第９回　成長戦略ワーキング・グループ
議事概要

１．日　時：令和３年４月27日（火）10:00～11:33

２．場　所：オンライン会議

３．出席者：

（委　員）大橋弘（座長）、髙橋滋、武井一浩、南雲岳彦

（専門委員）落合孝文、玉城絵美、村上文洋

（政　府）河野大臣、田和内閣府審議官

（事務局）山西規制改革推進室次長、吉岡参事官

（説明者）筑波大学　佐久間教授

東京大学　山口特任准教授

ソラミツ株式会社　宮沢代表取締役社長

国士舘大学　吉開教授

京都大学　稲谷教授

千葉大学　西貝准教授

法務省刑事局　吉田刑事法制管理官

法務省刑事局　栗木参事官

警察庁長官官房審議官（生活安全局担当）　檜垣審議官

４．議　事：

（開会）

１．デジタル時代における刑事法の在り方について

（閉会）

５．議事概要：

○大橋座長　それでは、定刻となりましたので、ただいまから「規制改革推進会議第９回成長戦略ワーキング・グループ」を開催したいと思います。

本日もウェブ会議ということで、オンラインで開催しております。お手元に資料を御準備いただいて御参加いただければと思います。

本日は、河野大臣にも御出席いただいております。

まず初めに、河野大臣から一言、御挨拶をいただければと思います。なお、本日は、河野大臣は冒頭のみの御出席となっております。お忙しいところありがとうございます。

よろしくお願いします。

○河野大臣　おはようございます。お忙しい中ありがとうございます。

デジタル時代の刑事政策の在り方について、今まであまり政府内でも議論がなされていなかったようなことを聞いております。経済政策の観点から刑事法が議論されたことがあまりなかったようでございます。

しかし、そういうわけにもいきませんので、熱心に御議論をいただいて、今後、経済、産業そして刑事政策をどのように連携させていったらいいのか、問題提起をしっかりしていただきたいと思っております。

今日は、本人認証、それから、デジタル通貨を取り上げていただくということでございます。

今まではIDとパスワードで本人認証をやっておりましたけれども、今回のワクチンの接種でもシステムが乱立して、IDとパスワードがいっぱいあってよく分からないということになったので、IDとパスワードを共通化して医療機関に使いやすくできないかということをやりましたけれども、新しいIDとパスワードに代わる認証方法が続々と誕生しております。

シンガポールに行きますと、日本のマイナポータルに当たるものに入るのは、携帯番号の登録と本人の顔認証だけで、懐から携帯電話を取り出すや否や、もう日本のマイナポータルに当たるところに入れる状況になっております。

しかしその一方で、顔認証などを誤認させるなりすましも開発されているという話がございますので、こうしたものを規制の観点からも対応を検討する必要があるのだろうと思います。

また、デジタル通貨の議論が大変に白熱をしております。日銀もデジタル通貨に関する議論をスタートすることのようでございます。

既に、カンボジアとかバハマでデジタル通貨をもう導入しているという話があります。今日は、カンボジアのデジタル通貨を共同開発した事業者からも御説明があると聞いておりますが、もう既にカンボジアの1600万人が送金や店舗での支払いに利用されていると聞いております。

また、これまでミャンマーとかマーシャル諸島、マン島、ラオス、カリブの様々な島々でもいろいろ動きがあると聞いております。

日銀のみならず世界の中央銀行の９割近くが、デジタル通貨に関する研究を何らかの形でやっているということですので、そうなると通貨偽造罪などを含めた刑事法の在り方が必要になってくると思います。

それ以外にもいろいろな観点があると思いますので、技術と刑事法の両面からしっかり御議論をいただく必要があると思いますので、どうぞよろしくお願いを申し上げます。

今日はありがとうございます。

○大橋座長　御挨拶ありがとうございます。

それでは早速、議題の１「デジタル時代における刑事法の在り方について」に入りたいと思います。

ヒアリングとして本日は、筑波大学より佐久間教授にお越しいただいております。佐久間教授、お忙しいところありがとうございます。

10分程度、御説明のお時間をいただいているということですので、御準備よろしければ

ぜひお願いできればと思います。
○筑波大学（佐久間教授）　筑波大学の佐久間です。今日はどうぞよろしくお願いいたします。
それでは、「AIによる誤認識・偽造・差別の問題」というタイトルで少しお話をさせていただきたいと思います。
御存じのとおり、AIの画像認識能力は年々性能を向上させておりまして、今は人間の認識能力を超えるところまで来ております。
そういったような、単純な問題に限って言うとですけれども、人間のエキスパートの能力を達成しているときに、AIに一体、何を望んでいるのかなのですけれども、ただ単に文字認識で行っているような正確に認識をされているということだけではなくて、人間の人生とか命を左右するような重大な判断にAIが使われていくことが考えられるわけです。
そういったときには、AIによる判断はただ単に正確なだけではなくて、安定していることが重視されます。安定しているとはどういうことかというと、多少の変化に影響されないということです。例えば車載カメラの自動認識であれば、天候に左右されないとかノイズに左右されない、あるいは外部の攻撃者が意図的に攻撃を仕掛けたときにもそういったものに対して左右されないといったような性質が重要になってきます。
そのときに問題とされるのが、敵対的サンプルと呼ばれる問題です。この敵対的サンプルというのは、攻撃者がAIに攻撃を仕掛けたときに発生するタイプの問題です。
具体的には、左側の画像はパンダの画像です。この画像は、人間にはパンダにしか見えません。これをAIに認識させると当然パンダと認識します。
一方で、一番右側の画像は、真ん中にあるようなノイズを加えた画像になっています。人間には見えないぐらい微弱なノイズなので、相変わらず人間は一番右の画像をパンダと認識するわけですが、これをAIに認識させるとテナガザルと認識します。
こういったように、人間には見えない微弱なノイズを加えることで、AIの認識を操作してしまうことができることをこのエグザンプルは示唆しています。
具体的に、例えば道路標識にこういったステッカーを貼ることによって、車載カメラの標識認識機能を攪乱させることができるという実験も行われています。
この実験では、ストップサインにここに書いてあるような特徴的なステッカーを貼ることによって、標識の認識をストップサインからスピードリミットの標識に変更することに成功しています。
これが何を意味するかというと、普通ストップサインがあれば自動車は止まらなければいけないわけですけれども、このステッカーが貼られていると自動車はそこで止まらずにそのまま直進してしまう可能性があるわけです。そういった攻撃が現実に可能であることをこのエグザンプルは示唆しています。
そして、これは我々の研究室の研究結果なのですけれども、同じような攻撃が音声に対しても実施可能であることを示しました。

具体的には、ここで行った実験は音楽に対して特殊なノイズを加えることによって、人間には音楽にしか聞こえませんが、これをAI、例えばスマートフォンとかスマートスピーカーに認識させると、ある種のボイスコマンドに認識されるタイプの攻撃を行うことができることを示したものです。

音声の敵対的サンプルの場合は、スピーカーとかラジオとか、そういったものを通じて広く拡散するリスクがあります。例えば今ここで私がこういったノイズを私のパソコンの前で鳴らすことによって、皆さんのiPhoneに対して何らかのボイスコマンドを皆さんに気づかれずに送ることができるリスクがあるということです。

こういったように、今回お示しした様々な攻撃というのは、人間が行っていると言えば行っているのですけれども、そういった特殊なノイズを生成する際にAIを使っています。そして、対象もAIです。したがいまして、それを守るのもAIの仕事ということになります。

攻撃者というのは常に防御するためのAIを上回るような攻撃のためのAIをつくろうとしますので、こういったAI同士のいたちごっこになってしまうのですけれども、逆に言うといたちごっこを続けること自体が、AIの安全性を守ることにつながることになります。

したがって、ディフェンスのための研究を常に続けていかないと安全性は維持できないということが言えるのではないかと思っております。

少し毛色が変わりますが、現代のAIは非常に、人間の目には本物にしか見えないような画像とか音声とかテキストというものを無限に生成することができます。

左上の図は、一番上の列は実在する人間の顔画像です。その下の画像は、実在する人物に見えますが実際にはそうではなくて、AIが生成したフェイクの顔画像です。ここにあるように、実在する人間にみえるような画像は無限に生成することができます。

右側は本来、動画なのですけれども、右側の人間の顔画像を左側、これはオバマ元大統領ですけれども、これにすげ替えて動画をつくることができるような技術です。こういうものは偽物をつくるという意味でディープフェイクと呼ばれるのですが、これはいろいろと問題があるわけです。

例えばこういったものを使って有名人の顔画像をすげ替えることによって、偽造ポルノをつくったりとか、あるいは証拠を捏造したりとかそういったことに使われます。あるいは、政治的には実在しないニュース、言葉を実在する人物にしゃべらせることによってデマを発生させたりとか、そういうことができます。

また、動画だけではなくて文章でもそういったことが可能になります。要するに、虚偽の内容の長文のテキスト、人間が書いたものと見分けがつかないような長文テキストを大量に生成して、例えばそれをTwitterなどにどんどん投稿することよってデマを巻き起こしたり、世論を誘導したりといった心理的というか、世論を誘導するようなタイプの攻撃というものもAIで可能になります。

ポイントは、人間でももちろんこれはできるわけなのですけれども、AIがやることなので巧妙かつ大量に自動生成できるところが、やはり気をつけなければいけないところかな

と思います。

それから、AIによる差別という観点についても、気にする必要があるかなと思います。

これは米国の例なのですけれども、コンパスアルゴリズムと呼ばれるものが知られておりまして、ある被告人を保釈するのか仮釈放するのか、あるいはどういった判決を下すのかということを考えるために被告人の過去の経歴とかどういった犯罪を犯したのか、あるいは人種とか年齢とかそういったデータを使って再犯リスクを予測するアルゴリズムが使われています。

このコンパスアルゴリズムにおきまして、ある報道の方なのですけれども、再犯リスクスコアリングは人種の影響を受けていることを統計的な調査によって見つけ出しました。具体的には、人種が白人だと実際には再犯リスクが高いのにスコアリングとしては低く判定している。有色人種の場合は実際には再犯リスクが低いのに高いリスク評価をしてしまうことが差別を生み出していることを主張しています。

こういったようにアルゴリズムによるスコアリングが差別を生み出すという問題も重要かと思っています。

AIが社会に信頼されるためには、必要条件としては精度の高い判断をすること。それから、法令を遵守していること。これが必要条件とはなるわけなのですが、冒頭に申しましたとおり、その制約といいますか信頼性を高めるための手足を縛るような部分も非常に重要になっていきます。

具体的には､環境変化や攻撃に対して安定な判断をしなければいけないこと｡それから、プライバシーとか差別がないといった人権を尊重するような範囲内で判断をしなければいけないということ。

AIが下した判断に対して、その根拠が説明できるということ、判断過程がクリアであることが、例えばAIがもし間違えた判断を下したときに、それを事後的に検証するためにも必要になってくるかなと思います。

AIの判断の品質のクオリティーを守るための様々な技術的な検討が必要かと考えています。

私からの説明は以上になります。どうもありがとうございました。

○大橋座長　どうもありがとうございます。

後ほど、また意見交換させていただければと思いますので、続いてのヒアリングに移ります。

次は、東京大学より山口特任准教授にお越しいただいています。お忙しいところありがとうございます。

10分ほどお時間いただいているようですので、御説明をお願いいたします。

○東京大学（山口特任准教授）　東京大学の山口でございます。

「近年の個人認証の傾向」ということで、私からお話をさせていただきます。

そもそも、個人認証は何だっけと考えてみますと、実は登録した人とインターネットで

端末を通じて連絡をしてくる人が同一人物であろうかということを確認する手段を言います。

ですので、当たり前の話ですけれども、登録の時点で本人が違っていた場合は、ずっと継続がされることになりますし、ここが何らかのはずみで利用のときに違う人にすり替わってしまったらそれを見出すための努力をすることになります。

個人認証の３要素というのは、古くから３要素と呼ばれている手法がございまして、それは知識、所持、身体的特徴という要素がありました。IDとかパスワードと言われている世界とか、マイナンバーカードに代表されるようなICカード、顔認証とか指紋認証で出てくるような身体的特徴を見出したようなバイオメトリクスの認証手法がございますが、最近は行動を活用した認証が広く利用されるようになってきました。これは後から御説明しますが、皆さん既に御経験があることかと思います。

ただ、行動の場合は、人間の行動は全く一貫性を持って同じ行動を取ることはほぼなくて、私たちの言葉では揺らぎと呼んでいますけれども、行動には揺らぎがあるのでその揺らぎをどう是正するかということで、ある程度、認証のスコアを下げてあげて、その代わり複数の要素で多要素認証をするのが割と一般的になってきています。

法律的には、識別符号と書かれていると最近勉強しました。まだ私も勉強不足なので、今日もし議論があったら教えていただきたいぐらいなのですけれども、一般的に２つに認証は分かれると整理ができるかと思っています。

例えば記憶とか所持の絶対的な情報は左側に当たるようなところにありまして、計算量とか情報量によって表現されていて、ムーアの法則と呼ばれているCPUの進化とスピードというのが大体計算量によって表現されているものがありますけれども、それによって安全なビット数を決めて、例えばパスワードは10文字以上入れましょうとか記号を入れましょうとかいろいろありますけれども、その長さもムーアの法則に沿って出てきた計算量で表現されています。

また、ICカード、マイナンバーカードもそうですしクレジットカードとか一番身近で使われていると思いますけれども、そこに内蔵されている暗号の種類であるとか、チップの安全性もこういった絶対的な指標よって表現をされています。

ただ、計算量で評価をされる場合は人間のパスワードの漏えいとか、人のミスみたいなことがセキュリティーのモデルの外として整理をして安定性を評価しています。数学的に表現できないことを外に出すことで100％安全ですというものをつくっています。

一方、最近はやってきている生体認証とか行動の情報というのは実験的とか、統計的に他者と区別がついたことによって評価されます。

典型例が生体認証、指紋認証は指紋がほかの人と絶対に一致しませんと皆様思い込んでいると思いますけれども、それは誰かが示してくれたわけではなくて、実験的、経験的に一致する人がたまたまいなかったから、生体情報は一人一つしか持っていないのですということを示しています。

ですからもしかして、バースデーパラドックスとか言われますけれども、たまたま全く同じような指紋を持つ人が世の中にいるのかもしれない。けれども、世界中の人の全部の指紋をつくったデータベースは存在しないので、多分大丈夫でしょうということでやっています。

行動データは、最近IPアドレスとか位置情報とかそういったもので区別する情報でやってきていまして、それを多要素でやることが多いですけれども、これも経験的に安全性を表現しています。

ですので、逆に言うと生体情報も行動データも100％になることはありません。

行動データを活用したと昨今言われていますけれども、例えばこんなメールを皆様お受け取りになったことはありませんか。このアクティビティに心当たりがありますかとかというメールが来たり最近はいろいろなサービスでやるようになってきました。

これはリスクベース認証と、とある会社が名づけていましてそう言われることが増えてきています。端末のOSの種類であるとか、例えば機種変したときのスマホの情報、ブラウザのIPなどからも位置情報の情報からふだんのアクセスと違うかで判断しています。最近は減ってきましたけれども、海外出張に行くとあなたは本物ですかと聞かれることが多いですよね。そういったことになります。

あと最近は、周辺のWi-Fiの情報とかBluetoothの情報を活用してやるような認証も出てきていますし、研究としても最近はセキュリティーのトップカンファレンスでも行動データを活用した認証の研究が盛んに行われるようになってきました。実用化が先だったかなという印象でもあります。

今日は、この中でも私たちがやっている実験の具体的な例をお見せします。

先ほど申しました行動の電波の情報を活用した事例についてお話させていただきます。

では、再生させていただきます。

（動画再生開始）

○東京大学（山口特任准教授）　これは、行動認証によって本人が認証されていた場合は、本人が近づくとドアが自動的に開いて物を買えるという一つのデモンストレーションです。

このように周りの電波情報を利用して、本人が本人と確認されたときのみ物を買って、これは実験的にお見せしていますけれども、実は一つ一つの商品にICチップが乗っていましてそのチップによって決済をして、実際のクレジットカードで決済をするようなデモンストレーションもしておりまして、これは本当に普通にクレジットカードで決済をしてお金を引き落とすところまでつくり込んでいます。

ここは今、マルと出しているのでドアが開きましたけれども、本人と認められないような行動パターンを取った場合は、今日はデモンストレーション的に簡単な一番短いものをお見せしているのですけれども、バツと上に出てきてパスワードを入力してくださいと出るようになっていて、そこが多要素認証なのですけれども、パスワードでもログインして本人が買物できたりすることがあります。

（動画再生終了）

○東京大学（山口特任准教授）　リスクのことを考えてしまうと、いろいろ切りがないので、あんまりくどくど言っても仕方がないという気分になったりするのですけれども、もちろん登録の時点とか生体認証の登録が不完全な場合はリスクが生じることもありますし、IDとパスワードの問題だけ言いますと、やはりユーザーはたくさんのパスワードは覚えられないからほかのところでも同じパスワードを使っていてそこが漏えいしてみたいな、パスワードリスト攻撃と呼ばれている攻撃、偽造の生体情報がつくられたり、単純に言うとカードを落としてしまったときにほかの人がカードをつくったりとかカードのコピーがあったり、いろいろな問題が起きてきます。

安全性評価の場合は、リスクをうちに含めるか外とするかによって表現をしているわけですけれども、経験的に言うと絶対100％にはならないので、どの辺りで妥協するかという議論になります。

個人認証の問題は決して新しい問題ではなくて、私が学生のときの20年以上前からIDとパスワードは問題だといろいろな人が言っていますけれども、利用は全く減っていません。ICカードなどはセキュリティー上安全だと言われていますけれども、利便性の観点から利用が進んでいない現状もあります。

一方で、例えばクレジットカードの事例を皆様思い出してみてください。クレジットカードはお店で決済をするとき、例えばコンビニでやるときはPINを聞かれないですけれども、大きなレストランに行くとPINを聞かれたりとかサインになったりということを表現しています。

これは、そこの店舗で買物をされる平均の金額というものが計算されていて、安全性をお金で表現をしていて、便利なほうを取っているのですね。例えば限度額が高いゴールドカードというのはチップが高額なのです。有効期限も３年ぐらいで短くなっていてころころカードが来るようにできています。

一方で、デパートで使うようなデパートカードというのは限度額が10万円だったりするような安いカードがありますけれども、その場合は、有効期限は実は10年ぐらいになっているのです。

ここら辺が費用対効果の観点から、どういった辺りで安全性を重視するか。ゴールドカードとかプラチナカードとかクレジットカードの高いカードは、一度の買物で車が買えたりするほど高い物が買えたりしますので、その辺りがどの辺りに攻めてくるかというのがクレジットカードはすごくよくできていて、こういった考え方をふだんの事例にどういうふうに進めていくかというのが難しいところかと思います。

経験的なリスク評価をする時代になったのかとも思っていまして、現実的な手法を取ることがどんどん増えていくかと思っています。

一方で、行政のIDとパスワードの問題は、無謬性と言われている行政はミスしてはならないみたいな昔から言われている流れと、現実的にクレジットカードのようにお金で払っ

てしまえばいいという解と、どの辺りでプラスにするかマイナスにするかみたいなところを取っていくのかがとても難しいなと最近は感じています。

私からは以上でございます。

○大橋座長　ありがとうございます。

後ほど、また意見交換をさせていただければと思います。

続きまして、ソラミツ株式会社にヒアリングを行います。本日は、宮沢代表取締役社長にお時間をいただいております。お忙しいところありがとうございます。

早速ですけれども、御説明の時間10分いただいているということですので、お願いできればと思います。

○ソラミツ株式会社(宮沢代表取締役社長)　ソラミツ株式会社代表の宮沢でございます。

それでは、御説明いたします。

最初に簡単に自己紹介ですが、私は東京工業大学の特任教授、それから、ISOのブロックチェーン国際標準化の日本代表委員、日本銀行の委員、内閣官房の委員等を務めております。

経歴としましては、交通カードのSuicaの開発、それから、電子マネーEdyの創業、金融庁の金融審議会の委員も務めまして、資金決済法の第一次の立法もお手伝いをさせていただきました。

その後、カンボジア中央銀行のデジタル通貨の開発の総責任者として、デジタル通貨の開発をしてまいりました。最近、世界初の中銀デジタル通貨バコンという本を出版いたしました。

私どもの会社が開発しましたブロックチェーン技術でございますけれども、実は我々の開発した成果物は全てThe Linux Foundationという組織に無償で譲渡をしまして、世界の資産として世界中のエンジニアが皆さんで開発をするというオープンソースになっております。全世界260社の中から３社が選ばれまして、IBM、インテル、ソラミツの３社を世界標準として育てていこうということで進めております。

様々な監査・安定性・耐久性をテストしまして、世界中の政府、自治体、金融機関が安心して使えるようなものになっております。

また、オープンソースですので、我々の企業がたとえ消滅しても、技術は存続するという継続性がございます。

その結果、様々な世界中の企業、政府から採用されておりまして、カンボジアの国立銀行、モスクワの証券取引所、インドネシアの銀行、スイス等で採用されております。国内におきましても、会津若松等でブロックチェーンを使ったデジタル地域通貨、日本初の正式運用をしておりますし、保険会社、証券会社等、またインターオペラビリティということで世界中のブロックチェーンをつないでいくプロジェクトのPolkadotというところの役員をやっております。

非常に高速大量処理ができて、１秒から２秒で決済が終わったり、１秒間に5,000件程度

の処理ができる、また電力を使わないということで地球資源にも優しい。このようなブロックチェーンでございます。

昨年の10月28日にカンボジアの中央銀行で、世界初の中央銀行デジタル通貨正式運用に成功しました。現在、1600万人の国民が使用を始めておりまして、実はほとんどの国民が銀行口座を持っておりませんので電話番号で送金したりQRコードで支払ったりしております。

この仕組みなのですけれども、実は非常に強固な本人認証をしておりまして、なりすましを完全に防ぐ。ID、パスワード等は一切使っておりません。二要素認証というPKIの秘密鍵と指紋等の二要素認証で行っております。

なぜ中銀デジタル通貨をカンボジアが早く導入したかという背景なのですが、現在、日本のように既に５年以上前にキャッシュレス決済手段が乱立しまして、相互運用性がない、決済手数料が高い、それから、加盟店の資金繰りが悪化する、決済事業者の倒産・不正などのリスクがあるという問題が起きました。

そこで、カンボジア政府は２つの案をつくりまして、１つは既存の銀行ネットワークにキャッシュレス利用者をつなげるという案ですが、これにつきましてはコンプライアンス・システム対応コストが非常に決済事業者にとって重荷になるということで反対がありました。

Ｂ案につきましては、中銀デジタル通貨を整備しまして、そこに銀行やキャッシュレス決済手段が使用する方式でございます。この場合には、コンプライアンス・システム対応コストは低くて済む。当然、リスクも起きないということでございます。

実はカンボジアの官僚の方々を非常に私も感心したのですが、シリコンバレー等に留学をしておりまして、技術に非常に明るい。世界中の技術の勉強をし、５年前ですけれどもブロックチェーンの技術が最も適正ということでＢ案を選択しております。

今までのキャッシュレスとの違いですが、特に日本のキャッシュレスの仕組みとクレジットカードの仕組みは、店舗に対して支払い指図をする場合、実際にお金の価値が店舗に行っているわけではなくて、その電文を集めて１か月に１回、銀行口座に振り込む形になっております。いわゆる支払いがファイナリティがない。後から、銀行口座にお金が流れ込むというふうに、２つの金流と実際の商流が完全に分断している仕組みでございます。そのため、店舗の資金繰りが苦しくなる。それから、非常に複雑でございまして、複数の銀行を経由するために高コスト。

それに対しまして新しい流れ、世界的に今回のカンボジア、それから、中国のデジタル人民元、あるいはフェイスブックのリブラ等は、デジタルデータそのものにお金の価値がございまして、これが利用者から店舗に移る。現金と同じように、その時点で中央銀行ファイナリティがあるということで、決済に基本的に銀行が介在しないやり方でございます。

そのため、受け取った店舗はすぐに利用ができる。資金繰りが改善され、大幅に簡素化されまして、決済コストが10分の１から20分の１ぐらいに下がっております。

また、台帳の持ち方で比較しますと、現在の決済システムは中央銀行を中心としたピラミッドになっておりまして、複数の台帳をそれぞれ銀行、決済事業者が持っている。これは、つじつまを合わせながらクリアリングしていくということで、非常に複雑な仕組みになっておりますが、新しい考え方は基本的に国で１つの台帳を持っている。ブロックチェーンで複数に分散されておりますが、１つの台帳に対して中央銀行、銀行、決済事業者あるいは利用者がアクセスをするやり方でございます。したがって、非常にシンプルでクリアリングが不要になり、コストが大幅に下がる。中国のデジタル人民元もこれと同じ考えでございます。

キャッシュレスとデジタル通貨と比較しますと、今までのキャッシュレスは主にお店での支払いというB2C、あるいは今、厚労省で審議をされております給与のデジタル支払いが解禁になりますと、デジタルの支払いができるようになりますけれども、企業間のデジタル決済等には対応ができないということになります。

それに対しまして、デジタル通貨はB2C、B2E、B2Bといった幅広い現金の市場を全てクリアできるものでございます。

また、転々流通で地域内の経済循環によって、30倍から40倍の経済効果がある。あるいは、そのお金自体にプログラムを書くことによって、減価するマネーによる経済活性化等ができるというものでございます。

特に法人決済にこのデジタル通貨を使いますと金流と商流が一体化し、例えば入金の消しこみがいらないなどの非常に業務の効率化が図れるということが言われております。

もう一つ、本人認証のところでございますけれども、内閣官房のIT総合戦略室で官民推進会合が過去６回開かれておりまして、その中でマイナンバーとひもづけをする分散型IDの議論がされております。

これはスマートフォンにデジタルIDを入れまして、それを健康、交通、購買様々なものに使っていこう。あるいは、法人IDという形で企業を結びつけていこうということで、IDの共通化という議論がされております。

この分散型IDですが、いわゆるマイナンバーカードとの位置づけは、マイナンバーカードは一種の実印であろう。それに対しまして、分散型IDはスマホに格納しまして認印・銀行印的に様々な用途に使う。このような扱い方を想定しております。

分散型IDは中立的で特定の企業に依存しないW3Cの世界標準技術でございまして、地域ごとに分散して発行しても重複はしない。中央認証局が不要である。一応、登録すれば自分の個人情報は自分の意志で企業に提供ができるワンスオンリーを実現しております。

私の説明は以上でございます。ありがとうございました。

○大橋座長　どうもありがとうございました。

後ほど、意見交換させていただければと思います。

続きまして、国士舘大学より吉開教授にお時間をいただいております。吉開教授はクラウド時代における捜査実務が直面する問題点に加えて、事務局から後ほど御説明がある意

見書、骨子案についてもコメントを若干いただきたいと思います。

それでは、御説明のお時間を10分程度いただいているということですので、早速ですがお願いいたします。

○国士舘大学（吉開教授）　よろしくお願いいたします。国士舘大学の吉開と申します。

最初に私のバックグラウンドを簡単に御説明させていただきますと、平成９年に検事になりまして、17年間検事をやっておりました。うち10年ぐらいは捜査に関わっておりまして、東京地検と大阪地検の特捜部に通算して７年間ぐらい在席しておりますので、それなりに捜査のことは分かっているつもりではあるのですが、ただ平成26年に現職に転職しまして、それからは現場を離れておりますのでそういった限界があることは御理解いただければと思っております。

本日、お話しさせていただきたいと思っているのは、私が考えているところでございますが、電磁的記録、データを犯罪捜査の証拠として収集することを巡る混乱についてのお話でございます。

まず最初に、犯罪捜査における客観証拠の重要性ということで、客観証拠というのは例えば殺人事件の凶器でありますとか、あるいは粉飾決算の事件であれば契約書とか会計帳簿などということになりますけれども、そういったいわゆる物証と言われるものが非常に重要である。

その理由として、「供述証拠は不安定」と書きましたが、いわゆる証人の証言とか、被疑者、被告人の自白が供述証拠になるわけですけれども、人の話というのは見間違いや聞き間違い、記憶違い、あるいはうそが入りますので、非常に不安定で確実な証拠ではないところがある。ですので、犯罪捜査の現場では人に聞くよりものを見よと言われたりしますが、客観証拠をまずは見ましょうと。

ただ、客観証拠だけで捜査ができるかというとそうでもありませんので、当然、取調べをして話を聞かなければいけないのですが、捜査機関に十分な客観証拠の収集手段を与えることは、昨今海外からも若干批判がございますけれども、取調べというものに対していろいろ厳しい見方もございますので、こういった証言とか自白を取るための取調べの比重を相対的に減らすことができる。完全になくすことは無理だと思いますが、客観証拠の収集手段を与えることはそういった取調べの比重を減らすことにもつながることがあると思います。

そうなってきますと、客観証拠を集めなければいけないわけですが、現在の法律で客観証拠を集める中心的な手段は捜索差押えになっておりまして、ある場所に行って証拠物などがあるかどうか探すのが捜索であり、見つけると差押えということで取り上げて証拠にすることになるわけなのですが、これはいわゆる強制処分ということで裁判官が発した令状に基づいて実行するのが原則になっております。

捜査は本来任意です。相手方の同意とか承諾を得て、協力を得てやるのが原則なのですけれども、御案内のとおり犯罪をする人たちの中には必ずしも協力的ではない人が多いの

も事実でございますので、強制手段というものがないと真相解明は難しくなってくるところがございます。

こういった捜査機関の権限強化の話をしますと、弁護人とのバランスで被疑者、被告人の人権保障との関係で問題はないのかという御指摘もあろうかと思うのですが、現在は平成16年に法律が改正になりまして、証拠開示制度が整備されております。ですので、それ以降はいわゆる客観証拠であれば、今言ったような物証であれば弁護人も捜査機関が集めた証拠を見ることができるようになっております。

それからしますと、最終的に弁護人のほうでそういった証拠を見てチェックができる点からしても､客観証拠をより広く集められるようにする権限を捜査機関に付与することは、真相解明にとっても重要なのではないかと私的には考えております。

（２）に参りまして、「デジタル時代の影響」なのですが、今日のお話でお分かりのとおり客観証拠はもう物証ではなくてデータになってきている。もう契約書とか帳簿などもほとんどデジタル化している状況で、こういったデータになってまいりますとパソコンの中に入っておりますので、パソコンを開いて中を確認しないと確認ができない。昔の紙媒体であればすぐわかったわけですけれども、今は紙媒体ではなくなっている問題があります。

また、データは御案内のとおり改変消去が大変容易で、すぐにディレートできます。さらに、非常に大量に存在している。消さない場合も多いので、紙の場合は整理したりもするかもしれませんが、データは非常にコンパクトに収納ができますので、あまり消されずに残っているということで非常に大量にあるといった特徴がございます。これは、犯罪捜査にとっては非常に困難な問題を引き起こしていると言えます。

さらにもう一つの問題が記録媒体、これはデータの保存先と私のほうで説明をつけましたが、このデータを保存する先がかつてはパソコン本体のハードディスクに大体皆さん保存されていた、あるいはフロッピーディスクとかUSBメモリなどというものに保存されていたと思いますが、現在はクラウド化している。

このクラウドというものが引き起こした問題としましては、日本国憲法は、先ほど申し上げた捜索差押えのための令状には場所を明示しなければいけないということを要求しております。例えば私の研究室に捜索差押えに入るのであれば、私の研究室と特定しなければいけない。その令状を使ってほかの先生の研究室に入ってはいけないことになります。

ところがクラウドは、御案内のとおり私の研究室にはございませんので、クラウドのサーバはほかの場所にございます。そういったほかの場所にあるデータを、私の研究室という場所を明示した令状で差押えていいのかという問題が出てきた。

こういったデジタル時代の影響を踏まえて最近、混乱しているのではないかと考えるところが、ＡとＢとＣという３パターンに分けて御説明申し上げますと、かつてのようなパソコン本体、例えばＣドライブに保存されたデータということであれば、これは今までどおりの捜索差押えの令状で対応ができます。

ところが、クラウドの発達に伴いまして、データが場所の外にあるサーバに保存されている場合で、サーバが国内にあるということであれば平成23年に法改正が実施されましてリモートアクセスという方法が導入されました。

このリモートアクセスは、例えば私の研究室に対する捜索差押え令状があれば、そこのパソコンを使ってそのクラウドのサーバに保存されたデータを捜索差押えしてよいという制度になります。

これでクラウドができたことによる問題点はかなり解消されたと思われたのですが、ただリモートアクセスできるのは差押え前に限ると。要するに、私の研究室のパソコンからクラウドのサーバにリモートアクセスをして､データを私のパソコンにダウンロードする。そのダウンロードしたデータを差し押さえてくださいという仕組みになっているのですが、差し押さえる前にリモートアクセスしなければいけないということが法文上もそうなっておりますし、裁判所の裁判例でもそのように示されております。

その結果、問題として出てくるのが、例えば捜索差押えの現場で、私のパソコンにIDとパスワードがかかっている。それはロックを外さなければ見られないわけなのですが、例えばそれを私が捜査機関に対して拒否すると､捜査機関はどうしようもなくなってしまう。中が見られないということになってしまいます。

例えばID、パスワードのロックを外す方法というのは、捜査機関から専門機関に依頼すれば可能かと思いますけれども、では一旦そこで差し押さえてしまって、例えば警察でロックを解除して、それから、リモートアクセスしましょうというのは違法になってしまうという問題がございます。

また実際問題、捜索の現場でいろいろなものを差押えするわけなのですが、実際に時間がたくさんあるわけではなくて、かなり短い時間に証拠になる物を確認して捜索差押えは終了しないと、何日もかかってしまうことも場合によってはございます。ですので、その場で確認できる限りで確認して差押えをしてきて、パソコン本体のデータを確認していたら、どうもこれはクラウドにデータがあるようだ。では、そのクラウドのデータについても確認しないと捜査が十分できませんというときに、差押え後にリモートアクセスすることができるかという論点も生じています。

これについては、いろいろな考え方がございますが、まだ確定した判例などは出ていないところで、この辺でも若干問題が出ていると言えるかと思います。

さらに問題がＣの場合で、クラウド上のデータでサーバが国外にある場合に、主権侵害の問題がある。国外の捜査は、基本的にそれぞれの国の主権がございますので、国際捜査共助によらなければいけないので、それによらずリモートアクセスをするのは違法だという裁判例が出ました。

この裁判例についてはいろいろ意見もあるところですが、最近、最高裁で判断が出まして、サイバー犯罪に関する条約の32条に基づき、データが同条約の締約国に所在し、正当な権限を有する者の合法的かつ任意の同意があればリモートアクセス可能だという解釈が

出されております。

ただ、これは合法的かつ任意の同意ですので、正当な権限を有する者が同意しなかった場合には国外サーバにアクセスできないことになってしまいますし、もう一つ指摘されているのが、サーバの所在国が必ずしも確認できる場合ばかりではない。そうすると、そもそも国際捜査共助によりなさいと言われても、どこの国に共助をかければいいのかという問題も出てきていると聞いております。

若干のコメントということで、エンフォースメントの実効性を維持するには、手段の検討も非常に重要ではないかと現場にいた人間としては考えます。

意見書などを拝見しますと、やや規制をする法律をつくる方向の議論に寄っているような印象を受けますが、やはりそこは実際に実現する手段を考えていく必要があるのではないかというところと、現状論を踏まえてあるべき論を議論されたほうがいいのではないかと思います。

とりわけ、私は現場におりましたので、結局、法律をつくってもそれを使うユーザーになるのは現場の人間でございますから、現場の声というものもできる限り組み上げていただきたいということ。

あとは現実問題として、日本では刑事罰は最終的手段という認識が強い。また、取引とか偽計といった手段は、私もより日本でも入れていくべきだとは考えておりますが、国民全体に非常に嫌悪感が強い。捜査機関は清く正しくなければいけなくて、そういった取引とか偽計を使うことはいけないことなのだという認識がなかなか変わってこない。少しずつ変えていかなければいけないと思いますが、そういったところも踏まえて議論をしていかないと、いきなりあるべき論でぽんといっても、ついてこないのではないかという印象がございます。

あとは、今回ご紹介したサイバー犯罪条約は、国際的な解決方法として条約の見直しというか、追加議定書の作成について話が進んでいるとも聞いておりますが、そういったもののみならず、国内的な解決方法として、立法や解釈、できる限り現行法の解釈で対応できる方法を考えることと、それがどうしても駄目な場合に立法での対応を考えるところを模索していく必要があるのではなかろうか。

刑事法の業界は、とにかく刑罰は最終的手段ということで、先手を打つのがなかなか難しくて、どうしても後手に回りがちであるところは現状論として御理解いただいたほうがよろしいのではないかと思っております。

私のほうからは、以上でございます。

○大橋座長　ありがとうございました。

後ほど、また意見交換させていただきます。

続きまして、事務局から今般２回にわたる刑事法の議論に係る意見書の骨子案ということで、５分程度御説明をいただければと思います。

○吉岡参事官　事務局から説明いたします。お手元の資料１－６を御覧いただければと思

います。

前回の議論を踏まえまして、目次のとおりに項目を立てさせていただいております。

早速でございますが、２ページ以降を御説明させていただきます。今回、御議論いただくものについては反映をしておりませんので、御容赦いただければと思います。

まず「はじめに」のところでございますが、黄色いマーカーに沿って御説明いたします。

サイバー空間の脅威は、非常に身近になっている。それから、サイバー犯罪と技術の対策はいたちごっこになっているので、法規制の双方から抑えていく必要があるということ。経済活動は、法制度と密接な関わりがありまして、刑事施策も例外ではなく、不断の点検整備が必要であること。経済社会の基盤として刑事罰の議論は避けて通れないものといったことを記述することになろうかと思います。

２番目でございますが、「Society5.0時代に出現する身近な脅威」といたしましては次のようなことを記述することかと思います。

まず、未知の攻撃が今後到来するであろう場合には、広範囲に甚大な被害を招来するおそれがあるということでございます。

３ページ目でございますが、このような甚大な公益侵害はいきなり生じる可能性が高く、具体的な事件が生じる前に先手に対応することが必要なのではないかという問題点もございます。

具体的な脅威としましては、次のようなものを紹介するのがよろしいかと思っております。具体例の１つでございますが、2015年にはアメリカの自動車メーカーＡ社が、外部からのハッキングによって遠隔操作され、車両140万台についてリコールを発表したことがございました。

それから、３番目でございます。「デジタル時代における経済と刑事法の関わり」としまして、次のような内容を記述してはいかがかと思っております。

１つ目でございますが、刑事法はデジタル時代のイノベーションを支える一翼を担うものであることを再認識することとございます。

４ページ目でございます。４ポツ目、刑事法の検討体制の在り方についてでございます。次のような内容を記述することが妥当ではないかと考えております。

１つ目が、刑事司法分野の関係者とデジタル技術の関係者が積極的に意思疎通を行うこと。経済政策を所管する部局と刑事を所管する部局が協力して議論を行うこと。特別な部会や会議体を設置するような必要があるのではないかということでございます。

５番目でございます。刑事法の総論的な考え方について、次のような内容を記述してはいかがかと思っております。

まず１つ目でございますが、現在の刑法はデジタル部分につきましては複数の類型が積み重なって複雑化してきました結果、一般人にとって体系的、制度的に理解しにくくなってきているということ。

それから、デジタル関係の犯罪は今や既存の犯罪に付随した犯罪と捉えることは必ずし

も実態を反映してはいないということ。このため、一括して体系だった整理が必要ではないかということでございます。

５ページ目でございます。「デジタル時代における構成要件と違法性阻却事由のあり方」でございます。

構成要件につきましては、構成要件を広く取ると萎縮効果が生じ、狭く取ると野放図になる。このため、構成要件の書き方につきましては、分かりやすさや予見可能性を重視して入念に検討を行うべきであるということが改めて喚起されるということでございます。

特に、サイバーセキュリティーの研究や教育のためのウイルスなどの作成や保管については、これが不正指令電磁的記録に関する罪が成立しないことを保障する必要があると考えられます。

次でございますが、不正アクセスなどの電子的な行為を始める時点で危険犯として成立することも考えられること。

重要なシステムにつきましては、これを結果的加重犯の基本犯として処罰する類型を整備することも考えられること。

②の違法性阻却事由でございますが、イノベーションを委縮させてはならないという観点から、構成要件に該当するものの行為であっても違法性阻却を広範に認めることで救済するという発想もあり、こうした意見も否定せずに検討する必要があるのではないかということ。

３番目ですが、特に予見可能性の観点が重要だという観点から、６ページに参りますが、構成要件の外縁や正当業務行為の違法性阻却事由の解釈・運用の指針を定めることも考えられること。

不正指令電磁的記録に関する罪につきましては、イノベーションを特に委縮させることのないよう、積極的に明らかにすることも考えることとしております。

６ページ目のエンフォースメントの在り方につきましては、迅速に評価、立案を繰り返す不断の検討を行う必要であること。証拠の収集、起訴を見据えて現場が判断しやすいよう配慮する立法が必要であること。割れ窓理論が働いて、抑止力が効くどころか逆効果になるようなことは避けねばならないこと。実行の方向として、域外捜査やデータそのものの差押えなどについては制度面で適切に対応する必要があること。

（４）でございますが、「企業の刑事責任」についても、新たに考えていかなければならないということでございますが、訴追延期合意制度なども一考に値すると考えられるところでございます。

７ページ目でございます。

６ポツでございますが、各論につきまして次のような内容を記載してはいかがかと思います。

まず、「電磁的記録に関する犯罪」でございますが、技術の環境変化を踏まえ、今日的状況に合わせて見直すことが妥当であると考えられること。印章と同様の技術が生まれて

いる。それから、メタデータという重要な情報が存在していることから、電磁的記録に関する犯罪にはこれらのことを反映する必要があるのではないかということでございます。

印章偽造罪に妥当する電子のものがあってもいいのではないかということでございます。有印私文書偽造罪という、有印という通称が犯行を及ぼしているのではないかということから、通称の在り方も検討が必要ではないかということでございます。

（２）でございますが、コネクテッドカーの中から、インフラをみだりに操作するような罪についてでございます。

まず、コネクテッドカーの中に他者が乗り込んで、電子計算機を操作する場合。それから、自分の車を改造することによってインフラなどへ干渉する行為などが懸念されるということ。これについては、新幹線鉄道特例法というものが参考になるのではないかということでございます。

８ページ目でございますが、不正アクセス、通貨偽造、その他につきましては、本日の議論を踏まえまして、また骨子を作成させていただきたいと思います。

７番目でございますが、こういう刑事法の考え方は各業法の規制改革へ応用できるのではないだろうかということでございます。

事前規制から事後規制の方向の中で、事前規制の緩和と事後規制による不正な方法の抑止の双方がセットでなされれば、事前規制の改革が進みやすいのではないかということでございます。

以上でございます。

○大橋座長　ありがとうございます。

ただいまの御説明について、御意見、御質問をぜひいただければと思っております。

なお、本日は京都大学から稲谷教授、千葉大学の西貝准教授、また法務省刑事局より吉田刑事法制管理官、栗木参事官、警察庁より檜垣審議官にも御参加をいただいております。お忙しいところありがとうございます。

それでは、御意見がある方はぜひ手挙げの機能を使ってお知らせいただければ、私より指名をさせていただきますのでよろしくお願いいたします。

それでは、玉城専門委員からお願いできますか。

○玉城専門委員　分かりました。どなたも手が挙がっていなかったので。

いろいろ皆様、教えていただきありがとうございます。かなり丁寧に列挙して、技術面まで詳しく教えてくださりありがとうございます。

私からの意見なのですけれども、山口先生が識別符号について技術的な要素として記憶所持と生体行動の２つにきれいに分けてくださって、とても分かりやすかったです。

生体行動に関しておっしゃっていたとおり、今後、生体行動による認証が多くなってくるところで、現在の刑事法では対応が難しいのかなと思われます。

特にですけれども、生体行動の場合、技術的なカバーはなされてくるとは思うのですが、今後、流用とか盗用にどのように対応していくのかが課題となってくると思われます。意

図的に流用しているのか、意図的に盗用したのかが課題となると思うのです。

例えばなのですけれども、わざと一緒に行動したとか、わざとターゲットの方のバッグの中に携帯電話を忍ばせて、たまたま入ってしまったとして行動データを取ってしまう方法もありますので、それが本当に流用、盗用なのか、たまたま間違えてコピーになってしまったのかどうかというところを今後、刑事法でもきちんと決めていかなければいけないのかなと思います。

それもそうなのですけれども、まとめて見ると、他人の識別符号を意図的に自分の識別符号にしているのか、もしくは意図的ではなく識別符号にしてしまったのかというところが、今後の論点になるかと思います。

そして、全体として刑事法というか法律全般そうなのですけれども、法律に関しては基本的には人間とその生活に関して、空間的とか身体的とか物体的な制約が定常的にあることが前提となっていると文章を読んでいつも思っております。

例えばなのですけれども、日本国内のこの場所にいて犯罪が起きていてそこを調べればいいとなるわけです。ですけれども、インターネット技術が発展してきて、AIも発展してきて、そうなってくると空間的とか身体的な制約が徐々になくなってくる。もちろん、物体の空間的な制約もなくなってくる。

そのため、犯罪が発生した時点では、インターネット上の例えば東京都の中のサーバにデータがあったとしても、もしかしたら翌日には長野県にデータが移っているかもしれないですし、身体とか空間的なもの、物体的なものが定常的に定義できるものではなくなってきている。そのため、どこの時点で物体があったのか、その人がいたのか。つまり、犯罪が発生した時点での空間とか身体的、物体的な制約をつけなければ、インターネットの中で情報がどんどん流れていってしまうところでの特定というか、調査が今後難しくなってくるのではないかなと思います。

これに関しては、今回のワーキング・グループだけで特定するものではなくて、御提案にあったとおり何かしらの検討会を設置してより深く検討していく必要があると考えられます。

もう一点なのですけれども､私自身が人の体を制御するという研究をしているのですね。今は技術的に倫理的な観点から、１つの指で80グラム以上の力は出せないようにしているのですけれども、もしこういう技術的に装置として開放して１つの指に１キロぐらい力を出せるようにしてサインの制御をしてしまうとか、誰かの代わりに何かインプットしてしまう。今は法律がないので開放していないのですけれども、もし完全に人の体を制御するというのを技術的に開放してしまうと、人の情報自体、生体情報も含めそれ自体がもしかしたら認証としての意味を持たないかもしれないことも発生してくるので、こちらもきちんと検討会を設置して、かなり時間をかけて議論していくべきかと思います。

以上です。ありがとうございます。

○大橋座長　ありがとうございます。

後ほど、法務省や警察庁の方にも今のコメントに対して御回答、反応いただければと思います。

それでは今、手が挙がっている村上専門委員、お願いいたします。

○村上専門委員　村上です。皆さん、御説明ありがとうございました。

私からは意見と質問をお願いしたいと思います。

まず、事務局資料に書かれている検討の場を設けることは賛成です。検討の場だけではなく、新たな種類の犯罪が発生したときにすぐに対処できるような体制づくりにも取り組む必要があると思います。これが意見です。

吉開先生に、もし御存じでしたら教えていただきたいのですが、クラウド上のデータの取扱いに関しては、日本だけではなく海外も同じような問題を抱えていると思うのですが、海外諸国でこの問題に対して、何か取り組んでいることを御存じでしたら教えていただけますでしょうか。

また、警察、検事、弁護士それぞれにおいて、デジタル分野に知見のある人材を育てないといけないと思うのですが、こういった人材育成に関して、どのような課題があり、進め方が考えられるか、御意見いただければと思います。

私からは以上です。よろしくお願いいたします。

○大橋座長　ありがとうございます。

次に、髙橋委員、お願いいたします。

○髙橋（滋）委員　非常に興味深い御説明ありがとうございました。

私からは、佐久間先生と山口先生に御質問させていただければありがたいと思います。敵対的サンプルという重要な話なのですが、今のAIのレベルでどのぐらいこういう敵対的サンプルをつくり出すことが技術的というか確率論的に、レベル的に可能なのかということと、人為的にこういうものをつくり出すことはあり得ると思うのですが、自然現象の中で例えば落ち葉がくっついたとか、こういうことでも敵対的サンプルになり得るのかという点について教えていただければありがたいと思いました。

それから、山口先生に御教示いただきたいのです。技術も100％ではないので結局コストベネフィットという話があって、ある意味では行政との関係でもそこら辺が問題になるという話を御教示いただきました。これは例えば今の伝統的な実印の管理とか印鑑証明との関係で、個人認証のレベルがどのぐらいの強固性を持っているのか。もしくは、プラスマイナスで、要するに、それぞれにいい面、悪い面があって、では新しいところの個人認証のどこについて気をつければ、今までの既存の認証に比べて強固になるのかとか、そういうことについての研究はあるのか。

さらに言うと、例えば今、行政手続において対面で見なければ分からない、確認できないという認証をいまだにいろいろな手続で取っているのですが、では本当に対面でいろいろ質問して本人かどうかを試すというやり方と比較して、新しい技術の認証がどのぐらい強固性を持っているのかを比較ができるような研究があるのかどうか。この辺について、

教えていただければありがたいと思います。
どうもありがとうございます。
○大橋座長　ありがとうございます。
ただいまお手が挙がっているのは以上ですので､それではそれぞれの委員からの御質問、コメントに対する御回答をいただければと思います。
まずは佐久間先生から、髙橋先生の御質問について、簡潔にもしあれば御回答いただくことはできますでしょうか。
○筑波大学（佐久間教授）　佐久間です。御質問、どうもありがとうございます。
まず、１つ目の御質問で、技術的にそういった敵対的サンプルをつくることがどの程度可能なのかということなのですけれども、これは技術的には非常に簡単です。どのようなサンプルに対しても、それを誤識別させるようなノイズを設計するのは、多少のプログラミング能力があれば簡単にできてしまうというレベルです。
一方で、そういったものを作成できるには条件が必要で、識別させているモデルにある程度アクセスできることが必要です。これは一般的なシステムセキュリティーでも同様かと思うのですけれども、システムの攻撃したい部分に対してどのぐらいの情報を入手できるのかに依存しておりまして、モデル単体に直接アクセスできると非常につくるのは簡単なのですけれども、厳重に整備されていればだんだんそういうものを作成するのは難しくなっていく形になります。
２つ目の御質問で、では自然にそういったサンプルが発生してしまうのかどうかというのは２つの観点から考える必要があって、まずそもそもAIによる認識というのは、人間による認識と同様に100％正しい答えを返さないということです。識別率が例えば98％というものには達すると思うのですけれども、２％はごく自然に間違えます。そういった意味で、単純に間違うことはあります。
一方で、先ほどお示ししましたように、パンダにしか見えないのだけれども、全然別の動物になってしまうような誤認識というのは、人為的に誘発されたノイズでないと発生しないので、それは攻撃の意図を持った人が作為的にそういうことをしないと起こらないのではないかなと思います。
以上です。
○髙橋（滋）委員　どうもありがとうございました。
○大橋座長　続きまして、山口先生、手短にお願いできますか。
○東京大学（山口特任准教授）　はい。
御質問の、実際の実印サービスと今のマイナンバーカードのサービスがどのくらいセキュリティー上、違いがあるかという御質問と取りました。そういった研究は現実としてはないというよりは、とても難しいのだと思います。それは、対面のやり取りでのセキュリティー評価ということの言葉での表現がとても難しいからだと思います。
人間の場合は、直感的にこの人はちょっとうさんくさいみたいなことを感じる能力があ

って、それを電子的になった途端に微妙なニュアンスというものが急にできなくなってしまうと思っていまして、そこの表現をどうやって示していくかということが現状はできていないので、なるべく先ほど申しました登録とか認証のときに一致するような努力を表現としてしながらも、現実としてできていないのかと思います。

ただ一方で、感覚的な、今度は利便性とセキュリティーの話だけ申しますと、実印の話の利用する頻度とセキュリティーのバランスから考えると、今のマイナンバーカードのやり取りみたいなものは少しセキュリティー上は重過ぎるのかなと思います。実印はもっと手軽に、登録にしても何にしても使っていらっしゃいますよね。バランスが今はどっちにしても悪いので、どうしたらいいのかというのは研究としては何もなくて、感覚的なお答えになってしまって恐縮です。

○大橋座長　ありがとうございます。

次に、吉開先生、村上専門委員から海外事例の御質問があるのですが。

○国士舘大学（吉開教授）　私も海外事例は詳しいわけではないのですが、調べた限りですと、そもそもリモートアクセスが主権侵害であるという確立した国際法は存在しないと言われておりますし、ほかの国では外国サーバに対するリモートアクセスはかなりやっているという報告もあると聞いております。

あと人材育成のほうの話なのですが、どうしても法学教育が専門性重視で法律の知識を理解するのでかなりいっぱいいっぱいのところがあるのですけれども、やはり今後は法学教育の中でそういった他の専門家との協働をできるような人材を育成していくように意識づけるということ。これは法科大学院でできると思いますし、あとは実際にそれが可能な場をどうやってつくっていくかが考えられるかと思います。

以上です。

○大橋座長　ありがとうございます。

では、法務省からお願いします。

○法務省（吉田管理官）　法務省刑事局刑事法制管理官の吉田でございます。

先ほどの御指摘の趣旨を必ずしもうまくくみ取れなかったのですけれども、ある電子データに起因して犯罪が発生した後に、そのデータが別の場所に移動したというようなお話があったかと思います。

犯罪地がどこかという問題と、それに関連する証拠がどこにあるかという問題は別でございまして、犯罪行為地は基本的には犯罪の時点で確定されることになります。その後、その証拠が別の場所に移動すれば、それについて法律に基づいて証拠を収集していくことになります。

検討の場を設けて検討すべきであるという御指摘もあったかと思うのですけれども、先ほどお話を伺った限りだと何を議論することを念頭に置かれているのかがよく分からないところがありまして、いずれにしても、前回も御説明したとおり、我々としてもデジタル社会の進展に応じた刑事法の在り方を検討していく必要はあると考えておりまして、現に

起きている事象を踏まえながら、現行の刑事法の枠内でどこまで対処できるのか、対処できない事象がある場合に、それに対してどのような規定を設けていくことが考えられるのかをきちんと検討していく必要があるだろうと思っております。

ただ、そのための検討の在り方の方法論として、先ほどお話があったような検討の場を設けることが果たして適当なのかどうかということは事柄に応じて考える必要があると思っておりまして、我々としては検討することはやぶさかではないのですけれども、その方法論の点については､先ほどのお話ではうまく理解できなかったということでございます。

○大橋座長　既に骨子案も御説明させていただいていて、現行法の中でうまく対応できないところの御指摘も今日も含めて２回あったという認識でいるのですけれども、そこの辺りの御対応はどうされていくと捉えればいいのでしょうか。

○法務省（吉田管理官）　骨子案については、私も拝見いたしましたけれども、コネクテッドカーの問題とか、あるいは信号機の問題とか、前回会議におきまして、私のほうで既存の罰則でこういう形で対応することが考えられると申し上げた点があったかと思うのですけれども、必ずしもそれが反映されていないのではないかとも思われまして、その意味で、この骨子案をどういうものとしてお考えになっているのか私どもとしてはつまびらかではないのですけれども、こういう特定の行為が示されたときに、それに対して既存の法令でこういうことが考えられるということは個別にお示し、お答えしていくことは考えられるところでございます。

私どもとしては、前回も申し上げましたけれども、検討していくことを否定しているわけでは全くなくて、技術の進展に応じて刑事罰で捕捉していかないといけない領域というのは新たに生じ得るわけですので、そこはきちんと検討していきたいと思っております。

ただ、罰則をつくることありきとか、あるいはほかの法律からデジタル部分だけを移植することありきで議論されると、我々としては色々と法制的な面、それから、刑事法の基本的な原則その他の考え方に照らして考えないといけないところはたくさんありますので、そこはきちんと検討するということをお願いしたいと考えております。

我々の立場としては、そういうことでございます。

○大橋座長　御検討することの後押しをしたいということが、そもそもの本意だと思いますので、ぜひどういうふうな形で検討するのかということがすり合わせできればというのがこの場の趣旨かと思います。

すみません。落合委員から挙がっているのですが、私から１点だけ。例えばですけれども、この報告書にもあるのですが、前回、西貝先生から不正指令、電磁的記録に関する罪に関して研究のためのプログラムをつくることに関して、かなりこの法律、罪によって躊躇が研究上見られるというお話もあったと思っています。

これを含めて幾つか、御回答いただいていないところがあるのかと認識として持っていますけれども、例えばここの部分についてはどうされるのかという御回答をいただいてもよろしいですか。

○法務省（吉田管理官）　御指摘の点は、まさに立法当時、国会でも様々な議論が行われたところでございます。

正当な研究・教育の目的であえて不正指令電磁的記録に当たるプログラムを研究者の方が作って、その動作の状況を確認することは実際にあり得るところでございます。それが罰則によって捕捉されることがあってはいけないという御指摘は国会でもいただきました。そうした御指摘に対応するために、構成要件として、まずは「正当な理由がないのに」ということを明記しております。

「正当な理由がないのに」というのは「違法に」ということですけれども、その中身については、国会でも既に答弁されているところでございますけれども、今申し上げたような研究・教育目的で作成するような場合、あるいはそれを動かす、動作させるような場合には正当な理由があるということで処罰対象にならないという御説明を既に申し上げているところでございます。

さらに言えば、構成要件上、「人の電子計算機における実行の用に供する目的で」という要件があるのですけれども、この要件自体も、元々は、不正指令電磁的記録であることを知らない、事情を知らない人のコンピューターで作動させるという意味のものとして使っておりますので、この要件によっても、本来的には、研究・教育目的で作成する行為は処罰対象から外されるということでございます。

ただ、それでは若干分かりにくいという御指摘があったので、さらに「正当な理由がないのに」という要件も念のために規定したということでございまして、この辺は国会でも繰り返し答弁申し上げているところでございますので、そのような解釈で御理解いただければと考えております。

○大橋座長　この骨子案の趣旨は、国会答弁を国民がきっちり理解しているわけでもないので、そこで分かりやすいかとか予見可能性もしっかり高めていただくというのもこの骨子案の中の趣旨ですので、研究者の中にこういう方がいらっしゃったということで今回、御答弁いただきましたけれども、しっかり分かりやすさも追及していただければと思います。

落合専門委員、髙橋委員からも上がっていますので、お願いできればと思います。

○落合専門委員　分かりました。ありがとうございます。

私からは２点ほどでして、１つが今日、認証に関する議論をさせていただいていたところですが、認証の分野については現在、結構差し迫った危険がある分野だと思っております。

例えば金融分野ですと資金移動業者に関する事件が話題になったかと思いますけれども、要するに認証を悪用するかによって行われているかになるわけです。それも踏まえて金融庁では二要素以上の堅固な認証を行う方向に整理を行っております。多要素になるとどうなるかというと、パスワードだけではないという話になってきますので、こういう生体情報だったりとか行動認証だったりとか対象に入ってきます。当然ながら例えば金融機関な

どが基本的にそういうものを入れていくようにしているわけです。医療の分野などでも医療機関のガイドラインが適用になるような場合には、二要素認証に今後していくべきだとなっています。そういう意味では様々な認証手法が既に使われていますし事件も起こっている分野ではあります。認証に関する点については将来的なものというより直近に差し迫ったものとして、今の範囲でいいのかどうかをお考えいただくべきなのではないでしょうかというのが、１点目です。

２点目は、こちらはもう少し先の話でもあるのかなと思うのですけれども、デジタル通貨の議論も本日あったと思っております。

こちらについては日銀で実証実験もされているということでありますが、直ちに導入するというよりは、ある程度調査研究として行っている段階だと理解しています。

そういうことで、デジタル通貨に関する偽造とかについては先ほどの認証に比べれば差し迫った事象ではないと理解しておりますが、例えば新幹線の場合に、新幹線ができる前に特例法をつくって処罰に関する規定を定めたりということを行ったりしていることもあります。実際にはデジタル通貨を導入するかどうか自体未定の事項ではあると思うのですけれども、仮に導入するような場合には、当初から通貨偽造罪であったり、こういうものをデジタル通貨をどう保護するのかなどは事前に日銀、財務省、金融庁などと調整の上、御検討いただく必要なのではないかとも思いますけれどもいかがでしょうか。

この２点です。

○大橋座長　ありがとうございます。

髙橋委員、お願いできますか。

○髙橋（滋）委員　どうもありがとうございます。

法務省にぜひお願いしたいのですが、我々は別に刑法の謙抑性であるとか、そういうことまでを否定しようとしているわけではないのです。

要は、今まで法務省がいろいろとデジタル化について対応されてきたことを否定する趣旨ではなくて、今、これだけ社会が本格的にデジタル化しつつあって、本当に産業革命に匹敵するぐらい、もしくはそれを凌駕するぐらい物すごく社会の動きが速くなっている。

今までの安定した社会の刑法の検討のテンポでは、もう間にあわなくなっているのではないかと思われる訳です。ですから、社会が動いていく先を読みながら、世界の動きに遅れないように、ぜひ技術者とか国民であるとか経済の人を踏まえて、問題がどういうことが出てくるのかを予見して先取り的に、問題が出てきたときにすぐに対応する。そして、私は行政法学者ですから、当然、行政法的な措置とか民事的な措置とかがあって、それでもできないところがあるのではないか。問題のきざしが出てきたら、ただちに対応できるような制度をシステムとしてつくってくださいというお願いをしているのです。

そのときに、前回も議論をしましたけれども、一般技術者が怖くて技術開発できない。もしくは一般国民が理解できないような、専門家による構成要件の解釈だけでは困るわけです。

そういった意味で、一般国民や技術者が分かりやすく、これなら大丈夫、これなら危ない、こういうことはやってはいけないのだということが分かるように、構成要件は一般の人に分かりやすくもう一回考えていただく場を設けていただけませんかということをお願いしています。この点は前回の議論を全く踏まえていないという話ではないと思いますので、よく御検討いただければありがたいと思います。

御回答ください。

○大橋座長　それでは、法務省と警察庁の順番でお願いできますでしょうか。

○法務省（吉田管理官）　法務省の吉田でございます。

まず、デジタル通貨の点についてでございますけれども、もし現実的にデジタル通貨が我が国で強制通用力を持って通用することになるということであれば、それに先立って刑事法の整備をしていく必要があるのだろうと思います。

デジタル通貨が現実に我が国で通用しているのに、通用開始の時点で、それについて、現行法で言えば通貨偽造罪等に相当する罪がないということになりますと、それは通貨の保護として十分でないことになりますので、そのような場合にはデジタル通貨の検討と合わせて、並行して検討していくことになるのだろうと考えております。

それから、現在の事象を踏まえて一定程度、将来的な予見を持って刑事法を整備していくべきであると、一般国民にも分かりやすいものであるべきであるという御指摘についてですけれども、一般論としては、それはそのとおりだろうと思います。

ただ、どの法分野もそうだろうと思うのですけれども、一定程度はやはり専門的な用語、あるいは専門的な解釈を要することは不可避だろうと思いますので、こと刑事法の分野についてのみ、そうした専門的な解釈を排しておよそ一般の方が全てを理解できるような法体系にするということは現実的には無理ではないかと思われます。

その上で、それでも一般の国民の方に分かりやすいように、様々な注釈書等も出ておりますけれども、そうしたものだけでなくて、立案段階においても、一般国民から見た場合の分かりやすさということも踏まえながら立案をしていくことが重要なのだろうと考えております。

先ほど少し申し上げましたけれども、前回申し上げた意見が骨子案に必ずしも反映されていないように見受けられますので、我々としては、この骨子案を是とするとは言えないことは御理解いただきたいと思います。

骨子案の内容について、今後、どういう形で御意見を述べさせていただけるのか分からないのですけれども、どういう形で意見を提出するのかについてはこれから検討していきたいと思っております。別で意見を述べさせていただけるとも聞いておりますので、その機会を使って御意見を述べることがあり得ることは御了承いただきたいと思います。

○大橋座長　警察庁、お願いできますか。

○警察庁（檜垣審議官）　警察庁の檜垣と申します。

認証の関係で不正アクセス法との関係が幾つか出ましたので、若干お話をさせていただ

きたいと思います。

今日、お話があった中で行動認証といった多様な認証システムが紹介されておりましたけれども、これらが不正アクセス法で規制されるかどうかという点につきましては、これは具体的なシステムの組み方によるのではないかと思います。

不正アクセス法のアクセス制御機能は、コンピューターの側で利用者を一人一人識別するための仕組みでありますので、どのような形で認証が行われるかによりますけれども、最終的にはコンピューター側でこれは誰だと区別するためのものがあるかと思います。

ですので、これを識別符号として捉えることができれば不正アクセス法の対象になってこようかと思いますが、ではどういうものが該当するかというのは、具体的なシステムのつくり方によるかと思っておりますし、認証に当たって複数の手段を取られていくようでありますから、それらの中でどれが識別方法に該当してくるのかということになります。

また、御質問の中であった識別符号について、意図的に一緒だったとか、たまたま一緒だったというお話があったかと思います。

簡単に使えるようなものであれば、そもそも認証機能に使えるのかどうかという疑問もありますけれども、例えば動作によって認証するといった場合に偶然一緒になってしまったという場合にあって、それが本当に偶然であったらそもそも犯罪として成立するのかどうかということにはなろうかと思います。

あと、認証の問題で待ったなしだというお話もございましたが、認証の確実性につきましては罰則の世界でどうかなるというものでもございませんので、ぜひ皆様方に非常に高度な確実性のある認証機能を普及させていただければと思います。

以上です。

○大橋座長　ありがとうございます。

まだ、議論は尽きないところなのですけれども、お時間がまいりました。

本日は、骨子案を踏まえて、基本的には取引手段の信用性をいかに担保するとか、あるいは骨子案には公共の安全性も書かれていると思いますけれども、その点に関してデジタルのバランスが取れているのかどうかということで議論をさせていただいたと思っています。

立法段階でしっかり検討していただくことが非常に重要だということが今回、我々の意見だったと思いますので、これはまた事務局を通じていろいろ調整はさせていただくつもりですけれども、ぜひ引き続き議論を続けさせていただければと思いますので、法務省、警察庁の皆さん、ぜひよろしくお願いいたします。

それでは、ヒアリングはここまでとさせていただきます。諸先生方も含めて、お時間ありがとうございました。

それでは最後になのですけれども、本日、御議論いただきました骨子案なのですが、まだこれから肉づけをしてまいっていきたいと思っていますが、大きな方向性として委員の皆様方の中で御了解していただけるかどうかをここでぜひ確認をさせていただきたいと思

っています。皆様方いかがでしょうか。

委員の先生方、方向性として大丈夫ですか。

○落合専門委員　私はよろしいかと思いました。

○村上専門委員　村上です。私もいいと思います。

ただ、先ほど法務省の方がおっしゃっていたように、関係者との調整をどこまでしっかりできるかがポイントだと思います。

○大橋座長　ありがとうございます。

今、村上専門委員からもありましたけれども、事務局におかれては調整のほうもしっかりやっていただきつつ、委員の思いは今日の議論、あるいは前回の議論にも反映されているとおりなので、ぜひそこは大事に守っていただいて進めていただければと思います。

○吉岡参事官　了解いたしました。

○大橋座長　事務局、よろしいですか。ありがとうございます。

それでは、本日の議事はこれにて全て終了になります。

本日はお忙しいところ御参集いただきまして、ありがとうございました。

引き続き、またよろしくお願いいたします。