平成２３年度総合セキュリティ対策会議（第６回）

平成２４年２月９日

１．開会

２．検討

【事務局より、報告書案の全体的な構成及び「第１章　サイバー犯罪の現状と事後追跡可能性について」について説明】

○委員：内容については、このとおりで結構だと思います。表現に関して、「重要なインフラとして必要不可欠なものとなる中で、これを狙ったサイバー犯罪が」という記述についてですが、「これ」というのは重要インフラということになりますけれども、「狙っている」というよりは、こういう状況に「乗じた」とか、「利用した」というふうにしておいたほうがより正確になると思いました。

○事務局：修正いたします。

○委員：資料を見ると、携帯電話がサイバー犯罪に使われている割合が、やはり非常に多い。携帯電話については、携帯電話本人確認法があって、それに違反すると犯罪とされており、ある程度抑止のための制度は用意されています。しかし、相変わらず、例えば振り込め詐欺、あるいは出会い系サイト等のツールとして使われています。つまり、取締りと抑止は表裏一体だという主張ですが、一方で犯罪として規定されていてもなかなか抑止されないという現実が、携帯電話で起きているということです。そうしますと、そのデータ通信カードにしろ、ほかの手段にしろ、おそらく同じようにいろいろな方法で他人名義のものを入手して犯罪に利用しようとする者は必ず出てくるわけで、少なくとも携帯電話ではそういう経験、現実がある、ということについても意識して、何か対応を書き込めると良いというのが意見です。

○事務局：今回のテーマを選定した趣旨としましては、御指摘のとおり、携帯電話につきましては法律がございますし、ログの保存につきましても、先般、刑法、サイバー犯罪条約に伴う刑訴法の改正ということもございまして、推移を見守っていくということで、法律上大きく手当てされてない３つのテーマについて選定した次第です。御指摘の点につきましては、まさに携帯電話が犯罪に悪用されて

いるという実態もありますので、対策として強化することは重要ですけれども、今後、そういう形で対応していきたいとは思っております。

○事務局：御指摘の点については、対策を言うときにどのように書くかという問題だろうと思いますし、あるいはこの報告書をさらに進めて、具体的にどういう対策をとるかというときには、当然念頭に入れなければならないということだろうと思います。

【事務局より、「第２章　第１　データ通信カード、無線ＬＡＮ」について説明】

○委員：無線ＬＡＮについて、最近、スマートフォン等により、いわゆる３Ｇのほうがパンクしており、そのオフロード手段として、無線ＬＡＮを活用することがかなり議論されていると思います。そのため、ここで出てきている、いわゆる無線ＬＡＮという部分は、再度いろいろな面で脚光を浴びている。そこで、一つには無線ＬＡＮの端末そのものを暗号化して使用されないようにするということ、もう一つには、アクセスポイントのログの取等、誰がどこで使ったかわかるようにしておくなどの協力を求めていくというようなことも必要な可能性があると思いました。

○事務局：御意見を参考にさせていただきます。

○委員：一般家庭で使われている無線ＬＡＮ製品でそのログを取得していくということについて、ユーザーにとってのメリットがあるかというと、基本的にはないのではないかと考えます。一方、ログを取るという場合に、どれだけの期間のログを取らなければいけないかとか、その機器に対するその要求仕様というものが出てまいりますので、一般家庭用の無線ＬＡＮ製品でログを取得するという件については、十分議論されるべきと考えます。

　ただ、今、御発言の中にありましたように、携帯電話のデータオフロードのための設備といいますか、インフラとしての無線ＬＡＮとしてホットスポットとか、Ｗｉ－Ｆｉスポットとか言っておりますけれども、そういったものに関してのログというところでは必要性があると考えます。

○委員：無線ＬＡＮ製品のセキュリティや不正使用について、ここで問題なのは、あくまで他人の無線ＬＡＮが踏み台となって犯罪の痕跡がたどれなくなるということであって、決して無線ＬＡＮのユーザーのデータが不正に利用されるとい

うことを気にしているわけではありません。すると、無線ＬＡＮ機器の高度な暗号化ということを利用者に働きかけるというふうな記載がしきりに出てくるのですが、データの暗号化というのは、どちらかというと、不正傍受に対してとるべき無線ＬＡＮの対策であって、不正接続に対しては、一般的にはＳＳＩＤをステルス化する、ＭＡＣアドレスによるアクセス制限をするといった対策があるのだと思われます。そのため、暗号化ということだけを強くユーザーに対して啓蒙していくということは、あくまでデータが保護されるだけであって、不正にアクセスポイントに接続されて、不正利用されるということには必ずしもつながらないのではないかと思うのですが、どうなのでしょうか。

○委員：事業者としてお答えしますと、言われるとおり、暗号化というのは、一般的に無線部分のデータを解析できないようにするという意味で、傍受を防止する対策であるというのは、そのとおりです。ただし、無線ＬＡＮの製品の仕組みとしまして、ＰＳＫと呼んでおりますが、暗号化をかけるためのキーを事前配付しまして、事前配付したキーの一致を見て、初めてそのアクセスを可能にするというような仕組みがあります。そのため、暗号化をきちんとかけてあれば、その暗号キーを持った者しか接続ができないという形で、不正にアクセスポイントに接続されて、不正利用されることも排除することができるという仕組みになっております。

【事務局より、「第２章　第２　インターネットカフェ」について説明】

○委員：インターネットカフェの条例について、東京で制定されたということについては記述があり、他の道府県でも当然そういう機運があること、及び準備をしていることは理解しているのですが、その現状については如何でしょうか。少なくとも制定されてはいないということは明らかですが、条例を制定する上でどういう基本的な障害があるのか、それとも別の何らかの問題があるのかということです。

　また、逆に言えば、どうして東京ではうまくいったというか、条例を制定するに至ったのかという点についても、他の道府県との対比という意味で教えていただければ参考になると思います。

○事務局：他の道府県警察における条例制定の検討状況につきましては、数県で検

討しているという状況は伺っているものの、現在制定しているのは東京都だけでございます。インターネットカフェにつきましては、以前の会議でも御指摘がありましたとおり、都心型や郊外型といったいろいろなパターンがありますので、各都道府県の実情に合わせて、これからの問題として検討しているところが多いとは考えております。

○事務局：若干補足をいたしますと、具体的に動きのある県もあったのですけれども、ちょうど今年度のこの会議におきまして、このインターネットカフェの法制化の問題が取り扱われるということも、都道府県警察のほうも知っておりまして、それで、国の検討状況を参考にしながら条例提出するかどうかということも、例えば条例をつくったとしても、数年後に法律が後からきて、その意味がなくなってしまうということもよくあることですので、そういったことも考えられて検討されているというふうに聞いております。

例えば御質問にございましたように、何か反対の動きだとか、あるいはそういう条例ができると困る事業者さんが御反対になってとか、そういう事情で条例ができてないというようなことについては承知しておりません。

○委員：改めてサイバー犯罪とはなにか、ある意味で実世界における犯罪ということで、他人になりすまして何か詐欺行為をしたり、お金を、クレジットカードを盗んだりとか、そういう意味での犯罪と考えたときに、インターネットバンキング等々でいろいろお金がなくなるという事案のほかに、大学の入試問題をウェブに投稿したという事案もサイバー犯罪とされています。これをサイバー犯罪としてとらえるのかどうかという点について、素朴な疑問を持ちました。

○事務局：サイバー犯罪は毎年いろいろなものが発生しまして、枚挙にいとまがありません。平成２３年中はまさにインターネットバンキングの事案と、やはり身近なものでさえサイバー犯罪に悪用されているという、インパクトが大きいものとしてこの事例を取り上げました。

○事務局：若干補足いたしますと、例の大学の入試問題の場合には、これは結局業務妨害ということで立件しようとしたということです。報告書案中にサイバー犯罪の検挙件数の推移という表がございます。この中に３分類がございまして、１つは、不正アクセス禁止法違反、それから、２番目が刑法等で決められている電子計算機業務妨害等が含まれるコンピュータ・電磁的記録対象犯罪、最後に、先

ほど説明にもありましたネットワーク利用犯罪というものがあります。このネットワーク利用犯罪というのは、先ほどの入試問題の例でまいりますと、その入試の不正をするために携帯電話等を、端末を使って、他人の助力を得ようとしたということで、それはネットワークを不正の目的で利用して犯罪を敢行しているということで、この分類の中にちょうど該当します。ただし、確かに見ようによってわかりにくい事例ですので、そこの例として挙げるのにもっと違う身近なもののほうがいいのかもしれないので、その点については再度検討いたします。

○委員長：携帯電話を利用した試験問題の漏えいも、見方はいろいろ分かれると思うのですが、大学で入試を実施する側から見ますと、問題が漏れてしまったら、何ヶ月も準備してきたことが全て無駄なり、全部の試験が無効になってしまいます。業務の妨害というのは、それほど重大じゃないよという見方もありますけれども、やはり生徒としては非常に重大だと受けとめる向きもあるということだと思います。その上で、話題にはなりましたので、ここで例として挙げているということだと思います。

【事務局より、「第２章　第３　インターネット上の高度匿名化技術」について説明】

○委員：この第３の書き出しは、これまでの議論を反映したいいものだと思っています。真摯で善意の目的でできたものであるから、そういうものも阻害しないようにしなければならないし、コミュニティ自体も、世界的に見て、善意の技術者の方々を中心として研究者等で行われているという。

　そこで、全体の方針は良いと思うのですが、本報告書の名宛人は国民一般であり、警察庁のホームページにも公開して世界にも発信し、いろいろな方が読みます。その前提に基づくと、技術の概要等について、本章を説明する上でどうしてもなければならない部分なのかという点が気になりました。

○事務局：御指摘を踏まえて、もう少し簡素な内容に修正いたします。

○委員：インターネットを利用するときに、匿名というのを基本にするのか、あるいは顕名というのを基本にするのかという、大きな考え方の分かれ道があると思います。電話を利用した場合というのは、自分の電話番号を明らかにしなければ相手のところに通知が行き着かないというシステムになっているおり、電話を用

いた通話の中身について、例えば捜査一課が知るという場合には、令状を持ってやってくださいと、そういうシステムになっております。一方、ネットの場合には、誰が誰宛にアクセスしているのかということを完全に秘匿してしまうということを、権利として認めなければいけないのだろうかという大きな問いが背後にはあるのではないかと思います。

ネットでどこからどこにアクセスするかということについては、ＤＮＳサーバーがあって、最終的には上位のＤＮＳサーバーがあるわけですよね。そこで、例えば今までの議論というのは、どっちかというと、下のほうで記録を残す、あるいはそこでだれがアクセスしたかということがわかるようにするためにはどうするかということで、議論がされてきているわけですけれども、上のほうでログの記録を、例えばＤＮＳサーバーで上を通過していくものについて記録を残すというようなことは考えられないのでしょうか。もちろんその場合には、みだりにその正当な理由もないのにどこからどこにアクセスしているかというような情報を知られないようにするというプライバシーの保護の問題、監視があまり厳しくなり過ぎても問題だということがあります。また、そういうログを保存するということに伴って発生するコストの問題もあります。また、技術的にどの程度可能であるのかという技術の問題等が様々に関係してきます。しかし、そういう下のところで十分に把握できないということを考えると、その上のほうで何か記録を残すということも検討されてもいいのではないかと思います。

○事務局：１点目の本報告書の中でどの程度顕名か、匿名かという、考え方、言い換えれば価値理念について言及するということについてですが、今回、事後追跡可能性の保障ということで、警察当局として、事後捜査を行う場合に最低限さかのぼることができるというところの保障がないと、捜査が困難になる、という点を組み立ての基本にしております。一方、例えば捜査ではなく抑止を主体として考えますと、ネットの活動を全て顕名にして、そもそも犯罪そのものを行いにくい環境をつくってしまえばよいというような考え方もあるかと思います。しかし、事後捜査という考え方から事前抑止という考え方に変えるということは、大分主張の内容が変わってまいりますし、どうしても争いの多いところであると考えました。そこで、少なくとも事後追跡の可能性が開かれていないという状態の中では、抑止もまたあり得ないということで、その最低限のところだけは、今回何と

か御確認いただけないかというようなことで入れているということになります。

２点目の技術的な部分については、引き続き検討いたします。

○委員長：政治目的や何かの必要性がある場合等の条件があるかもしれませんが、完全な匿名の通信を行う権利を確保しなければならないと考えるか、それともそれはやはり排除しなれければならないと考えるか、その結論をこの報告書の中で出すということは、この会議の任務を超えていると思われます。

現にここではこういうものがあって、悪用される可能性があって、あるとすれば、警察庁としては、各国の捜査機関及び国際社会を通じて意見交換をしながら、将来的な悪用への対策を検討するというのがここのテーマの結びになっています。今後、完全な匿名性によって行われることの人類に対しての侵害の重大性等の問題について、きっちりこたえなければだめだというような局面に差しかかる場合もあり得ないことはないと思いますが、少なくともこの委員会では、こういう制度があって、こういう乱用の可能性もあるところで、それを見守っていこうという結論となるでしょう。事後追跡可能性という観点から、高度匿名化技術のような問題については今後検討するという形でこういうまとめをしており、議論を始めていかなければいけないというメッセージを打ち出す上で、今回はこのぐらいの書き方にする、と考えております。

○委員：表現上の問題なのですが、Ｐ２Ｐ技術は一般的にも相当知られており、これを読む方はほとんど分かっているとは思いますが、もう少し丁寧に説明したほうが良いのではないかと思います。

○事務局：注をつけてわかりやすくしたいと思います。

【事務局より、「第３章　事後追跡可能性の確保に向けた今後の在り方」について説明】

○委員：事後追跡性について、関係者といいますか、その取り巻くところで、追跡できるということを保障しているという趣旨ですけれども、一方、犯罪を犯そうとしている人間にも、そういったことをすると追跡されますよというメッセージを伝えていく、広報していくというような活動がもう一つ入ると、より良くなると思いました。

○委員：第１に、「保障」という言い方についてですが、追跡可能性を保障するとい

うのは、それをしなければならない者にとってみれば、非常にきつい言い方であると感じます。これは事業者的な視点もありますし、国民のプライバシーの侵害というような側面もまたありますので、そこまで踏み込んで書くべきであるかという点については、より多くの議論が必要であると思います。例えば、追跡可能性確保に向けたその協力の推進とか、その程度の表現にとどめるべきではないかと思います。

第２に、新しくサービスを導入する際に、その段階で追跡可能性についてきちっと保障されるような検討をする、という点です。それが望ましいという結論ですが、事業者側の視点で言えば、新しいサービスのイノベーションを阻害するおそれもありますし、当然そのための方法論とか、そういったものでほんとうにできるのかどうかという疑念もございます。また、国民的な視点で言えば、プライバシーの侵害がどの程度防げるのかということもあります。そのため、議論が不十分だと考えますので、私の提案としては、この「また」以降は全部削るべきではないかと思います。

○事務局：御指摘の２点は、いずれも意見が相当出てくる可能性のある箇所で、事務局としても慎重に言葉を選んで書いたつもりでございます。

１点目の「保障」というのがちょっときつい言い方であるとの御指摘ですが、保障というのは、あくまでも、例えば犯罪とか、そういう障害というか、事後の問題が発生しないように、差しさわりがないようにするということを保障というふうに読んで、この表現を選んだということでございます。

２点目の「望ましい」という言い方です。通常であれば、「行われる必要がある」、「行われることが重要だ」といった書き方をすることが多いのですけれども、今回はあくまでも「望ましい」ベース、そうしていただけるとありがたいぐらいの意味合いであり、例えば、「絶対」といった法律の義務づけベースの話ではありません。そこで、わざとトーンを落として「望ましい」という表現を選択しました。

○委員：申し上げたいのは、その議論のベースとなっているのは、あくまで捜査という視点でしか議論をしてないということだと思っていまして、そういう意味で、例えば捜査という視点では、こういう保障が必要であるとか、あるいは捜査という視点では「望ましい」といった表現であれば問題ないのかもしれませんが、そ

の議論をするに際して捜査以外の側面も十分議論しないと、踏み込んだ言い方に対しては慎重になるべきではないかと思います。

○委員：企業がサービスを提供するときには、そのサービスによってどういう悪用があるのかということをある程度推察した上で構築する部分もありますので、一律的にすべて追跡可能性を確保しておくということを決めるのではなくて、やはりそこはメリハリをつけて、起きることを予想した上で保存期間なんかも決めているところはあります。そのため、一律的にこれが望ましいというふうに書くのは少なくともちょっと行き過ぎかなというふうには思います。

また、現在は国際競争が本当に進んできておりますので、こういった面における国際標準もにらみ、日本だけが突出して厳しいというふうにならないように、国際的な推移も見守りながら決めていくということが必要と考えます。

○委員長：「事後追跡可能性が保障されるような制度をとらなければいけない」と書けば、それは「一律的に必要である」ということになります。一方、どの程度までログを保存しなければならないといった事項については、現実には具体的なものに合わせてやっているところです。そのように、現実はまさに、「サイバー犯罪の事後追跡可能性が保障されるよう必要な検討が行われることが望ましい」という表現と一致していると言えます。つまり、現実には、事後追跡可能性と個人のプライバシーの侵害、営業の自由等との比較考量をしています。したがって、本報告書の表現は、「どこまでやるのかということを検討することが望ましい」というニュアンスであると思います。

また、先ほどの「保障」という言葉と同様、「確かに保障しろ」と言えば、１００％やらないとだめだよというニュアンスにもとれてしまうことは確かです。しかし、「必要な検討」という言葉であれば、捜査の側から望ましいことは全部やれということではなくて、事業をなさる方の側からの利益考量といいますか、この程度のことまでだったら、お客のプライバシーの問題もあるし、その営業的なマイナスも少なくて済むというバランスをとる。どこまでやれるかを考えるということは入っている文章であると思います。

同時に、先ほど委員から御指摘のあった点と関連しますが、ネットの世界では、完全な匿名性を確保するべきで、それを排除する方向性というのが好ましくないという種類の議論も、あり得ないことはない。それら極論との間で、どの程度ま

で犯罪抑止のために、あるいは営業の利益とか、プライバシーのことにもバランスをとるのかという、どこに線を引くかということであると思います。

○委員：私も、「保障」という考え方の保障には若干ひっかかるところがございまして、これだと、ちょっと言い方が厳し過ぎると思います。特に、現実的には本当に保障できるのか疑問であると考えています。そういった観点からは、「サイバー犯罪の事後追跡可能性を高める必要性」といった表現であれば、異論はないと思います。

また、新しくサービスを導入する際に、事後追跡可能性について保障されるような検討をするという書きぶりになっていますが、これも現実を考えると非常に厳しいところで、ここまでほんとうに言い切れるのかというところがあると思っています。したがいまして、これを残すとしたら、頭の部分だけで、「また、現時点においても、新しい通信手段・環境のサービスが続々と登場しているところであり、継続して事後追跡可能性を検討する必要がある」といった書きぶりが適切ではないかなというのが私の意見です。

○委員：事後追跡を可能にしておくということは、これは犯罪捜査上、必要なことでありますし、また、事業として営んでいる事業者にもそれをある程度義務づけるということもあっていいかと思うのですが、一つ心配であるのは、そもそもこの高度匿名化技術等は技術的な仕組み上、個人を経由しているという部分です。そのため、ＤＤｏＳ攻撃で個人のパソコンが踏み台になったのと同様に、知らず知らずのうちに、個人がその経由地として巻き込まれてしまう場合があり得ます。その場合に個人がどれだけの責務を負うのかということについて、例えば、自分はそういった場合に何か情報開示しなければならないのかどうか、あるいはさらに何か責めを負うのかどうか、といったことについては、本報告書では触れていません。そこで、それらについても配慮しています、というメッセージは盛り込まれても良いと思います。

○事務局：まさに御指摘の点が難しいところで、そこで、純粋に理念で整理いたしまして、「刑事訴訟法に基づく捜査」というふうな書き方にしました。結局のところ、例えば企業であれ、個人であれ、捜査機関が犯罪をさかのぼっていく際に、必要があれば裁判所に令状請求し、その許諾の下で、犯罪に直接関係のない第三者についても強制処分に及ぶというケースも時にはあります。それは専ら犯罪捜

査という、治安確保というその公益のために法律上認められた権限ですが、その運用については、当然第三者である個人に関して必要以上の権利侵害をしないように配慮しながら、捜査活動を行っています。したがって、もし書くといたしますと、そういったような配慮を書き込むということになりますので、工夫をしてみたいと思います。

○委員長：委員の御指摘は、本報告書のこの箇所だけを読むと、一般の個人のユーザーが何か義務をたくさん重ねられることで萎縮する、不安を覚えるのではないか、という御趣旨ですか。

○委員：そうです。だから、先ほど、家庭用の無線ＬＡＮのログの保存についてどうするか、といった話題がありましたけれども、そういう個人が何らかの対策というか、事前的に講じなければいけないことがあるのかどうかという部分ですね。で、それは犯罪捜査ということで言えば、協力する義務は個人にもあるとは思うのですけれども、ある程度それを心して、事前に心構えとして持たなければならないものがあるのかどうかというのは、これを読んだ限りでは分かりづらいため、個人の方がその辺を心配されるのではないかという意味です。

○委員：新しくサービスを導入する際に、事後追跡可能性について検討をするという点についてです。このサービスが、例えばクラウドサービスみたいなものだったとしまして、それを犯人側が匿名で契約して、そこを攻撃の拠点として何かどこかに攻撃を与えるというようなことは、サービス事業者としてはどうしても防ぎたいと思っております。ですから、ここで記述されているような最低限のそういった検討とか、いわゆる契約者の情報をある程度記録を何年かとっておくとか、そういったことは必要な検討であると思います。したがって、当該記述については、あまり削除し過ぎず、少し残しておいたほうがよいと思います。

○委員：同じ箇所についてですが、犯人側の匿名化手段となる余地がないかという視点も一つの考量要素として、いろいろな方の意見はきちんと聞き、その上で「サイバー犯罪の事後追跡可能性が保障されるよう必要な検討が社会的合意のもと行われる」といった表現であれば、理解を得ることができると思います。異論のもう一つは、新しいサービスの導入のたびに検討していたら、事業者としては困るということだと思います。しかし、その場合であれば、表現を変えることで「軽重」や「必要に応じて」というニュアンスを出せるかもしれません。

さらに言えば、こういうサービスの開始のたびに検討する、といったことは、プライバシー保護の分野であれば、国際標準となりつつありますが、環境アセスメントのプライバシー版とでもいうべきものがあります。Privacy・Impact・Assessment（PIA）という名称として、新たなサービスを開始する際には、プライバシー保護にどういう影響を及ぼすか検討する、というのが国際的な流れになりつつあるということです。そのため、将来的に、別の観点・方向から、プライバシー保護とは逆の方向になり、こういう問題も事前にインパクトの影響評価的なものを組み込むべきである、という動きにならないとは言えないと思います。したがって、そこのところを踏まえた上で書いておくのはありうることだと思います。サービスの開始の際に事後追跡可能性について検討することについて書いておくことは、委員の御意見にもあったように、事業者の方々にとってもプラスの面もあると思いますので、「一律に」といったニュアンスが消せるような形にしたらいかがでしょうか。

○委員：ある製品を世の中に出すということに当たって、それが法制化されているか、あるいは法によって規制されているかどうかという問題はあるものの、危険のあるものを出すことについては、製品を世の中に出す者がその責任を持っているということは、常識的に理解できることと思います。

新しくサービスを導入する際に、事後追跡可能性について検討をするという点について、この文章を見ると、サービスが定着してから事後追跡可能性を確保させようとするのではなく、一律に何でもスクリーニングするべきであるというふうにも読めないわけではないようなところが、問題点となっていると思います。一方、基本的に危険なものを出すと、あるいは危険なものがもう一目瞭然でわかるというようなものについて、何もそれについて限定もせずに出すというのは、やはり危険な考え方であり、事業者としては責任の一端というものがあると、個人的には思います。

そのため、危険性を有するものについては、事業者が自ら分かる場合には、事業者が自ら措置をとるということも必要であると思いますし、あるいは、他から指摘を受けて、その危険性について検討するということもあると思います。ただし、その危険性が分かっていないものについては、多分その危険性が見えたときに初めて対処するという問題になるのでしょう。したがって、おそらくは、犯人

側の匿名化手段となる危険性というものがどのように認識されるかということと、それについて事後追跡可能性が保障されるということは、相関関係にあると思われます。

個人的には、新しくサービスを導入する際に、事後追跡可能性について検討をするという点については、報告書に書く意味はあると思いますし、同時に、このままでは一律に何でもかんでもスクリーニングしてしまうというふうにも見えるというところからは、この文章は危険性があるとも思います。そのあたりをご配慮した表現とするのがよろしいと思います。

○委員：「保障」の件について多くの議論が出ていますが、やはり「保障」という言葉自身が問題なのだと思われます。というのは、この「保障」という漢字で言うホショウは、本来持っていて当然の権利といったものが保障される場合にこの字を使うと思うのですね。で、この場合はそもそも追跡可能性ですから、本来それが保障されているものでもないわけで、それをなるべく高めるという話だと思います。そういう意味でいきますと、保障というよりは、むしろ担保されるとか、そんなような表現のほうが適切ではないでしょうか。

○委員長：委員からは、既に「高める」、「担保」といった表現の提案がありました。「保障」という言葉は、いろいろなニュアンスを持っており、「最低限これは絶対やらなければならない」といったニュアンスを持つ場合は、問題だと思います。ですから、この箇所は修正する必要があります。

一方、「また」以下全部削除するというのは、一つの選択肢ではありますが、いろいろな御意見が出ており、次回検討したいと思います。それでも、まだ問題点が残るということがあれば、この場で御議論いただいた上で修正して、それでもなお合意が得られないのであれば、削らざるを得ない場合もあり得るということだと思います。

○委員：多くの議論が出ている「保障」という表現についてです。このように、どの表現が適切であるか検討する際には、仮に英語やドイツ語、フランス語等の外国語に訳してみて、ぴったりおさまる言葉を選ぶのがよいと思います。例えば、世界に我が国の政策として事後追跡可能性の検討について発信するとしたら、どういった表現を用いるかということを考えると、落としどころが見えるようなときもあります。「保障」について言えば、多分事業者の方々は、この言葉をコン

ピュータの世界のデフォルトという表現に対応したニュアンスとして受け取られるのではないかと思います。「あらかじめ組み込まれている、デフォルトである」というのは、強すぎるニュアンスなのだと思います。

○委員：私は、この「また」以下の部分を残すことに賛成です。事後追跡可能性は、万が一のことが発生したときの最後のよりどころでありますし、最悪の事態を考える場合、事後追跡可能性を一切やらないし、さらには逆に事後追跡を不可能にすることを保障するというような業者が出現したら、どうなるかということが懸念されます。また、こういったことを遵守する事業者には、必ず何らかしらの負荷が出ますので、正直者がばかを見ないように、関係者一同でこういったことに賛同していただいている業者さんを盛り上げて成長させていくようなことも、信頼性として必要と思います。要するに、定着して事業継続できていかないと話にならないので、そのあたりご考慮いただきたいとは思います。

○委員：１点だけ申し上げておきたいことがございまして、事業者も、事後追跡可能性がないと捜査に支障に来すということはよく理解しております。しかしそれを保障するというところまで、どこまでやるのかということについては、ここでの議論では捜査の視点でしか議論してないというところが問題であると思います。先ほど、危険のないような製品、サービスを提供するのは、事業者の義務だという御意見がありましたが、その危険というのはいろいろな危険が含まれます。例えば、事後追跡ができないために捜査ができなくて、その犯人が捕まらないという危険もあるかもしれませんし、逆にそれを保障するためにプライバシーが侵害されるという危険も、かなりの連関性を伴って発生するだろうというふうに予想しております。ですから、そういったいろいろな視点での議論なしに、あまり踏み込んだ表現で結論として書くことについては、問題があると思います。

○委員長：次回は、今回の第３章の部分で多数出された御意見を整理し、再度文章化したものをお示しして、御議論のうえ、最後でまとめたいと思います。

３．報告

【事務局より、「不正アクセス防止対策に関する行動計画」及び「不正アクセス禁止法の改正」について、報告】

○委員：効果的な普及啓発についてです。先週、全国各都道府県から、二、三名ず

つの方が少年補導員に関するリーダー研修として集まりました。その機会に、サイバー関係についてちょっとお話をして聞いたのですが、アンケートの中でインターネットがよくわからないという人が多くいました。そういった環境の中で、子供たちが育っているというのが現状です。今日のこういった話し合いの中でも、そういったことを頭の片隅に入れておいていただくと、更に子供に対していい発言、考え方が出てくるのではないかと思いました。

これから育つ子供たちは、パソコンを傍らに育っていく子供たちだと思います。そして、子供たちのオンライン生活がこれから更に幅広く子供たちに浸透していくことだと思います。そして、ネットの中の知人とつながって、更にコミュニケーション、コミュニティを重要視してくると思います。その中で、そういったデジタルネイティブの子供たちを守っていくには、やはりそれなりのセキュリティ、要するに、子供たちに対するセキュリティの教育を、更に考えていく必要があると思います。

○事務局：不正アクセス防止対策に関する官民意見集約委員会でも、そこが一番重要だということで議論になりました。そのため、生徒・学生・保護者・教育機関を対象とした普及啓発ということで、最重要課題として認識して位置づけております。

○委員長：文部科学省も入っているのですか。

○事務局：本件の担当者は、警察庁、総務省、経済産業省、ＩＰＡ、オンラインゲーム協会、情報セキュリティ関連事業者等なっております。経緯といたしましては、文部科学省もぜひ入っていただけないかということでお声がけしたのですが、ちょっと断られまして、ヒアリングだけはやっていただきました。

○委員長：別の情報セキュリティ政策会議等でも問題になるのですが、事業者は一生懸命にいろんなキャラバンを組むなどの取組をされます。しかし、啓発、教育の一番中心は学校教育ですので、そこを巻き込めないと、国の政策で重要だ、重要だと言いながらも、ポイントをついてないという印象を受けます。それも含めて、何か子供の現実の社会とＩＴの現実と、それから、政策を議論するところがずれてしまっている感じがします。本来は、現実に基づいて取り組むべきと思います。