いざというときにそれを公共機関が使えるような形でのキーの管理方式というようなところでもって動いているんですが、暗号規制と例えば組織犯罪を同一に並べて考えること自体がちょっとナンセンスかなというふうに思います。

暗号規制というのはあくまでも汎用的な暗号方式を規制するものであって、例えば犯罪組織がそういった既存で流れているような暗号体系を使って、そんな抜け道があるような暗号を果たして使うのか。暗号のアルゴリズムというのはインターネットの世界では非常にたくさん流れておりまして、逆にこういった暗号をつくる技術者はインターネットの世界ではごろごろいる。そういった人間が特定の用途に沿ったような形でもって、アンダーグラウンドでもって暗号のソフトをつくってしまえば暗号規制自体が何の意味も持たないというふうに私自身は考えています。

○海野徹君　これで質問を終わります。

○大森礼子君　公明党の大森礼子です。参考人の方、きょうは大変にありがとうございます。

最初に、通信傍受法案そのものではなくて、インターネットの持つ問題点ということで少しお尋ねしたいのです。

インターネットが急激に広がりまして、先ほどの高橋参考人のお話でも急激過ぎる発展と、こういうふうな表現がございました。インターネットによりまして、Eメールの場合ですと特定多数の方に一度に発信できる、それからホームページですと不特定多数の方に自分の意思といいますか、これを表現して伝達することができる。これまで我々は、表現の自由というのはもちろん憲法上保障されて持っているわけですが、その表現の場というものがなかなかございませんでした。ところが、インターネットによりまして、特にホームページなんかを考えますと、自分の意思といいますか、伝えたいことを広く表現し伝達する場を得られたということで非常に画期的な発明物だなというふうに思うわけでございます。

ただ、そうしますと、先ほどインターネット・フォー・エブリワンという言葉も出ましたけれども、どんな便利な発明物であってもやはり光と影の部分があると私は考えます。

それで、今回はインターネットとの関係でも、公権力の通信傍受法案によるプライバシー侵害の点のみが強調されているような嫌いがあるのですけれども、私人によるプライバシー侵害ということも非常に大きな問題になってくるのではないか。あるいは一たん情報を流すと、流された人は後をフォローするといいますか、それをコントロールすることが非常に難しくなってくる。名誉毀損的な表現もあるかもわかりませんし、あるいは虚偽の風説の流布というようなことも起こるかもしれないわけです。

こういう一方で、性質上持つその危険性について、これはインターネットの業者の方が健全な発展を一方で望まれると、これを阻害するような性質のものが常につきまとうわけですが、こういう危険性についてどのように認識しておられるか、一般論としてで結構ですから、高橋参考人、本名参考人に順次お尋ねいたします。

○参考人（高橋徹君）　私人によるプライバシー侵害というのは、別にインターネットでなくてもしょっちゅう行われているわけです。何でインターネットだけが問題になるのかというところがよくわからないわけです。要するに、世の中にあるものがすべて、インターネットのユーザーがふえればふえるほど、インターネット上にあらわれてくるんだというふうに考える方が早い。インターネットをつくって発展させようとする意思を持ったインターネットコミュニティーの人間というのは、できるだけそういうものを排除しようとして今までやってきています。それを自律的な原理でもってやっていこうということに積極的に努めてきた、それ以上にその問題は起きています。

ただし、先ほども申し上げましたけれども、検挙率が非常に高い。それから、自律的な排除の原理というのが働いていますので、それによっておさまることも非常に多いわけです。それは、警察権力がそこへ介入するというところまで行かない場合でも、結構問題解決をやっております。一般的にはそういうことだと思います。

ですから、私人によるプライバシー侵害というのは日常茶飯事で一般社会には存在しているものであり、その一部がインターネットにも反映してきているんだというふうに私は理解しています。

○大森礼子君　本名参考人にお願いいたします。

○参考人（本名信雄君）　私人によるプライバシーの侵害、高橋さんと全く同意見なんですけれども、インターネットというのは基本的に人間が行っている日々の生活と全く一緒です。ただ、顔が見えない、声が聞こえないという物理的な制約というのがありますけれども、基本的にネットワークというのは単なる経路ないしは情報を運ぶための通路、その中で活動しているのはあくまでも人間で、機械が活動しているわけではありません。

ですから、人間によって活動されているフィールドというのは、当然現実の人間関係そのものを持ち込むというそういった状況にもあります。それが、今まであった日常生活の中では見えない人にまで見えてくるというのがインターネットの大きな一つの特徴というふうにとらえています。

○大森礼子君　私人によるプライバシー侵害、ちょっと言い方が悪かったかもしれませんが、例えば個人に関することを広く表現して伝達するというこういう意味のプライバシー侵害ということでございます。確かに人間の行っている行動の一つでありということなんでしょうが、その規模が非常に大きく違うということ、不特定の人にも情報が流されてしまうという、こういう規模において非常に大きく違うのかなという気がいたします。

それで、利用規約のことについて先ほど参考人が触れられましたけれども、インターネットのプロバイダーの利用規約には、多くの場合、犯罪に結びつく行為とか違法行為、公序良俗に反する行為等に利用することを禁ずる条項とか、そういう条項を実はプロバイダー側で削除することができるという条項が盛られているというふうに伺っていますけれども、これは統一的な条項、それとも個々のプロバイダーとユーザーとの間のことなのでしょうか。これが一点。それから、それぞれの参考人のところではどのような形でこういう約款が入っておりますか。簡単に教えていただければと思います。

○参考人（高橋徹君）　個々のプロバイダーによって違います。業界としましては、社団法人テレコムサービス協会というところでプロバイダーのためのガイドラインをつくっております。大体こういうことであるべきであるというのをみんなで相談して、それを出しています。

それから、電子ネットワーク協議会というのがありまして、そこでは倫理綱領というのを出しております。その倫理綱領の中で、あれをやってはいけない、これをやってはいけないということをいろいろ書いてございますので、それを越えたようなプロバイダーの約款というのは一般的にはまずないだろうというふうに考えます。

○大森礼子君　本名参考人、お願いいたします。

○参考人（本名信雄君）　高橋さんが述べたとおりです。

実質、公序良俗という範囲は、一応我々にとっては法律の中で表現されている範疇を示すといった形でもってとらえております。特に、我々自身がそれに基づいていきなりそのユーザーに対して罰則を加えるといった作業を行いません。そこに行き着くまでには過程がございまして、例えば先ほどの私人によるプライバシーの侵害みたいな部分ないしはネットワーク上でもって誹謗中傷が行われた場合には、とりあえず当事者間でもってちゃんと解決するようにまず私どもは勧めます。

仮に、その誹謗中傷の誹謗中傷する側が例えば私どもの会員であれば、当然そういった行為はやめなさいという形でもって勧告をします。それでもやめない場合については、その部分を強制的に削除します。それでも続けて同じような行為を犯すのであれば、その人の会員資格を私どものサービス上から削除します。そういった多段階の運用を経て、会員との間のサービスを使っていただく上での契約というのは成り立っております。

以上です。

○大森礼子君　そういうふうに自律的にというんでしょうか、利用規約によって取り組んでおられる。ですから、ユーザーの方も申し込む場合には、一定の施設についてはその利用について制約を受ける。場合によったらその使用を拒絶されるという、これを承諾した上でインターネットを使用していることになると思います。

インターネットの健全な発展ということですが、先ほど光と影と言いましたけれども、やはり便利な通信手段ができればそれを悪用する者が出てくる。電話でも同じなわけです。そしてその場合に、捜査手法というものが追いつかなくなったときに、その場合でも通信の秘密だということで一切こちらを制約はできないのかというところから今回の通信傍受法案というものが出てきたわけでございます。

それで、今利用規約等についてそういう規定があるということ、これはインターネットが犯罪とか違法行為に利用されて、その結果としてインターネットの健全な発展が妨げられること、これを防止しようとする意図も含むのであろうと私は理解します。

それから、インターネットは非常に自由な情報交換が可能な場であるわけですけれども、悪用して犯罪に関連する通信に利用するということは通信事業者の方にとっても本意ではないというふうに考えておりますけれども、その点いかがかということ。

それから、結局、一方で通信の秘密を保持しなければ事業が成り立たないという、非常にこれは大事なことだと思います。要するに、どこにその調和点を求めるかということに行き着くのではないかと思うのですが、通信事業者の方の立場から、悪用される場合については制約を加えるというこの点については御理解いただけるものかどうか、お聞かせいただきたいと思います。高橋参考人から本名参考人の順番でお願いいたします。

○参考人（高橋徹君）　今の御質問の最後の部分が少しわからないんですが……

○大森礼子君　では、言い直しましょう。

簡単に申し上げますと、通信の秘密、それから一応犯罪の防止といいますか、犯罪被害に遭うということ、これも一つの大きな人権侵害である、この調和点で今回の法案が出てきたわけです。そういう犯罪に対抗するため非常に厳格な要件と考えておりますけれども、もちろん令状に基づいてです。こういう法案の存在自体について、こういう制約の必要性については、範囲はいろいろあるかもしれませんけれども、通信事業者の立場においても御理解いただけるものでしょうかという質問です。

○参考人（高橋徹君）　通信事業者の立場からして、当然通信事業者の自律的な排除機能を超えるような場合というのが存在するということは知っておりますので、現在までも警察に協力してきた。それ以上のことがなぜ必要なのかは、今なぜそれが出てくるのかはよくわかりません。それも技術検討なしに。

○大森礼子君　本名参考人お願いいたします。

○参考人（本名信雄君）　従来からも、私どもプロバイダーないしはサービス提供者側というのは、その都度犯罪の発生に従って関連する警察等の照会があった場合についてはできる限り協力してまいりましたし、今後とも協力していく姿勢は変わりありません。

ただ、現行にある法律を、私も法律の専門家ではないのでよくわからないんですが、駆使することによって、実質、電気通信の中におけるこういった犯罪抑止、犯罪防止のための手法というのがとれるのではないかなという気はしないでもありません。ですから、傍受ということが、先ほど来言っていますように、リアルタイムモニタリングというそういった観点から施行されるのであれば、データ通信の中においてはちょっと難しいのかなというふうな感じがします。

ですから、そういう現実的な技術的な背景をやっぱり十分御審議いただくのがまず先決ではないかなというふうに考えております。

○大森礼子君　電話傍受の場合とこういうインターネットの場合とちょっと状況が違うと思うのです。本名参考人は先ほど捜索差し押さえ令状の方でできればやってほしいと言っておられましたけれども、確かに情報という形として残ります。ですが、この法案でも通信傍受というそれをリアルタイムでキャッチするというのは補充性というものを要件としておりますから、インターネットの場合にはそういう差し押さえですか、この方が多用されることにもなるのかなという気はいたしております。

それから、捜査機関との協議についてですが、先ほど本名参考人の方も、現実の場面で一体だれを相手に技術的なディスカッションをすればいいのかよくわからないという御意見をお述べになりました。それから、高橋参考人の方も協議機関が必要であるという、こういう御意見を述べられました。私もそのとおりであると思います。

それで、この協議につきましては三つの段階について考えることができるのかなと。統一的な運用マニュアルというんですか、これをつくる段階と、それから令状を実施する個々の場面について具体的にどうするかということと、それからそれに加えまして技術的なものも日進月歩で進んでいきますし、いろんな環境の状況変化があるかもしれない。そこで、定期的にまた協議するということも必要なのかなと個人的には思っております。

そこで、捜査機関側との協議ということについ

て、どのようなものを想定しておられるか、そしてどのようなものであることを希望されるかということをそれぞれ、まず高橋参考人から、続いて本名参考人の方からお聞かせいただきたいと思います。

○参考人（高橋徹君）　現実に今の日本にないものを想定して話をしているわけですが、今の協議機関というものが統一的な基準によってというか最低レベルのところは統一的な基準があってしかるべきであろうというふうに私は思います。

現実に起きてくる事件そのものは全部個々のケースによって違うわけですから、それは本当に何というか機密を保持する義務を負った人たち、当事者の中でもって議論されなくちゃいけない。それを一般に公開して議論するような話ではないだろうと思います。

協議機関とはいえ、例えばアメリカにおけるナショナル・セキュリティー・エージェンシー、NSAというのがありますけれども、NSAの人たちはやっぱりそういう機密の保守義務というのを必ず持ってやっているわけです。そういう人たちの中での技術の議論というのがなされなくちゃいけないわけですが、そういう機密の保守義務を持った人たちの中での技術のレベルというものを保証できるかどうかということが一番大きな問題になってくるんじゃないでしょうか。ただ、次々に新しい技術が出てくるときに、それをフォローできる人がそのグループの中にちゃんと存在し得るかどうか。

これはちょっとそれるかもしれませんが、韓国の場合は、インターネット上で悪いことをやったいわゆるクラッカーという人たちを収監して懲役に付すわけです。そして、懲役から出てきた人たちを全部警察が高給で雇い上げるということをやっているので、大変数が減っておりますという話を聞いたことがあります。

○大森礼子君　本名参考人、いかがでしょうか。

○参考人（本名信雄君）　私どもが考えている協議機関というのは、あくまでも技術サイドに立った形での実現性、信憑性を議論する場というふうにとらえております。ですから、法律自体の運用的なマニュアルの整備とか、そこへは毛頭タッチするつもりはございませんで、実際傍受が施行される段階でもってさまざま発生する技術的な問題をあらかじめクリアにしておくのと、先ほど高橋さんがおっしゃいましたように、このインターネットの世界というのは非常に技術的な進歩の度合いが激しい世界でございます。そういった世界についていけるような事業者、こういった傍受をやるに際して協力しなければいけない事業者と当局側との間でもってそういった技術的なディスカッションをする場というのが非常に急務に要るんじゃないかというふうに思っております。

○大森礼子君　今のマニュアル化という点については、御意見の中で、各都道府県警察や検察庁により運用に差が生じないよう、また恣意的な運用がなされないよう、全国的な運用方針の均一化が図られるべきではないかとありまして、この中においてもそういう御意見を反映することが必要なのかなと思いまして、申し上げました。

○参考人（本名信雄君）　時にはあるかと思いますが、全面的に関与するつもりはございません。

○大森礼子君　終わります。

○橋本敦君　きょうは参考人の皆さん、ありがとうございます。

最初に、高橋参考人に御意見をお伺いしたいと思いますが、基本的な問題として、事業そのものが通信の秘密を保持しなければ成り立たないという立場から御意見がございました。私も、今日の通信の国民的な発達あるいはグローバルな展開、そういったユーザーとの関係から見ても非常に大事な基本問題だと、こう思います。そういう中で、ユーザーのプライバシーを侵すおそれ、これが通信事業法でも厳格に決められているわけですけれども、この信頼関係を損ねるおそれがあるということこの問題が、捜査に必要だということで傍受が入るということで、一体その損ねるおそれを解決できる道はあるのだろうか。そこのところを私は大変疑問に思っているわけです。

例えば、電話の通話の場合には一秒間で五、六文字ぐらい、こう言われているんですが、電子メールなら六千ないし一万二千文字が流れていく、そういう通信が行われていくわけです。そういう通信の一体どこが犯罪関連性があるかということを膨大な通信の中から限定的にセレクトして傍受するということは、実際技術的に不可能ではないかという思いすらするんですが、そういう意味で、電話の傍受と違って、まさにインターネット関係のコンピューター通信についてはユーザーの皆さんのプライバシーを守るということ自体がもう基本的に難しいんじゃないかと私は思って心配をしておるんですが、高橋さんの御意見はいかがでしょうか。

○参考人（高橋徹君）　おっしゃるように膨大なデータの中から該当する場面だけを拾い上げるということはこれは非常に難しい。しかし、技術がそれを可能にすることはあり得るわけです。しかし、その技術を可能にするためには膨大な投資が必要であって、その投資も年々新しい技術あるいは交通量がぐんぐんふえていく、年に三倍になるわけですから、それを追いかけていくような投資が必要になってくる。これをだれができますかということです。国民がそこに集中してやるんだったら多分できるでしょう。そういうことが現実的には不可能であるということを意味するものだと思います。技術の方はできないことはないと思う。原理的にはできると思いますが、そういう意味ではユーザーのプライバシーを損ねるおそれということはやっぱり解決できないというふうに今の状況では私は見ざるを得ないと思います。

○橋本敦君　それとの関連で本名参考人の方にもお伺いしたいんですが、お話の中で送信あるいは受信されるメールにつきまして、これをリアルタイムで目視して抽出することは極めて難しくて、現実的でないというお話がございました。

私は、この問題も非常に大事だと思っておるんですが、それはこの法案に関連をして、いわゆるプライバシー侵害を最小限に減らすということからスポットモニタリングが電話通信傍受の場合には行われて、関連性のない通信を聞かないように最小化措置というのがとられるということが言われているわけです。これはアメリカあたりでもやられている。だから通信についてはなるほど最小化措置はできますが、インターネット、コンピューター通信については、お話がありましたように最小化措置そのものが働くということが技術的にどうしても現実的でないということが技術的にどうしても私は言えるんじゃないかと思うんですが、この点について本名参考人の御意見をもう一度お伺いしたいと思いますが、いかがでしょうか。

○参考人（本名信雄君）　先ほど来高橋さんの方からもお話があるんですが、技術の世界ですからやってやれないことはないというふうに思います。ただ、それをやるためには莫大な費用がかかってくる。そういったことを勘案してやった場合、果たしてその方法が適切かどうかという判断が一つ入ってきます。

仮にそういったことでもってできたとして、ある特定するものが目視でもってチェックしてこれが要るか要らないかというような、リアルタイムに流れる中でもってそのデータをチェックすることは人間の目では不可能です。ですから、一たんどこかへ静止させておいて、それを全文くまなく読んだ上でこれは関係ないという判断を下さなきゃいけないですね。ですから、スポットモニタリングというのは技術的にこの世界では不可能です。それを全文読んだときに、読んだということ自体は読んだ人の頭の中には残っているわけで、それが消去できるかどうかという技術的な問題も出てくると思います。

ですから、先ほど来言っていますように、コンピューター通信、特にインターネット社会でもって行われているこういったデータ通信を主体にしたそこの部分を傍受すること自体は、やっぱりまず技術の面から果たして妥当なのかどうかという十分な議論を経た上で、それでもいけるというの

であればそれはそれで実施すればいいんじゃないかなというふうに考えております。

○**橋本敦君**　現状ではなかなかそれは大変だというお話だと思うんです。

それで結局のところ、傍受ということで特定のプロバイダーの場所あるいはしかるべきところでメールを捜査員が見るということで、目で見て検証するということ以外に私はないと思うんですが、膨大なメールを結局全部見ないと犯罪関連性が特定できないというそういう状況になりませんか、実際の実務上の問題として。これは立会人の問題にも関連するんですが、そういう点の心配はいかがお考えでしょうか。

○**参考人（本名信雄君）**　犯罪でもって特定される個人が認識できるのであれば、そこの部分だけ抜き出すということ自体は可能ですから、ほかの全く第三者のメールを含めて読むというようなことはないとは思います。

ただ、電子メールの世界というのは、先ほど来お話ししていますけれども、例えばあるメールボックスへ送られたものをそのメールボックスの人がこっちへ飛ばせと言ったら無条件で飛んでいくわけです。ですから、そのメールボックスには何も残っていなくて、ただそこは中継しているサーバーだと。それが多段にかまされた場合、一体どこを追いかければいいんですかと。ですから、例えば仮に私どものユーザーさんがそういった状況でもってモニタリングの対象になった場合、ではそこのメールボックスを監視していましょうと。ただ、監視しているときには、その人は転送というファンクションを設定してほかのプロバイダーのメールサーバーへ飛ばしているということ自体で、そこには何も残っていないわけです。

ですから、百年待ってもそこには何も残ってこないという状況になりますから、そういったインターネットの世界のメールの仕組みというのも考えてどうすればいいのかということをやっぱり十分議論しないと、すべて空振りに終わるというようなケースもあるのではないかなというふうに思います。

○**橋本敦君**　本名さんは先ほどのお話の中で、通信傍受用のソフトウエアの開発、こういうことが一つは協力義務との関係で問題になるというお話がございました。その点については、この通信傍受を実際行うについて、そこまで民間の皆さんに協力義務を押しつけることは私は経費の点からいっても、またほかの問題からいってもとてもできないと思うんですけれども、プロバイダーのソフトウエアを設定することによって傍受する場合に、捜査当局にその設定を任せるわけにいかないというお話がございました。

そうなりますと、捜査当局に任せるわけにいかないとなれば、皆さんの方でおやりになる以外にないのかなと。そうなってくると、実際問題としてソフトの開発ということで必要な協力を嫌でもやらされるということになってしまわないかなという心配もするんですけれども、そこらあたり本名さんはいかがお考えでしょうか。

○**参考人（本名信雄君）**　そういう心配は可能性としてはありますので、そうならないようにお願いしたいというのが私どもの希望です。

○**橋本敦君**　それからもう一つ問題として、仮にプライバシーが侵害された場合に、国民の側から何らかの権利救済措置ということで問題が出ないという保証はないわけで、その場合に事業者の皆さんの方に、不当にプライバシーが侵害された、メールが不当に傍受されたということで損害賠償請求ということがないとも言えないと思うんですが、そういう場合の対応はどうお考えになっていらっしゃるかということが一つ。

それからもう一つは、本名さんのお話の中で、捜査当局が傍受をやる関係で持ち込んだソフトウエアの動作が原因でサービス提供に遅延、中断が生じた場合に、その補償を国がどう負担してくれるかというお話もございました。そういった問題はこの法案では両面とも全く触れられていないという点で私は欠陥がある、こう思っているんですが、そこらあたりについてはどういうようにお考えでしょうか。その御心配の向きですね。

○**参考人（本名信雄君）**　私どもが傍受に協力することによって、仮にその傍受対象者から、その人は全く関係なかったといったところでもって何らかの損害賠償請求を受けるケースは当然考えられます。今回の私どもに提示していただいたこの法案関連の条文の中には、その辺の免責とか担保とかそういったところが全く記されていないので、心配は心配です。

それからあとは、先ほどおっしゃいましたソフトを入れたがためにパフォーマンスの低下ないしはそれが原因でもってクラッシュを起こしてその部分で損害が出た場合の補償、それは、そのクラッシュないしは障害によって逆に契約者から私どもか賠償責任を求められるというようなことも当然考えられますので、そういったことも含めてその辺をどういうふうに考えられるのか、できれば明示してほしいというのが正直なところです。

○**橋本敦君**　高橋さんのお話の中で、プロバイダーの立ち会いに問題があるという御指摘がございました。私も、電子メールの傍受については、立ち会いという問題は具体的に技術的にも実際問題としてもこれは大変難しい問題だなと考えておるんですが、高橋さんのおっしゃる立ち会いに問題があるという点を具体的にわかりやすくお話しいただけますでしょうか。

○**参考人（高橋徹君）**　立ち会う人間が技術者でないと、ほとんどの問題が解決できないと思います。技術者である場合には、それは運用技術の責任者に相当するような人たちです。それは現実のネットワークの運用全体に携わっている人たちですので、日常業務にまず差し支える。

それから、インターネットの自律統治の世界でずっと運用をやってきているわけですから、問題は自分たちで解決したいというふうに思うのが前提です。そのプライドをまず壊してしまうというのがあります。彼か彼女かの立場を揺るがせた上で、警察の言うことに従いなさいという話になっていく。

そうすると、技術者の常として、プライドを傷つけたままでまともに仕事をやれますかというような問題が出てきます。これは私が見ている限りではそんな生半可な技術屋さんはなかなかいないものですから、やっぱりそうなってくると非常に角が立ってくるというのがまずあります。

それから、自分たちで排除できることをもし警察の技術力でできないような場合、これはもう全く立場が逆転して、プロバイダーが警察の技術者を監視しないといけない。現在そういうレベルが多々あると思います。だから問題だというふうに申し上げているわけであって、そういうことになったら、本当に日常の業務に差し支えてきます。ということが現実的な問題です。

○**橋本敦君**　いろいろお話を伺いましたが、資料としても法務省に寄せられた電気通信事業者の御意見があるわけですが、その中で、インターネット、電子メール等についてはその利用形態、秘密保護システム等が現在確立途上でもあり、電話などと異なる技術的特性を有することなどから、これらの問題は傍受法案、私どもはいわゆる盗聴法案と言っていますが、この対象から当面除外して、もっともっと十分議論を尽くした上で立法化することも考えてほしいという要望が電気通信事業者から寄せられているんです。

お二人の参考人のお話を伺っても、こういう観点はまだまだ大事ではないかなという思いがいたしますが、最後に御意見として、こういう事業者の御意見があることについてそれぞれ御意見を承って、私の質問は終わらせていただきたいと思います。

○**参考人（高橋徹君）**　対象から除外するということは、傍受法の本来のねらいからすればそれは論外であるということを先ほど申し上げました。

ただし、インターネットか発展途上であり、かつさまざまな論議がそこでおさまっていない、だから除外すべきであるという議論については、それはどこまで行っても発展途上であるということ

を申し上げたい。これは、議論がどこかでおさまるということがないのがインターネットの特徴です。常に日々革新しながら進んでいくというのがあるわけであって、どこかで何かが定まって、それ以上は先に進みませんよなんということがもしあったとすれば、それはインターネットが死ぬ日です。

○**参考人（本名信雄君）**　私も、この世界が発展途上だから傍受から除外しろということについては否定的です。やるなら当然含めてやらなければ、要は聖域をつくるという形になってしまいますから、それでは本来の趣旨から反するというふうに思います。

　ただ、やるならやるでもっと我々が見えるような形でもって議論が進まないのかなというのが正直なところで、現在もらっている情報の中で、我々が仮に協力を求められたときに何をやっていいのか全然わからない。この法案が成立した後、たしか二カ月後でしたか、施行自体が、ちょっとその辺忘れましたけれども、仮にそういうタイミングでもってやってくれと言われた場合に、では我々はどうするんですかというのが今の正直な気持ちです。ですから、もしやるならやるでもってきっちりやれるような環境を私どもに見せてほしいというのが実感です。

○**橋本敦君**　現在その環境が具体的に見えていない、こういうお話ですね。わかりました。

　終わります。

○**福島瑞穂君**　社民党の福島瑞穂です。きょうは本当にありがとうございます。

　まず冒頭、素朴な質問で、技術的なことを教えていただきたいんですが、インターネットにおける盗聴は一体どうやって技術的にやれるのか。先ほどリアルタイムモニタリングは難しいという意見もありましたし、専用線は余りに大量に流れているのでピックアップは難しいという話がありました。

　ですから、例えばＩＳＰとユーザーの間のダイヤルアップ回線上で盗聴する。二番目、メールボックスやログを盗聴する。三番目、電子メールのコピーをほかの場所へ転送する。四番目、ＩＳＰ内のＬＡＮで盗聴するなど、いろいろ可能性としてはあると思うのですが、一体全体どうやって技術的に盗聴が可能なのか。お二人の意見をお聞かせください。

○**参考人（高橋徹君）**　今おっしゃられたような盗聴は可能なわけです。一番有名なのは、ＬＡＮ上でＬＡＮに器具をがさっと差して、そこからデータを横合いに引っ張ってくるというのがあります。これはタッピングというやり方で、タッピングの手法というのはさまざまありますけれども、タッピングでいくとダイヤルアップのところの電話線にもタッピングできるわけです。それは回線そのものに物理的に力を加えて、そこからデータを持ってきてしまう。そういうことをダイヤルアップでもＬＡＮ上でもできないことはない。

　それが例えば光ファイバーでデータを送っているようなことになると、今度はこれは非常に難しい。光ファイバーにタッピングをしようと思ったら、これはとんでもない話になってしまう。そこでもう線が切れてしまうかもしれないし、そういうことができないように光ファイバーではデータを保護しているということになっています。電磁波の影響もありません。

　それから、そういうことができるとしても、その間に暗号化がもしかかっていたらこれはほとんど解読できないというのが今の通例ですから、盗聴が可能だというのは非常にわずかな部分、つまり一般のどうでもよろしいというふうな情報に関してはこれはやればできるでしょう。そのほかの本当に企業にとって機密の情報に関しては、暗号化がかけられているとすれば、どんなタッピングをやってもデータが見えるだけでその中身は見られないということになると思います。

○**福島瑞穂君**　本名さん、いかがでしょうか。

○**参考人（本名信雄君）**　技術的なことはもうほとんど高橋さんから御説明されたんですが、傍受対象の回線が例えばＩＳＰのアクセスポイント、ここにアクセスしてくる、何番にかけてくる通話を傍受するといったところで仮に発行された場合、私どもみたいなところでもって一つの、例えば東京のアクセスポイントがありますけれども、ここでは番号一つについて物理的な回線が四百六十回線つながっているわけです。その該当する通話が四百六十回線のどこに飛び込んでくるか、予想ができません。仮にやろうとすると、四百六十回線にすべて同じ機器をぶら下げておいて、そこを各回線レベルでもってスポットモニタリングするという、そういった手法は可能です。

　ただ、こういったネットワークは使う人はどこにいても使える状況ですから、その人が東京に住んでいるからといって東京のアクセスポイントを使うとは限らない。北海道のアクセスポイントを使うかもわからない。九州のアクセスポイントを使うかもわからない。そこは使う人がどこを選択するかでもって決まってくる段階で、ですから、この段階で電話のモニタリングをこの回線に特定してやること自体が余り意味がなくなってくる。

　そこから先、ではネットワークに入った段階でリアルタイムモニタリングできるかというと、先ほど高橋さんのお話にありましたように、アクセスポイントから実際バックボーンへつながってくる回線の中に、我々がよく使うプロトコルアナライザーという回線状況を監視するようなシステムがあるんですけれども、それを組み込んでやったとしても、そこで蓄えられる情報量というのはごく限られた情報しか蓄えるスペースがないわけです。それを莫大な量、何日間、例えば三十日まで延期できるという形でもって三十日間ぶんぶんぶん回して、そこに流れてくるデータを蓄えようとするとその設備だけでもう大変だと。それを各ＩＳＰのサイトで傍受するという地域限定という形で、要するに場所限定という形で運用すると、その機械が何台も必要になってくるという状況になってくるわけです。ですから、今考えているようなやり方では、傍受そのものが現実的に成り立つのが難しい状況にあるというふうにお考えいただければと思います。

○**福島瑞穂君**　はい、わかりました。

　ちょっとこれは愚問で済みませんが、プロバイダーという、あるいは会社でも個人でもいいですが、今全国でどれぐらいあるのでしょうか。

○**参考人（高橋徹君）**　電気通信事業者としてインターネットサービスをやりますというふうに郵政省に届け出をした会社が三千五百を超えています。しかしながら、実際に我々が見ているところの具体的なサービスを提供している企業というのは、個人も含めて、これは八百社を超えるぐらいだと思います。

○**福島瑞穂君**　きょうお話を聞いて、ニフティサーブのような大手は大手なりに負荷がかかるので非常に費用負担が大変なこともわかりましたが、同時に、結構弱小のプロバイダー、弱小と言うと申しわけないんですが、小さなプロバイダーの人たちと話をすると、例えば一人で自宅兼事務所でデスクにコンピューターを一台置いてやっているというふうな人も多いわけです。その人たちが非常に今悩んで困っておろおろしているのは、もし自分の事務所に来られて協力義務と言われても、一人でやっているし、一カ月、二十四時間、どうも対応できない。立会人などについても、一体どうなるんだろうという不安の声をよく聞くんです。

　ですから、そういう意味では立会人ということの確保とか、そういうことについての業界の実態とか意見とかありましたらお願いいたします。どちらでも結構です。

○**参考人（高橋徹君）**　私は今、日本インターネット協会の会長を務めておりますが、その会員の中に地域プロバイダー協会というのがあります。その人たちからの意見というのを伺ったわけですが、地域プロバイダーの人たちは、地域の協会の方で議論した結果、とても立ち会いなんか不可能だ、そんなことをやったらもうたちどころに仕事に差し支えがあってつぶれてしまいます、技術のレベルとしてもそれにずっと携わる人を確保する

こと自体が難しいという話が何度も出てきています。

○福島瑞穂君　本名さん、いかがでしょうか。

○参考人（本名信雄君）　立会人に何が求められるかがよくわからないというのが正直なところでもって、単に立って見ていればいいのかという段階から、あれやれこれやれという形でもってかなり作業が発生するのか、その辺も正直言ってわからない。立会人というのは、要は令状から外れた行為を捜査員がやった場合、ただ単に見過ごしていればいいのか、それとも何らかとめる権限があるのか、そこら辺もよくわからないというのが正直なところです。

それから、私どもみたいにある程度技術者を抱えてやっているようなプロバイダーから、中小の小というところであれば、本当に二人とか三人で運用しているところもあります。ですから、そういったところに二十四時間、初期十日、最高三十日という中でもって、丸一カ月立会人としてつき合えということは、その企業に対して、あんた事業やめなさいと言うのとほとんどイコールではないかというふうに思います。

○福島瑞穂君　プロバイダーの人に聞きますと、例えばプロバイダーが使用しているソフトウエアは、電子メールを除いて要するに手づくりであると。結構プロバイダーごとの手づくりでソフトウエアをつくっているので、捜査官、他人か勝手に使うと壊れてしまう場合があるので、結局自分たちがやることになってしまうのではないかと。あるいはそれを拒否した場合に、警察が自力執行した場合に、プロバイダーのコンピューターシステムが破壊あるいはトラブルが生ずる、あるいは何か消えてしまうとかというふうなことを非常に恐れているという意見も聞くんですが、そういうことについてはいかがでしょうか。

どちらでも結構です。

○参考人（高橋徹君）　インターネットの普通のソフトウエアというのは全部標準品になっていまして、標準にのっとってつくられたものが主なわけです。ですから、本当の意味での手づくりというのは余りない。ローカルなプロバイダーというか、小さなプロバイダーの人たちになればなるほど自分たちで一々開発なんかしない。ほとんどすべてのものが一般のもので間に合うというのがインターネットの世界です。

そういうことで、中には手を加えて、ほかのプロバイダーと競争するためにわざわざ違うものに仕立て上げてサービスを提供するというやり方もいろいろありますから、一概には言えません。そのところがプロバイダーにとっては企業秘密だったりするわけです。こういう機能がついているからほかのプロバイダーと区別して売りなんだという、そういうことはあると思います。そういうことを捜査の人に説明しても、多分捜査の人は一般のことしかわかっていないわけですから、運用している中で特殊な作業をやっているとすれば、そのことを理解しないととんでもない間違いが捜査の過程で生じないとも限らないと思います。

○福島瑞穂君　わかりました。

本名さん、いかがでしょうか。

○参考人（本名信雄君）　確かに、メールソフトというのは大体標準品といいますか、インターネットの世界でもって一般的に使われているソフトというのがあるんですけれども、ソフトは同じでもそのソフトをどうやって動かすかという、コンフィグレーションという作業があるんですけれども、そこは個々ばらばらだと思います。

例えば、メールを何日間とっておくとか、こういうメールはこのサーバーには届かせないとか、そういった個々の設定というのは、各プロバイダーが持っているオペレーションポリシーというのがありまして、自分たちのポリシーに合ったような形でもってメールシステムを設定していきます。

ですから、スタンダードなプログラムは使いますけれども、個々の設定というのは微妙に違っている。そういったところに対して、例えば捜査当局側が汎用だという形でもってプログラムを持ってきてできるかというのは、それこそ実際どういうものをつくるかによって変わってくるというふうに言えると思います。

○福島瑞穂君　わかりました。

今、プロバイダーで捜索押収されているところがありますけれども、その実体験などを聞くと、例えば管理者パスワードをよこしてほしいというふうに言われる。それは持っていかれると大変なので断固拒否すると、サーバーを持っていくと言われるので、仕方ないから幾つかの情報を現場の競り合いの中で少し出して帰ってもらうとか、いろんな話を聞いたりします。

先ほど本名さんが、協力義務か何なのかよくわからないということをおっしゃいましたけれども、例えば管理者パスワードをよこせというふうに捜査官に言われるということはどうなんでしょうか、管理者パスワードを渡すということはプロバイダーにとってどういう意味があるのでしょうか。

○参考人（本名信雄君）　管理者パスワードを渡せということは、管理者パスワードでもって運用できるシステム全体をその手にゆだねるということですから、とてもそんなことはできません。逆に言うと、では何がやりたいのかをはっきりさせてくれれば、そのやりたい範囲ができる、例えばそういった権限を与えるということは可能になるかもわかりません。

○福島瑞穂君　わかりました。

現在、捜索差し押さえ令状がプロバイダーやインターネット業界に来ているということもありますけれども、お二人の会社でそういうことが問題になったことというのはありますか。今まで何かそういうことで問題になったことはありますか。

○参考人（本名信雄君）　問題という意味がよくわからないんですが、そういった事例はありました。ただ、あくまでも何々を出してくださいという形でもって、それに該当するものを物理的な媒体でもってお渡ししたといったことは何度かございます。

○福島瑞穂君　高橋さんの方はいかがでしょうか。

○参考人（高橋徹君）　最近余り詳しい話は知りませんけれども、捜査の方から御相談をいただくことが多いというふうに聞いています。何々をよこせという以前に、こういうケースはどういうふうに攻めていったらいいんだろうかという話とか、そういう話の方が日常的にあるような感じです。

○福島瑞穂君　先ほど本名参考人が、この盗聴法ではなく、できれば捜索差し押さえ令状の方が、先ほどリアルタイムで引っ張るのが難しいのでという趣旨のことをおっしゃったように思いますけれども、この委員会の中でも差し押さえる場合、押収品目録をつくる場合と盗聴の令状が出る場合で、要件と効果が随分違うんじゃないかということも議論になりました。

ところで、今後、私自身は、例えば警察は盗聴の令状と捜索差し押さえの令状の両方を持っていって、それで盗聴に対する協力を例えば正当な理由があって相手が拒んだ場合に、それではサーバーを差し押さえるという、要するに二通持っていって、盗聴がだめなら、ではサーバーを差し押さえるというふうなことを言うのではないかと思うんですが、サーバーを差し押さえると言われた場合は、これは協力せざるを得ないのではないでしょうか。どうでしょうか。

○参考人（高橋徹君）　今から何年か前にネットワーク上のポルノ問題というのが起きたときに、サーバー差し押さえということが起きたことがあります。

そのときには、警察の方もサーバーを差し押さえるとどうなるかということが全然わかっていなくて、サーバーを持っていこうとしたら、持っていかれる方のプロバイダーが、それを持っていかれるとうちの商売はストップするんだと言ったら、ああそういうものか、ではここで君は貸与願を出しなさいと言って、差し押さえたサーバーをそのままそこに置いて貸しておくということをやったそうです。それで、必要な当該のファイル

だけ、アダルトの画像が入ったそこだけをサーバーから抜き出して、それを警察の方に渡したという話を聞いたことがあります。

つまり、一般にサーバーというのは一番基幹のコンピューターなわけですから、それを動いているものを押さえてしまうと、それの代替品がなかったりなんかしてやっぱり困るわけです。電子メールのサーバーなんかだといつも前のものにさかのぼって取りに来たりするから、それはずっと前のものから持っていないといけない。それをがばっと持っていかれたら、これはもう全く商売上がったりになってしまいます。コピーをつくるというのが当たり前の話です。そこだけ、必要なもののコピーを抜き出して提供すると。

○福島瑞穂君　先ほど、捜索差し押さえと盗聴による令状の場合のことをちょっと申し上げましたが、この委員会でも、メールサーバーにあるのはリアルタイムではないので捜索差し押さえの対象である、だけれども現に動いているのは盗聴令状の対象であると、政府の回答はそうだったんです。そうすると、一瞬の差で捜索差し押さえ令状になるのか盗聴令状になるのかというふうになったり、ちょっと不均衡ではないかと思うんですが、その点について本名さん、いかがでしょうか。

○参考人（本名信雄君）　先ほどからも申し上げておりますように、傍受というのがリアルタイム性というところに主眼を置いてやるのであれば、メール自体をリアルタイムでもって引っ張り込むというか、ないしは通過していくものを見るということ自体がもともと人間の目視の世界では不可能なんです。ですから、そういう観点で傍受をとらえるのであれば、傍受になじまないと言わざるを得ないです。

ですから、このデータ通信の中における傍受とは何かといったところから、もうちょっと慎重に審議してほしいなというふうに思っているわけです。

○福島瑞穂君　高橋さん、うんうんとうなずいていらっしゃいますが、それについてお願いします。

○参考人（高橋徹君）　今、本名さんがおっしゃる傍受はリアルタイムでは不可能だということはこれはもう当然の話です、何度も繰り返しに出ていますけれども。そういうことが今のこの法案のもとになっているとすれば、本当にデータ通信における通信傍受というのをどういうコンセプトで、要するにどういうふうに定義するのかということをはっきりさせていただきたい。でないと、何を意味しているのかということがわからない。一番振り出しに戻ってしまいますけれども。

○福島瑞穂君　どうもありがとうございました。

○平野貞夫君　参考人の御両人に質問するのも六番目になりますと、だんだん先生方が聞いた後になりまして、なかなか聞く問題が絞られてきますので、ちょっと角度を変えた質問をしたいと思います。

私は、機械類は全く不得手でございまして、携帯電話もこっちからかけるか、向こうからかかったものを受けるしかできない人間でございます。十年近く前でございますが、当時ＮＴＴにいた、今は新しいＮＴＴコミュニケーションズという会社の社長になった鈴木さんから、将来必ずインターネットが中心の社会になるから勉強せいと言われたんですけれども、私はインターネットは人類を不幸にするものだから嫌だ、こういうのは拒否すべきだ、こういう議論をしたことがございます。

なぜかならば、私は共産主義者じゃないんですけれども、マルクスが資本論で書いた資本主義の特徴である商品の人間化と人間の商品化、すなわち人間性の疎外、これはもうそのとおりだと思います。インターネットなんかはある意味では情報システムの人間化、そして人間の存在が情報化するという人間性そのものの疎外になるんじゃないかという哲学を持っておりました。これは正直言いまして通貨のあり方だとか、そういう社会全体が変わる、もう資本主義でなくなると思うんです、このインターネットの世界をずっと進めていきますと。それはもう半分は神の世界だと思うんです。

というのは、人間は生理的に発展するのは、例えば山手線の電車が五分に一回程度来るのがちょうどいい脳の状況なんです。インターネットというのは、もうはるかに人間の生理を超えた機械なんです。ところが、それを私みたいにいつまでも拒否というわけにもいかぬ、もう既に世の中を動かしておりますので。ところが、お二人の話を聞いていますと非常に感心したんです。頑固なことを言っちゃいかぬなという思いでございます。

そういう観点からお聞きしますが、まず高橋参考人が最初に言われた言葉に私は感動しております。それは、インターネットがセルフガバメントを前提とするということを最初に言われたんです。ところが、人類は残念ながら公序良俗という考えからだんだん離れていっているんじゃないかと思います。セルフガバメントの世界から遠くなっている存在ではないかと思うんですが、これさえあれば、ある意味じゃ通信傍受法をつくらなくてもいいかもわかりません。

そういう観点から、インターネットはセルフガバメントを前提とするという高橋参考人のお考えをもうちょっとかみ砕いて御説明していただけないでしょうか。

○参考人（高橋徹君）　大変難しい御質問をいただきまして、自律統治というふうに言ったりしておりますが、インターネットはもともと学術研究を主とする人たちの間ででき上がって、それで普及していったわけです。それが余りにも便利だから商業用に展開するのが当然だろうということをアメリカの政府の方が見て、それで商用をけしかけたというようなそういういきさつがあります。そういうふうにオープンにしないと不公平であると。

学術のコミュニティーで生まれたインターネットの世界では、ほとんど技術者の顔が見えている、実際には会ったこともないけれども、どこのだれがどんなことを言う、ああやっぱりあいつもそういうことを言っているんだということが見えるような関係から始まっているわけです。そうすると、お互いの牽制力というのがうまく働いて、議論が余り乱れないで調和的な関係になっていくというのがインターネットの一番主要な性格として発達したわけです。

だから、例えば変な人が出てきて突拍子もない外れた発言をしますと、それが次第に緩和されていくような議論が成り立つというのが、これが例えばニフティさんのフォーラムなんかでも同じようなことがずっとあったと思いますが、それがネットワークのカルチャー、インターネットのカルチャーとして根づいているわけです。

これに対して、それを超えた形で、インターネットのセルフガバメントを超えた形で何かを仕組もうとする人は非常に意図的な、例えば意図的な犯罪者という形の人は、それを超えて破って自分たちの何かをそこへ植えつけたいというそういうことを意図します。そういう意味では、本当にうまくバランスをとりながら発展させようという意思がそれぞれのメンバーによって非常に強く保たれてきたというのがインターネットの最大の特徴だと思います。

○平野貞夫君　わかりました。

先ほど本名参考人のお話の中で、インターネットというのは技術的進歩が物すごく激しいというお話がございました。結局、その技術的に激しいシステムに対して法制度というのは人間の生理発展程度のものしか正直言ってできないんです、法律の、世の中のシステムというのは。したがいまして、激しく進歩する技術に対応できる通信傍受法を整備する、完備するということは、これは私は不可能なことだと思います。

問題は、非常にきょうはお二人からいいアドバイスを受けて、具体的な問題点を指摘されて、それを我々は政府にも確認せにゃいかぬ材料をちょうだいしたと喜んでおるんですが、どうしてもず

れが出てくる。しかし、それでもやっぱり必要だということを、必要といいますかインターネットを通信傍受法から除外することはないというお考えをお述べいただきました。現にインターネットによる犯罪捜査に協力も既にされているという印象をお話の中から受けておるんですが、インターネットやパソコン通信を利用した犯罪というのは、ちょっと二、三例をいただいて、インターネット犯罪というのは実際どういう状況なものか、あるいはもし構わなければ捜査にどういう形で協力されているかということをお教えいただければありがたいと思います。

○参考人（本名信雄君）　私どもが過去に警察に協力した犯罪の内容というのは、まず一点がわいせつ図書の販売、これはネットワーク上でもってデジタル化した画像を販売している。実質的には、物として自分でそのネットワーク上から集めたわいせつ画像を、自分でＣＤ－ＲＯＭを焼けますから、ＣＤ－ＲＯＭに焼いて、それを頒布する。その頒布することの連絡をネットワーク通信を使ってやっているというケース。

それから、比較的多いのが取り込み詐欺が多いです。これは、例えば掲示板みたいなメッセージボード上でもって先着一名様に今結構売れているような品物をかなりの低価格で譲りますという形でもってオファーを出すと、それに対して買いますというレスポンスか返ってくるわけです。通常でしたら、普通の商行為でしたら、物を見て、物が届いてから代引きでもってお金を払うか、ないしは物が届いてから決済するというのが常套なんですけれども、やっぱりどうしても欲しいどうしても欲しいというそういった欲求を起こさせるようなうまい勧誘の仕方をするわけで、先に金を払い込むというそういった取り込み詐欺の形態が結構ございました。

そういったところで私どもも協力をしているわけですけれども、個々にはそういった人の個人情報の部分的な開示というようなところでもっての捜査協力がほとんどです。

○平野貞夫君　ありがとうございます。

これはお二人のどちらでも結構ですが、きのうある専門家から聞いた話で私は驚いているんですが、インターネットでいろんな物の売買をやります中で、マネーロンダリングの一つの方法として、恐らく外国の銀行でしょうが、ある銀行の口座ごと買って、そしてマネーロンダリングをするという、インターネットを使ったそういう犯罪があるやに聞いたんですが、そういうことはあり得るのでございましょうか。

○参考人（高橋徹君）　寡聞にして聞いたことはありませんが、マネーロンダリングをわざわざインターネット上でやらなくちゃいけない理由というのは余りなくて、現実の生きている銀行、建物がちゃんと存在している銀行の中でやるということは現実にあるわけです。

そうすると、今現にインターネット上の銀行というのは非常に限られていて、そこに口座を開いてもそれを売り買いできるなんというふうな条件は今の日本にはまだない。多分、あしたかあさってぐらいになればできるかもしれません。ただ、ないものを今日本でやっても意味がないと思います。それはもうほとんど今ベースは外国で、バーチャルバンクというのが成り立って、それがつぶれたりしているわけですから、そういうことは日本ではまだできておりません。

○平野貞夫君　わかりました。

まことに初歩的なことを聞いて恥ずかしいんですが、プロバイダーという職業、これは国家資格か何かあるんですか。どういう資格で存在しているんですか。

○参考人（高橋徹君）　プロバイダーというのは一般名称でありまして、これは電気通信事業者の提供するサービスの一つにすぎない、インターネットのサービスを提供するということを電気通信事業者の中のサービスの項目としてそれを書いているのがインターネットサービスプロバイダーである。

ですから、一番単純には、一般第二種電気通信事業者というのは、地方の電監に、郵政省のその地域の電気通信監理局にＡ４の届け出一枚でもって受理されるということでなれます。これはダイヤルＱ²のサービス提供者と同じレベルです。

それよりも上に特別第二種電気通信事業者というのがいて、これは国際通信に関与しなければ特別第二種にはなれないというのがあります。これを獲得するためには、ファイルにしてこのくらいの厚さの書類をやっぱりつくらないといけないんです。あれ出してこれ出してというのをたくさん重ねていって、このくらいになります。それでようやく特別第二種になる。

その上に、今度は第一種電気通信事業者というのがいて、これは電気通信の回線設備を自前で保有しているということが前提になっていますから、これはもう相当なお金が要るということになります。特別第二種でもやっぱり相当な費用がかかります。

問題なのは、一般第二種のＡ４の紙一枚の届け出用紙でもって事業者になれるというところで、手軽過ぎるという。ですから、資格だけを持つという意味では、大勢の人たちが、つまり三千五百を超えるような人たちが一般第二種電気通信事業者としてインターネットサービスを提供するという届け出をしているわけです。現実にやっている人はその中の四分の一以下だろうというふうに考えています。

○平野貞夫君　なるほど、お話を聞きますと、通信傍受をするにせよ、あるいは本来のインターネット業務をするにせよ、プロバイダーというシステムといいますか、場合によっては個々の人がやるわけでしょうけれども、その責任といいますか仕事が非常に重要だという理解を、印象を受けたわけなんですが、これは例えば郵政省とか通産省で認定するとか何とかという性格のものじゃございませんか。

○参考人（高橋徹君）　電気通信事業法というのは郵政省のベースのものですから、郵政省の電気通信局が関与しているわけです。そこが今の届け出の認可などを扱うわけです。通信事業者としてのレベルに応じた扱い方ができているわけです。

○平野貞夫君　将来、健全なインターネットの発展のためにそういったものを管理すると言ったら問題がありますが、何らかの一つの教育といいますか共通な基準みたいなものが必要になるんじゃないか。今でも必要だと思いますが、そういう社会的な管理をする対象にはならないですか。

○参考人（高橋徹君）　地域のプロバイダーの協会の人たちは、マル適マークを自分たちでつけて、何ができる、何ができる、何ができるというふうな丸をつける項目をいろいろ持って、このプロバイダーは全体として丸である、二重丸であるということを識別しようとしています。それもそのセルフガバナンスの世界です。

インターネットのあれこれがわからない人たちがそれに対して適当にマークをつけようといってもこれは無理な話ですから、ユーザーがいてプロバイダーがいる、その関係でもってきちんと成り立っていることで適切なことをやっているのかどうかというのはセルフガバナンスに任せていただきたいというのが私の主張になります。

○平野貞夫君　わかりました。

本名参考人にお伺いしますが、お話の中に傍受になじまないものに適用しないでほしいというお話があったと思いますが、できれば差し押さえでできることならやってくれないかということもあったんですが、なじまないものというと具体的にどんなイメージで理解すればいいですか。

○参考人（本名信雄君）　先ほど来いろいろとお話をさせていただいているんですが、今回意識されているのは、コンピューター通信の場合ですと、多分電子メールというのがかなりなウエートを占めているというふうに思っております。

電子メールのシステムというのは非常によくできたシステムで、その辺の設定によってはいろいろなことができるといった状況にあります。ですから、例えば私どもが提供しているサービスでも、ここのメールボックスに入ったメールはあっ

ちに飛ばしなさいといったことをリアルタイムでもって設定変更ができるんです。きょうはAという場所に飛ばして、あしたはBという場所に、そのまた先はCでもDでも。要するに、メールボックスをほかに外部でたくさんその人が持っていると、その時々に応じて自分が一番使いやすい環境へ、そこへ転送するようなそういったシステムも持っています。

ですから、そういったところに対して、ここのメールボックスを傍受しなさいというピンポイントでやったとしても、そこは単なる通過点で、そこでもって通過するメールを捕捉するのが現代の技術では非常に難しいというふうに先ほど来御説明させていただいております。

○平野貞夫君　お二人の話の中で、高橋さんでしたか、例えば警察の捜査技術の信頼を向上させるためにも、ソフトづくりといいますか、マニュアルづくり等にプロバイダーと協議機関をつくれとか、あるいはもし大きな損害とかそういった場合にその補償のシステムをつくれとか、大変参考になる意見がそのほかにもございましたので、我々も政府側に持ちかけてぜひ前向きに取り上げてみたいと思っておるんです。

もう質問をしませんが、最後に申し上げたいことは、もとの話に返りますが、私はインターネットというのは脳の神経細胞の一部分を表へ出したようなものだと思っています。したがいまして、人間社会の、本当に人間そのものも人間という名称で呼べなくなるような、場合によっては化け物になるかもわからぬ、そういう危惧は大分なくなりましたのですが、お二人ともそれの中心的な社会的立場で活躍されておりますので、どうか健全な発展のために御尽力いただきたいことを要望しまして、質問を終わります。

○中村敦夫君　中村敦夫でございます。

どうもお疲れさまでございます。お二方に、高橋さん、本名さんに御質問をいたします。

実は、午前中にも同じことを聞いたんですが、午前中の場合は電話の専門家たちに対して、その専門分野での質問としてお聞きしました。今回は、インターネットの専門家として、このケースをちょっとお聞きしたいんです。

実を言いますと、この法案はたくさん問題点があるんですけれども、その大きな一つにやはり立会人の問題というのがございまして、いろいろと今まで審議していても一体正体が何なのか明確ではないんです。チェック機能を果たすものではないということだけは答弁ではっきりしてきているわけなんです。そのことがかなり不安な材料になっているということなんです。

しかも、通信傍受、いわゆる盗聴基地です。それをする場所の問題というのをどこに規定するのかということで私は質問をしています。それがつまり警察署とか警察施設のようなもの、そういう場所でもいいということになると、ますます立会人というものが不透明になり、現場というもののイメージがはっきりしなくなるということなんです。それができるのかどうかということを私は質問をしました。答えは、法務省としては警察施設での盗聴は法的にはできないと今のところ答えているわけなんです。

ですから、法的にはできないということはそれはそれとして、では、その法的な部分を除いて、純粋に技術的には可能なのかどうか、インターネットの場合でお聞きしたいわけなんです。一つのケースとしては、通信事業者の施設と外部の施設、それを専用回線でつなぐ、一メートル、二メートルじゃなくて例えば百メートルでもつないでやるということが、施設の外部から電気通信設備をモニタリングするということになるわけですけれども、技術的にはこれは可能なんでしょうか、お二人に確認したいんですが。

○参考人（高橋徹君）　それは、プロバイダーと外部をつないでモニタリングをするということは可能です。割に単純なことだと思います。

○中村敦夫君　わかりました。技術的にこれは可能だと。

もう一つ、通信事業者の施設と外部の施設を、今言った専用回線、ケーブルではなくて携帯電話のようなもの、そういう装置でもってモニタリングするということも技術的に可能でしょうか。

○参考人（本名信雄君）　技術的には可能ですが、運用上は多分意味がなくなるでしょう。例えば、携帯電話で送れる情報量というのはたかが知れている。例えば、今の携帯電話ですと一秒間に九千六百ビットの情報量が送れるわけですけれども、モニタリングするためにはそれの百倍程度の能力がないと実際の用をなさない。ですから、現実的には、遠隔地からモニタリングをするのであれば、最初御質問があったような形でもって、あるところとあるところをかなり太い線で結ぶというのが現実的な方法になってくると思います。

○中村敦夫君　それは距離的な問題ですか。例えば、五十メートルぐらい離れているところに携帯電話をコンピューターに接続してやるといった場合に、特定の通信、これをモニタリングすることはそれほど難しくないかどうか。

○参考人（本名信雄君）　携帯電話でできる範囲というのはごくごく限られた範囲ですから、多分不可能だと思います、モニタリング自体。

○中村敦夫君　そうすると、携帯電話ではなくて、そのような特殊な無線装置みたいなものができた場合はどうなんでしょうか。要するに、専用回線じゃない、物体ではないものでやるという意味なんですが。

○参考人（本名信雄君）　当然、受信するからには発信側が必要になってきますので、例えば今の携帯電話で百倍ぐらいの、百倍とか千倍とかそういった能力を持つ無線装置を、発信側がプロバイダーの中、受信側がどこかその他の場所という観点であれば技術的には可能です。ただ、そういったものがあるかどうかというのは、ちょっと承知していないんですが。

○中村敦夫君　では、質問をちょっと変えます。

お二方とも今までも警察には協力して、いろいろその場合の犯罪の検挙率も高いというふうにおっしゃられてきたわけですけれども、具体的には今までのケースでいうとどんな形での協力なんですか。つまり、例えばメールを差し出すとか、具体的にはどういうふうな形で協力したのか、教えていただきたいんですが。

○参考人（高橋徹君）　いろんなケースがありますが、一つは、警察の方にユーザーから迷惑メールの話が持ち込まれて、迷惑をかけられた人から持ち込まれて、そのメールの差出人がどこにいるのか調べてほしいというようなケースがあります。

これも、どのサーバーを経由していくかという経路を調べて、何時何分ごろにそこを通過したかというふうな時間がわかりますから、その通信記録を調べて、大体あそこのプロバイダーから来たらしいということを調べて、途中では経路を偽ったりすることができるんです。それも多分こういうふうに偽ったろうなというふうに論理を立てて考えて煮詰めていって、大体この辺のあいつだということをプロバイダー同士が連絡をとり合って見つけていくような作業をやって、それを警察の方に知らせる。この人だと思われますというふうなことを言ったようなことはあります。

○中村敦夫君　本名さんの経験ではいかがでしょうか。

○参考人（本名信雄君）　私どもの方は、大体似ているんですけれども、その加害者と思われる人物が過去にどういうサービスを使っているのか、そういったトラッキング、ログと呼んでいますけれども、それをベースにしてそれを提供している。あわせて、先ほども言いましたように、一部個人情報の開示をやっております。その結果、それが捜査のベースになって捕まっているケースというのが何件かございます。

○中村敦夫君　それはメールとして打ち出して協力したということですか。

○参考人（本名信雄君）　メールの場合もありますし、実際その人のアクセス履歴というものをプリントアウトしてお渡ししたということもございます。

○中村敦夫君　インターネット犯罪というのは、また別のインターネットを利用した犯罪であって、ポルノとかもそういうものに入ると思うんですけれども、例えばこの法案がうたっているような四分野、麻薬とか銃器とかあるいは集団密航、大量殺人というようなケースで警察から協力を求められたということはお二方の経験上おありでしょうか。

○参考人（高橋徹君）　私の場合はそれはございません。大規模組織犯罪に該当するような話としては、今まで協力要請を受けたことはありません。

○参考人（本名信雄君）　現在まではございません。ほとんどが取り込み詐欺とかわいせつ画像の販売とか、そういったカテゴリーです。

○中村敦夫君　そうしますと、この法案が対象としているような犯罪をインターネットを盗聴することによって何かつかむというのは、具体的にはどういう形であらわれるんでしょうか。あるいは何をすることによってわかるんでしょうか。お二方の見解をお聞きしたいんですが。

○参考人（本名信雄君）　純粋たる個人的な想像なんですけれども、法案の中でもって対象となっている犯罪にかかわる部分であっても、ごくごく末端的なところでのやりとりが事によったら引っかかるのかなといったところです。

　組織犯罪というんですが、最近のこういったインターネット技術というのは、ちょっとした知識かあればある程度のことができることはできます。例えば、よくここで傍受の対象になるようなメールサーバーを立ち上げるというのは、ちょっとパソコンの知識があってそういった本を読むのが嫌いじゃなければ、一カ月ぐらいその世界にいれば簡単なメールサーバーぐらいは立ち上げられる。それをもとにしてインターネットに接続するということ自体は、今非常に簡単な状況になっております。ですから、ある程度そういった組織として動くのであれば、当然その組織の中のパワーでもってある程度処理できるようなことが考えられるのではないか。

　ですから、汎用的なプロバイダーを使うケースというのは、逆に言うと、ごくごくまれな部分と、それからどっちかというと受信者側よりも発信者側が手軽に使えるネットワーク、移動しながら使える、要するにポータビリティーのよさを考えた上で使うというようなケースが考えられるんじゃないかなというふうには思っています。

○参考人（高橋徹君）　余り大規模組織犯罪とおつき合いしたことがないものですから具体的なイメージが浮かびませんけれども、ただ国際インターネットのグループでもってしばしば話に出ることがあります。麻薬などの捜査で、国境をまたがってどんどん広げなくちゃいけないときに、さて我々はどうすればいいのかというふうな議論というのがありまして、それは要するに、例えばインターポールみたいな組織がありますね。インターポールとインターネットの国際組織がじかに連動するようなことがあればいいのかないのかというふうな議論も出てきています。それはＯＥＣＤの中でも本当にそういう話が出てきていますし、ＯＥＣＤのインターネットに関するワーキンググループの方でも問題になります。

　そのときの国内のプロバイダーが現在直面しているような問題とちょっとスケールが違っていて、にわかに小説で読むような感じになってしまうんです。中村さんの小説でそういうのがあるかどうか知りませんけれども。大規模組織犯罪が本当にここで起きているんだということのエビデンスを今まで見せてもらったことがない。ですから、三年前の議論なんかでも、いつもエビデンスを見せてくれれば協力しますよという話をすると、そうじゃなくて、エビデンスをとるために先にプロバイダーの情報開示が必要なんだという議論で、ぐるぐるめぐってしまってどうにもならなかったわけです。そういうものか今目の前で起きているというのは、我々、電子ネットワークの上ではほとんど関知し得ないものだというふうに認識しています。

○中村敦夫君　これまでのお話ですと、こういう大型犯罪、それのインターネット利用の摘発の御経験はないということで、近い将来もその絵がはっきりとは見えないというふうに受け取ったわけです。

　これまでの犯罪捜査協力がどのぐらい実は業者として負担になっているかというところがわからないんですが、今回この法案が成立するとなると、今度はさらに犯罪のおそれがある場合もやらなきゃいけない、こういうことになるわけです。そうしますと、業者としての負担というのはどの程度のものになっていくんでしょうか。お二方の想像できる範囲で結構でございます。

○参考人（本名信雄君）　ざっくりの話になりますけれども、通常、今まで協力してきたそういったところの工数を考えますと、依頼を受けてから一通りのデータを収集して要請にこたえられるところで大体三日間ぐらいでもって作業は終わるんですが、それは過去のものという形でもって、その中からあるものを取り出すという作業です。傍受の場合は、その始まった日から最高三十日というところがございますので、負担の度合いからするとかなり高くなる。立会人が日ごとかわってもいいのかどうかというのもわかりませんし、時間ごとにかわっていいのかもわかりません。その運用形態がわからないところでもって何とも言えないんですけれども、仮に一度立会人になったらその令状の効力がある限りはその人がやらなきゃいけないなんというようなことにでもなるとえらいことだなというようなところは認識としてあります。

○参考人（高橋徹君）　今、本名さんがおっしゃったような話で大体カバーできているんじゃないかと思いますが、立会人というのは本当にどこまで、三十日間べたっと張りついたらとても運用上の問題としては差し支えるし、そんな技術の人はなかなかいないというのはありますし、先ほども申し上げたようなこともあります。

　問題は、ほかのユーザーがどうも最近おかしいぞというふうなことが起こりかねないんじゃないかと。そういうことがもたらす影響というのが起こったときにどうしたらいいのかという、どうも自分のところに来るメールが何か、電話だったら雑音が入ってくるとかそういうたぐいのことが起こり得ないとも限らない。電子メールの場合にはデジタルですから余りそういうことはないはずなんですが、ただサーバーのぐあいがおかしくなったとかというふうな状態が続いたりすると、敏感なユーザーは全部トレースして見ますから、あそこはおかしいということを言われたときにまた信頼性のリカバリーの問題になってくるということもあります。

　そういうことを言っていくと、大規模組織犯罪の捜査に協力するということは結構体力がないとできない、小さいプロバイダーはとても対応できないだろうというのがあります。今、私の所属しているグループは専用線のユーザー数では第二番目の位置にありますけれども、そこで見てもなかなか人手を割いてずっと捜査に協力するということはつらいことだということです。

○中村敦夫君　私は、この法案そのものの大きな意図、要するに捜査の利便性のためにこの法案をとにかく拙速につくってしまって詰めのないまま社会に網をかけてしまうという危険性、それがもたらすであろうマイナス面というものをてんひんにかけるとどうしても反対せざるを得ないという立場にあるわけです。

　もう一つの問題としては、この法案そのものに大きな欠陥があるのではないか。なぜならば、これは基本的に言うと、電話盗聴を基本線につくられて、コンピューター通信、インターネットというところへ無理やり押しつけてしまっているために、具体的な場面で非常に整合性がない部分がたくさん出てきている。ですから、これは別々のものでなければいけない、法案として考えても。そういうふうな考え方を持っているわけです。

　当事者としてはなかなか法案に対して率直な意見を言いにくいでしょうが、印象としてはどうで

しょうか、私が感じているそういう点というのは。お二人に。一言、二言で結構です。

○**参考人（高橋徹君）**　今おっしゃったように、具体的な場面で整合性がないというのは本当におっしゃるとおりで、それは今まで我々が述べてきたことがそのままそうであると思います。そういうことからすれば、何でこんなに技術検討を抜きにしてどんどん事が運ぶのか、そこのところが本当に理解できない。拙速主義でいくと、私は国際の場面から笑い物にされるようなことが起きるんじゃなかろうかということを非常に恐れます。

例えば、私は来年ＩＮＥＴ二〇〇〇という大きなインターネットの大会を横浜でやる主催者になっておりますが、そういうときに必ず議論になるテーマなわけです。アメリカの場面ではクリッパー問題もだめになったし、それからネットワークのディーセンシーアクトという通信品位法も提出されて高裁でだめになっています。連邦高裁はだめだ、憲法違反だということをはっきり言っている。そういう非常にきつい社会があって、その人たちがインターネットコミュニティーでは非常に力を持っているわけです。例えば、ハーバードのバークマンセンターなんというところがインターネットの法的な議論をいつもやっている連中で、その連中が来年日本にわっと来ますから、そのときに、日本国ではこういうことをやっておりますよと言ったとたんに取り囲まれて、リンチじゃないですけれども、何と言われるか。本当に国辱、国辱というか国際に恥をさらすというふうなそういう場面が出てくるんじゃないかと一番恐れるところです。

そういうことがないようなものをちゃんと考えていただきたい。そういうことが議論できないんだったらやめていただきたい。これは本当にお願いです。

○**参考人（本名信雄君）**　高橋さんと全く同意見でして、やっぱりインターネットの世界、基本的にボーダーレスという世界でもって動いていまして、全く話す言葉は違いますけれども、ネットワーク的には全く国際、要するにインターナショナルの世界になっているわけです。

それから、先進国においてはこういった傍受という制度というものがあるというのも十分認識していますし、その制度があるということは実際その後ろにある運用というしっかりした母体もあるわけです。そういったものが、よその国のものはある程度見えるんですけれども、日本における傍受の法案自体、そこの後ろにある実際運用面でもって何が起こるのかというのがさっぱりわからないというのが、何で同じ国にいるのにわからないのかなというのが非常に素朴な疑問で、やるならやるでいいとは思うのですが、十分そういった背景を認識した上で公開すべき情報は積極的に公開していただく、それなくして我々の協力というのはできないというふうに思っています。

○**中村敦夫君**　ありがとうございました。

○**委員長（荒木清寛君）**　以上で参考人に対する質疑は終了いたしました。

両参考人に一言御礼のごあいさつを申し上げます。

本日は、御多用のところ貴重な御意見をお述べいただきまして、まことにありがとうございました。当委員会を代表いたしまして厚く御礼申し上げます。（拍手）

本日の審査はこの程度にとどめ、これにて散会いたします。

午後四時五十七分散会

七月二十三日本委員会に左の案件が付託された。

一、裁判所の人的・物的充実に関する請願（第四一四三号）

一、組織的犯罪対策三法案の廃案に関する請願（第四一四四号）

一、選択的夫婦別姓の導入など民法改正に関する請願（第四一四八号）

一、子供の視点からの少年法改正等に関する請願（第四一四九号）

第四一四三号　平成十一年七月十三日受理

裁判所の人的・物的充実に関する請願

請　願　者　静岡県袋井市堀越五ノ七ノ二　西田孝行外九百九十九名

紹介議員　海野　徹君

この請願の趣旨は、第二一七七号と同じである。

第四一四四号　平成十一年七月十三日受理

組織的犯罪対策三法案の廃案に関する請願

請　願　者　札幌市東区北二十七条東一〇ノ一ノ六　神原常雄外二百十五名

紹介議員　清水　澄子君

この請願の趣旨は、第三九二三号と同じである。

第四一四八号　平成十一年七月十四日受理

選択的夫婦別姓の導入など民法改正に関する請願

請　願　者　京都市山科区四ノ宮小金塚八ノ五六一　武田美枝子外三百十三名

紹介議員　吉川　春子君

この請願の趣旨は、第一七〇号と同じである。

第四一四九号　平成十一年七月十四日受理

子供の視点からの少年法改正等に関する請願

請　願　者　埼玉県浦和市文蔵三ノ一三ノ一四ノＢノ一　伊藤康之外千九百九十九名

紹介議員　吉川　春子君

この請願の趣旨は、第七五九号と同じである。

平成十一年八月二十日印刷　平成十一年八月二十三日発行　参議院事務局　印刷者　大蔵省印刷局