第８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８日（木）8:59～10:55

２．場　所：オンライン会議

３．出席者：

（委　員）小林喜光（議長）、高橋進（議長代理）大橋弘（座長）、菅原晶子（座長代理）、髙橋滋、武井一浩、南雲岳彦

（専門委員）落合孝文、玉城絵美、田中良弘、村上文洋

（政　府）河野大臣、藤井副大臣

（事務局）井上規制改革推進室長、黒田規制改革推進室次長、
山西規制改革推進室次長、渡部規制改革推進室次長、吉岡参事官

（説明者）一般社団法人JASPAR情報セキュリティ推進ＷＧ　飯山主査
一般社団法人JASPAR情報セキュリティ推進ＷＧ　根本副主査
一般社団法人JASPAR情報セキュリティ推進ＷＧ　宮下副主査
京都大学大学院法学研究科　稲谷教授
千葉大学大学院社会科学研究院専門法務研究科　西貝准教授
中島肇法律事務所　中島弁護士
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　新田長官官房審議官（交通局担当）
国土交通省不動産・建設経済局　天河官房審議官（不動産・建設経済）
国土交通省不動産・建設経済局不動産市場整備課　皆川課長
国土交通省不動産・建設経済局不動産業課　井﨑課長

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

２．データ駆動型社会に向けた情報の整備・連携・オープン化
＜不動産関連市場の活性化に向けたデータの整備・連携＞

（閉会）

５．議事概要：

○大橋座長　それでは、お時間ですので、ただいまより「規制改革推進会議第８回成長戦略ワーキング・グループ」を開催します。

本日もウェブ会議ツールを使ってオンラインで開催ということで、お手元に資料を御準備いただいて御参加をお願いいたします。

本日は、小林議長、高橋議長代理、デジタルガバメントワーキング・グループの田中専

門委員にも御出席いただきます。

また、河野大臣、藤井副大臣にも御出席いただいております。それでは、冒頭、河野大臣より一言御挨拶をお願いできればと思います。

○河野大臣　おはようございます。お忙しい中、本当に、朝一番からのワーキング・グループに御出席いただきまして、本当にありがとうございます。

成長戦略ワーキング・グループは、これからの２回、デジタル時代の刑事政策の在り方という、ちょっと今までと毛色が変わったような、また、非常に興味深い内容のものについて、御議論いただくことになります。

キャッシュレスでの決済とかデータのオンラインのやり取り。オンラインのこうした会議もそうですけれども、テレワークなど、デジタル技術というのが、日常生活で当たり前になってきています。

先月は、ホンダが、レベル３の自動運転車を世界に先駆けて発売するなど、いろいろますますこのオンラインの技術、デジタルの技術というのがいろいろなところでコアな技術として使われるようになると思いますけれども、その一方で、サイバー空間の脅威というのがやはり身近になってきている。あるいは自動運転など、そういう脅威が人間の安全、生命にも直結する。そういうことになる可能性があります。既にSFの世界では、自動運転車が乗っ取られたりということがよく行われるような状況にもなっている。そういう中で、我々の社会の安全を保つためには、やはり刑事上の対応が技術の進展と併せて求められてくるのだろうと思います。技術の進歩と安全・安心な社会。そして便利な社会。これらをみんな両立させていくために、やはり、そういう時代の刑事政策の在り方というのをしっかり議論していくことが大事なのだと思います。

2020年、電磁的なデータを対象とした犯罪は560件。４年間で1.5倍の増加ということでございました。

また、警察庁が運用する様々な不正の検知ネットワークシステムでは、１年間の不正の件数が４年間で４倍近く増えた、ということです。

今後、IoT、あらゆる家電がインターネットに接続する。自動車が自動運転になってくる。工場やら何やらもインターネットで管理される。そういうところが増えていくと、非常に高度化した技術を持ったハッカーがそういうところに悪さをするということも十分に考えられる。既に起きているのかもしれません。サイバー技術とサイバー犯罪。そして犯罪に対する対策というのは、これから先、いたちごっこになっていくと思います。そういうサイバーリスクに技術の観点からではなく、法律面からもしっかり対応をしていかなければいけないと思います。

日銀がデジタル通貨の議論をしていますけれども、例えば、通貨の偽造罪は「銀行券」しか対象にならないのかということを指摘したら、刑事局と日銀とそんな話をしたことがないのだということもありましたけれども、刑事政策もやはりこれから経済とか産業と関係ありません、などと言わずに、経済、産業の発展のためにも、刑事法がどうあったらい

いのかという議論をしていかなければいけないと思っております。

そういう中で、これから有識者の皆様にデジタル時代の刑事法の在り方、デジタル時代における経済政策と刑事法に関する議論をしっかりお願いしたいと思います。どうぞよろしくお願いします。

○大橋座長　まさに的確な御挨拶をありがとうございます。

それでは、議題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。早速ですが、ヒアリングに移ります。

本日は、一般社団法人JASPAR情報セキュリティ推進ワーキングより、飯山主査、根本副主査、宮下副主査にお時間をいただいております。

なお、本日JASPARからの画面共有のみの御説明いただく資料及び非公表を前提にお話ししていただく内容がございますので、こちらについては皆様方も非公表という取扱いでお願いできればと思います。

それでは、早速ですけれども、10分程度お時間を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。

○一般社団法人JASPAR（根本情報セキュリティ推進WG副主査）　皆さん、おはようございます。JASPAR情報セキュリティ推進ワーキング副主査をしております根本と申します。

本日は、「車両サイバーセキュリティ対応」について、以下の目次に沿って説明いたします。

最初に、JASPARについて紹介します。自動車業界におけるソフトウエア標準化を目的に活動しております。

車両を取り巻く環境です。機能進化及び車外との通信が増加したことにより、車両サイバーセキュリティ対応は重要で必須となりました。

車両内の資産は、ソフトウエア、パーソナルデータ、通信メッセージを設定しております。

セキュリティ対策の役割です。この表は、縦軸に資産の価値、横軸に攻撃の容易性を示しています。赤いエリアが危険、青いエリアが安全をイメージしたものです。例えば、重要な資産が簡単に攻撃できるところにあると危険なので、資産を攻撃から守るセキュリティ対策を行い、攻撃しにくいところに移動させることを示しています。よって、セキュリティ対策はターゲットを狙われにくい領域に設置させることが役割になります。

車両防御の具体的な例を示します。車外からの攻撃を受けやすい無線接続するユニットをL1階層にまとめ、強固なセキュリティ対策を実装いたします。その下に階層を分離するゲートウエイ機能を配置し、そして、一番奥のL3に機能安全等リスクの高いユニットを配置して守る多層防御アーキテクチャを適用しております。

では、車とつながる一般的なコネクテッド技術を紹介します。無線通信とサービス事例をまとめております。参照いただければと思います。

続きまして、一般的な車両搭載コネクテッドの認証を紹介いたします。大きく機器認証

と個人認証に分類されます。その下に、機器認証、個人認証の詳細を記載しております。これらは資産リスク、想定脅威に応じ適切な認証手法を選定するようにしております。

その中において、個人認証の具体例をまとめてきました。本日は時間の都合上、詳細は割愛いたします。参照いただければと思います。

次は、コネクテッドのセキュリティ対策概要です。コネクテッドシステムを構成する全体に対策が必要です。先ほど説明しました認証対策に加え、通信情報対策、ソフトウエア改ざん対策、脆弱性対策、車両アーキ対策を適用します。採用される対策技術は、IT業界もしくは我々JASPARがつくりました標準技術にて対応していけると考えております。

次に、外界認識システムのセキュリティ対策を説明いたします。外界対象については、様々なケースで誤認識が発生しないようなロジックを構築すべきと考えております。また、人為的な攻撃によってつくられた風景、画像があると考えられますが、それらと同様な画像が自然界に偶然存在する可能性があると考えられることから、認識ロジックで解決すべき課題と想定しております。サイバーセキュリティとして扱うかどうかということについては、今後、議論が必要と考えております。

以上、御清聴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。

○一般社団法人JASPAR（根本情報セキュリティ推進WG副主査）　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。

続きまして、京都大学の稲谷教授にヒアリングを行います。10分程度お時間をいただいているということですので、早速ですが、よろしくお願いいたします。

○京都大学（稲谷教授）　よろしくお願いいたします。おはようございます。

ただいま御紹介にあずかりました京都大学の稲谷と申します。刑事学、刑事政策を専門といたしております。本日はこのような貴重な機会を賜りありがとうございます。

私からは、「刑事法 ver.2.0」と題しまして、いわゆるSociety5.0における刑事法の在り方について御報告をさせていただきます。

それでは、早速ではございますが、報告の方へ移らせていただきます。画面を共有させていただきます。

まず、表紙の次、お手元の資料の２ページ目におきまして、Society5.0において生じるリスクの特徴についてまとめております。Society5.0におきましては、AI及びIoTの広範な適用により、あらゆるものがサイバー空間に接続され相互に影響を及ぼし合うという状況が生じます。しかもAIは学習、最適化いたしますし、ソフトウエアのアップデートによる製品やサービスの機能変化ということも随時生じますから、このシステムは動態的に変化いたします。

ところが、システムというのは大変複雑ですので、僅かな変化があるときに予測がつか

ない事象も起こします。ここに「バタフライ効果」と書いてございますのは、複雑なシステムにおいては蝶の羽ばたきがときとして竜巻に発展し得るような事象を指しておりますが、このような問題がそこかしこで生じる可能性があるわけです。実際、美人コンテストから始まったフェイスブックが民主主義や健全な市場をゆがめるような影響力を発揮することなど、当初は誰も予測がつかなかったわけですし、電気自動車会社のテスラが現在起こしつつある変化というのはモビリティーにとどまらず､我々のライフスタイルや価値観、産業構造や果てはエコシステムにまで及びつつあるわけです。このことは、ドローンや自動運転車などのAIやIoTを利用したシステムが社会実装された場合、これらの新たな社会インフラとなるシステムに干渉する行為が思いもかけないような大きな事故を引き起こしていることも意味しています。そのため、こうした行為によるリスクに適切に対処するために、制裁制度を用いる必要も生じることになるわけです。

３ページ目では、そのための方法論の案を示してございます。社会インフラとなるシステムに不当に干渉する行為を防ぐためには、干渉行為を法的に取り締まるための法律、干渉行為を防ぐためのアーキテクチャの構築の双方が必要となります。JASPARさんのほうでも若干示唆されておりましたが、言わば泥棒を取り締まる法律と泥棒に入られにくい構造の両方が必要となります。もっとも自宅の構造を工夫する場合とは異なりまして、製品やサービスを提供する会社にとって、これは若干失礼な言い方かもしれませんが、やはり安全性というのはコストがかかる対象になるわけです。しかもそれは最終的に製品の価格競争力に跳ね返ってまいります。

一方、製品を利用する消費者の側からは、どの製品が安全性に配慮しているのか容易には分かりません。その上、セキュリティを向上させるために必要な措置自体もこの状況下では刻一刻と変化しておりますから、あらかじめ規制当局の側で特定の措置を義務づけてしまいますと、かえってリスクを大きくする危険性があります。また、製品やサービスのアーキテクチャがしっかりしていないと、そもそも泥棒の数が多過ぎて取り締まれないという事態も生じ得ます。そのため、こうした製品やサービスを提供する企業の側でも適切なセキュリティを適宜構築、更新し、また、その情報について関係する規制当局、司法当局等に積極的に共有してもらうようにインセンティブを設定する必要も生じます｡つまり、システム全体として状況の変化に随時適合しながらリスクマネジメントという目的を達成し続けるために、いわゆるアジャイル・ガバナンスと呼ばれる手法を刑事司法でも採用する必要があるのです。

４ページ目は、近時公開されたガバナンスイノベーション報告書に基づきまして、アジャイル・ガバナンスについて説明してございます。この文脈におけるアジャイル・ガバナンスとは、イノベーションとともにリスクの源泉でもあるシステムの動態的な変化に対しまして、企業、市民、規制当局、司法当局というステークホルダーが密にコミュニケーションを取りながら、システム全体として迅速に対応していくということを意味しております。ただし、刑事司法は刑罰権力の濫用による社会的費用の大きさに鑑みまして、法の支

配という理念に基づいて伝統的にハードローを用いて権力を構造化してまいりました。このため、ほかの分野にもまして透明性・アカウンタビリティ・民主的正当性というアジャイル・ガバナンスの理念に忠実となる必要がございます。

５ページ目以降では､以上の総論を踏まえまして､重要インフラの防衛という観点から、もう少し具体的な政策について提言してございます。

まず、５ページ目にかけましては、刑法の改革の方向性について簡単に示してございます。ポイントは、Society5.0における重要インフラの機能を阻害し得る干渉行為を包括的に犯罪化し、さらに、それに起因する重大事項が生じた場合には、刑罰を重くするような犯罪類型を制定法で創出するという点にございます。現在の不正アクセス禁止法は、御承知のとおり、基本的に認証機能の阻害を問題としてございますが、人工知能の誤作動につながるノイズの作出、例えば、看板によく分からないノイズを張りつけてみてちょっと作動をおかしくしてみるとかそういった行為､あるいはIoTとインフラとの通信への干渉、こちらもJASPARさんのほうで若干言及されておりましたが、こういった行為につきましてもこのシステムに及ぼす影響やその危険性に鑑みますと、システムへの不当な干渉行為として取り締まる必要が高いと言えましょう。

また、システムが変化することへの対応や摘発すべき干渉行為の範囲を適切に制限するために、警察当局ないし司法当局の側で適宜対象インフラや対象行為について説明責任を果たすと指定できるような制度とすることが望ましいように思われます。

６ページ目では、アーキテクチャの側について示してございます。既に申し上げた理由から、製品、サービスを供給する企業側におきましてのサイバーセキュリティに関するリスクマネジメントを適切に行うようにインセンティブを付与しなければなりません。

ここで参考となりますのが、ガバナンスイノベーション報告書でも言及されているリスクベースアプローチと訴追延期合意制度との組合せでございます。具体的には、まず、製品、サービスへの干渉行為に起因する重大事故が生じた場合には、当該製品、サービスを提供する会社に事故結果について民刑事の厳格責任を定めますと。そうすると企業の側では、いわゆるSTAMPに代表されるようなシステムとしてリスクをマネジメントする手法に基づきまして、特に重大なリスクを探索、特定し、適切なセキュリティを構築することで過大な責任を負わないようにするインセンティブが生じます。また、干渉行為を認知した場合には速やかに関係当局と情報を共有し、重大事故へとつながらないように努力するインセンティブも生じるでしょう。

しかし、Society5.0というシステムの特性上、合理的な努力をしても事故を完全に防ぐことはできませんし、完全なセキュリティシステムを構築することも難しいです。そのような場合にも常に企業に責任を負わせますと、当然、イノベーションが萎縮することとなってしまいます。そこで一種の司法取引である訴追延期合意制度を利用して、セキュリティ対策や情報提供を真摯に行わない企業のみが高額の制裁金や認証取消しなどの重たい制裁の対象となるように制度を運用いたします。つまり、リスクについて真摯に説明責任や

応答責任を果たす企業は、刑事責任追及の対象とはなりませんから、過剰な負担を恐れることなく、引き続き市場にとどまってイノベーションを続けることができるのです。

この点、攻撃された企業の側が責任を負うことにはなるのはおかしいというご異論もあろうかと思います。しかし、こうした責任が全く存在しませんと、安全性というのは企業にとっては最終的には費用となりますから、真面目に安全対策をする企業が報われないことになってしまいかねませんし､ひいては悪貨が良貨を駆逐することにもなりかねません。実際､近時になって長年にわたる品質不正が幾つかの業界単位で明るみに出ておりますが、こうした事象は、従来の法人処罰制度では、真面目に努力する企業が競争上報われにくいために、市場として悪い均衡となっていたという可能性すら示唆しているわけです。もっとも、厳格責任という極めて重たい責任をコントロールするわけですから、実際に訴追権限を行使する司法当局には相応の説明責任が求められます。また、専門性を補うために、関係官庁や事故調査委員会などと協力する必要もございましょう。したがって、こうした点についてもアジャイル・ガバナンスの一部として整備を進め、法の支配の理念を実質的に実現していく必要もございます。

Society5.0における犯罪がしばしば国境を越えて、サイバー空間を通じて生じることに鑑み、その対応策について示してございます。具体的には、国境を越えて我が国の刑事司法が活動できる範囲を拡張していくための方法についてお示ししてございます。従来、サイバー犯罪において国境を越えた捜査を行うためには、捜査共助という方法が採られてまいりました。しかし、この方法は大変手間暇がかかりますので、サイバー犯罪を実効的に取り締まる上では不十分であるという認識が世界的に広まりつつあります。そのため、現在では、各国の捜査権限の直接的な相互の乗り入れのような方法が拡充しつつありますので、我が国としてもこのような方法によって対策をしていく必要が高いと言えましょう。

また、先ほど申し上げた訴追延期合意の方法による場合には、問題を起こした企業の側が自主的に情報提供していくことになりますので、国境を越えて刑事司法の影響力を広げていくことが可能となります。ただし、これらの方法を実現するためには、我が国の刑事司法の拡張を他国に受け入れてもらう必要があります。したがいまして、我が国の刑事司法の適正さについて、一層の説明を尽くしていく必要があるとも存じます。

８ページ目につきましては、本日の報告全体の要約となってございます。

また、９ページ目及び10ページ目につきましては、報告中に用いました熟語の簡単な説明資料となってございます。併せて御笑覧いただけますと幸いです。

以上をもちまして、私の御報告とさせていただきます。御静聴どうもありがとうございました。

○大橋座長　ありがとうございました。

続きまして、千葉大学の西貝准教授にヒアリングを行いたいと思います。10分程度でお願いできればと思います。

○千葉大学（西貝准教授）　御紹介にあずかりました千葉大学の西貝と申します。もとも

とはITを専攻しておりまして、今は刑法の研究をやっております。今日はその観点から御報告させていただきたいと思います。

まず、レジュメを共有させていただきます。ワードファイルのレジュメになってしまいますので見にくいかもしれませんが、御了承いただければと思います。このたびはこのような機会を頂戴いたしましてありがとうございます。

まず、既にJASPARさんと稲谷先生から、サイバーフィジカルセキュリティに関係する議論が結構出ておりますが、一応、私の専門はサイバーセキュリティと刑法なのですけれども、サイバーセキュリティと刑法の延長線上にサイバーフィジカルセキュリティの保護というのがあると考えておりまして、まずはサイバーセキュリティと刑事立法の在り方ということを考えつつ、その上でサイバーフィジカルセキュリティと刑事立法について考えていきたいと思います。

この２つは何が違うかというのを考えておりますと、先ほどまさに大臣がおっしゃったとおり、新しいサイバー攻撃に対応するためにはどのように技術的に対応していくかという話というのは、基本的にいたちごっこの世界でした。ですので、新しい攻撃手法が未知であることは基本的なものだと考えるべきでして、そうすると、刑事立法で新しいサイバー攻撃に対応するためにはどのようなことを考えていったらいいかというと、まさにレジュメの左側の１の最初に書いてあるところなのですけれども、ある程度構成要件を包括的に捉えなくてはいけないのではないかというのが私の印象でございます。なぜある程度包括的とあえて申し上げているのかといいますと、伝統的なフィジカルの世界で行われる犯罪と比較しますと、ある程度包括的でなければいけないということでございます。

そうすると、レジュメ自体は結構技術的なことが書いてあるのでむしろここの口頭での御報告はやや抽象的なイメージをつかんでいただきたいと思って申し上げているのですけれども、ある程度包括的な構成要件をつくりますと、結構大きくいきなり構成要件でいろいろな行為が捕捉されることになります。それに対して、従前は構成要件において狭く捕捉しており、違法性阻却事由といって犯罪が成立しない場合をも狭く捉えていたところ、サイバー攻撃に対して既にある程度広めに構成要件で捕捉している場合には違法性阻却が許される文脈というのも多いだろうと考えているわけです。

とりわけ一番議論されているのが、コンピューターウイルスを捕捉するための犯罪が最近つくられたのですけれども、この犯罪に対する対策を行うためにも、この犯罪の構成要件に該当するような行為が必要になってくる場合があると言われております。例えば、セキュリティ業者さんがコンピューターウイルスを保管して、それを使って自社のネットワーク内とかもしくはもうちょっと大きなネットワーク内でそれを使っていくということを考えた場合に、セキュリティ確保目的で最終的には行動しているにもかかわらず、場合によっては検挙される可能性もあるということになります。そういうことをある程度広く、それは端的に犯罪にならないよねというロジックが必要になってくるのですけれども、それは既にある程度包括的に構成要件をつくってしまっているので、構成要件には該当して

しまうということで違法性阻却も結構広く、今までの犯罪よりかは広く考える必要があるのではないかと考えているわけです。

あと、これがどういう議論になっていくかは分からないのですけれども、一回つくった法律をすぐに変えるべきではないという考え方は昔から指摘されてきたと思うのですけれども、サイバー攻撃に対する対応の仕方としては、他国の立法例を見てみますと、結構頻繁に刑事法レベルでも改正されているということがあります。例えば、オーストリアとかですと無権限アクセス罪は2002年につくったところ、もう既に２回改正されているということもありまして、謙抑的につくった、つまり構成要件を狭くつくったのだったら徐々に広げていこうという努力を定期的にしていることが分かりますし、あとは、逆に今回、日本のコンピューターウイルスに関する罪に関しては非常に捕捉範囲が広く取られているので、場合によっては技術者に対する萎縮効果を減らすために構成要件を限定しなくてはいけないかもしれないと考えているところでもございます。

以上、サイバーセキュリティと刑事立法学の１の方向について簡単に申し上げたのですけれども、これは産業界にとってどういう意味があるかといいますと、２と異なって、構成要件を広く取り過ぎますと、エンジニアたちにとっての萎縮効果が大きくなると。エンジニアたちにとっての萎縮効果が大きくなるのですけれども、今、ソフトウエア開発というのはどこでもできるわけで、海外でもできるし日本でもできると。そういう場合に、この国のコンピューターウイルス罪というのがどういうふうに考えられて検挙されているか分からんぞとなりますと、開発拠点が日本から去っていく可能性があるというリスクを感じているところでございます。つまり、サイバーセキュリティと刑事立法学という文脈では、なるべく違法性阻却というものを広く考えつつ、つまりいたちごっこに対応するために包括的な構成要件をつくりつつ、産業誘致のためにも違法性阻却が結構広く取られるべきですよということを今回申し上げたいと思います。

そして、個別具体的な事案は判例等で解決していくべきなのですけれども、構成要件が広く取られ過ぎてしまったねという場合には積極的に法改正とかを考えることによって是正していけばいいという感じでございます。つまりこの（３）なのですけれども、立法の失敗とかを嘆く必要はないと。あと、立法過程においてPDCAサイクルを回すと。つまりある意味で新しい立法の事実やサイバー攻撃に対応するために、意識的に構成要件や違法性阻却の範囲を考え直していけばいいのではないかと考えているところでございます。つまり、伝統的な犯罪だと時間の進みが遅いのですけれども、サイバー犯罪が出てくることになって、このようなことを考えざるを得なくなったということであると考えております。

次に２番なのですけれども、「サイバーフィジカルセキュリティと刑事立法学」と題しまして、ちょっと抽象的なのですけれども、簡単に言ってしまえば、コネクティッドカーをはじめとする重要インフラをどのように保護していくかということで、それを刑法の観点から考えるということでございます。これはほかの国と比較しますと、例えば、日本の保護の対応が、ちょっと保護が薄いとなりますと、この国は自動運転車が事故を起こした

りとか、あとはハッキングされたりして大事故が起きた場合にちゃんと検挙してくれないのだったら安全ではないのではないかということで、むしろ今度は逆に国民の安全、安心の観点からちょっと不安が残ってしまうということになります。

先ほど既に稲谷先生からも御指摘があったのですけれども、例えば、サイバー攻撃に対する犯罪、不正アクセス禁止法とかがあるのですけれども、それで十分にコネクティッドカーに対する、例えば、ハッキングが捕捉されているかというとそうでもないような現状があるように思っております。

詳細は省きますけれども、従前のサイバー犯罪の対策立法というのは、言わばフィジカルな面での対策立法とのパラレルの関係のものとして捉えられてきました。例えば、私文書偽造に対して、それが文書とデータは違うよねということで電磁的記録不正作出罪を1980年代につくったりとか、人のコンピューターシステムに侵入する場合に住居侵入が使えないよねと考えるなどして不正アクセス罪を2000年につくったりとか、あとは詐欺の類似のものとして電子計算機使用詐欺とかを入れてきました。でも例えば、仮想通貨とかに代表されるように電子計算機使用詐欺が使えるかどうかとかの細かい話というのはまだいろいろ課題が残っております。

それだけではなくて、最近は既に病院とかがランサムウェアの被害に遭ったりして、結局治療が遅れたりして人が死亡するインシデントとかが既に発生しておりますので、重要インフラの保護というのは最大限図る必要があると考えております。

そのような場合にどのようなアプローチがあるかといいますと、重要インフラというものを攻撃すること自体がすごい公共の危険を惹起するものなのだとして、重要インフラの保護のためにハッキングレベルの、重要インフラの重要なコンポーネントについて、それをちょっと触っただけでも、さっき稲谷先生から干渉という言葉がありましたが、その干渉をする行為自体を包括的に禁止してしまおうというアプローチも一方であると思います。

実は前の東京オリンピックですけれども、それのために新幹線が造られたと。その新幹線というのは非常に重要なものなので普通の鉄道と一緒には論じられないとして、みだりに操作罪というものが新幹線特例法という法律に入ったりもした経緯もございます。まさに私としては、今回のサイバー空間の脅威というのは、新しいハイテク電車が登場したのと似たようなものが、法律上、現象としてはあるのではないかと思っておりまして、いろいろな積極的な提案をしていきたいと思っているところです。

あとは、サイバー犯罪の致死罪の結果的加重犯的な致死罪をつくることも参考になるかと思っております。実はドイツやオーストリアというのは既に重要インフラとか公共の危険がハッキングの結果として生じた場合には重くするという条文を持っております。あまり使われてはいないようなのですけれども、そういうのを持っていることによって安全、安心側の観点からそれが意味があることであればこちらも検討していけばどうかと思っているところでございます。

残りは、私がサイバーセキュリティやサイバーフィジカルセキュリティについて、今ま

さに研究しているところでございますので、後ほどまた、この論文の内容等について必要があれば御議論させていただきたいと思います。御清聴ありがとうございました。
○大橋座長　ありがとうございました。
　続きまして、中島肇法律事務所の中島弁護士にヒアリングをさせていただきたいと思います。５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、早速ですけれどもお願いできればと思います。
○中島肇法律事務所（中島弁護士）　中島でございます。時間が短いので、まず画面を共有させていただきます。画面共有がうまくできないのですけれども。
○大橋座長　一応資料が皆さんのお手元にありますので、それで。
○中島肇法律事務所（中島弁護士）　では、恐縮ですが、お手元にございます「横浜地裁川崎支部平成12年７月６日判決について」というものを御参照いただければ幸いです。
　この判決は、私が裁判官時代に言い渡したものなのです。公刊物には搭載されていませんが、多くの論文で批判的に引用され、平成23年のわいせつ物の電磁的媒体を処罰する法改正が行われましたが、そのきっかけになった言わば反面教師の判決という栄誉に浴した判決でございます。既に立法的に解決された問題ではありますが、これを素材にしてごく簡単に、お二人の先生方は立法の面からのお話でしたが、言わば、法の解釈適用の面から罪刑法定主義の限界を少し論じてみたいと思います。
　この事案の概要は非常に素朴な犯罪でして、知り合いの女性の陰部を撮影した画像を、お金を払ってくれた人に添付ファイルとしてメールで送ったというごく素朴な犯罪でございました。これが、わいせつ物図画販売罪に当たるのかということが争点になった事案でございます。
　２枚目の弁護人の主張を見ていただければ分かりますように、当時の刑法175条、わいせつ図画というのは「その他の物」とありますので、データは「物」ではないから無罪であるという主張がなされましたが、この主張に対する私の判決の判断は、「争点に対する判断」に記載しましたように（レジュメでアンダーラインを付しました。）、なぜ物と立法されたのかというところが重要です。アンダーラインを見ていただきますと、この情報が有体物という媒体に固定されて初めて情報が同一性を維持したまま繰り返し再現可能になるのだと。だから、物でなければ情報を固定できないという前提があって、物から離れた情報、媒体から離れたまま情報が同一性を維持できるということを想定していなかった。ところが、このインターネットシステムというものができ、今でいうサイバー空間ができると、物から離れた情報が同一性を維持したまま伝播、伝えることができるようになったと。これは、物と同視していいのではないかというのが、この有罪判決の根拠でございます。
　もう１枚めくっていただいて、実はこのような論点は過去に遡ると非常に似た論争がございました。それが電気窃盗事件です。これは窃盗罪の対象は「物」だとされていたので、電気窃盗が立件されたときに電気は物なのかというところが同じように論争され、批判さ

れながら当時の大審院は、窃盗罪の対象を「物」にした理由は、「管理が可能」であればいいのだと判示致しました。窃盗罪の特徴は、管理しているものを移転する、違法に移転することに本質がある。だから、管理可能性と移転可能性があればいいという判断です。電気は管理できて移転可能ではないかと、電池にもなるではないかと。ということから、物に限定する必要がないと。民法で言う有体物に限定する必要がないのだという大審院の判例が出ておりまして、しばらく前まではそれは通説（小野説・団藤説辺りまで）でした。その後、立法によって電気は物とみなすという立法が加えられたにもかかわらず、これは注意規定であって、もともと電気は物だったのだというのが通説となっておりました。

ところが、私の判決に対しては、これは罪刑法定主義違反だという研究者の方々の御批判をいただいたのですが、かつては「電気は物だ」というのが通説だったではないですかというのが実務家としての私の疑問です。新しい技術革新に関しては、立法が追いついていないときに野放しにはできないというとき、電気窃盗事件の大審院判決は、法の適用解釈を柔軟に（目的に）することによって硬直な刑事法を社会経済に適応させた先例だったと思うのです。河野大臣が冒頭のご挨拶で的確におっしゃっていましたが、刑事法といえども経済インフラなのだと。刑事法の分野は「罪刑法定主義」を金科玉条として、この重要な役目を見落としているのではないかというのが私の主張です。

今後指針となるものは何かを提示したのが、３ページ目の最後の罪刑法定主義の見地からの最高裁昭和50年９月10日判決（徳島市公安条例事件）の団藤補足意見でございます。アンダーラインを付した箇所にありますように、曖昧で不明確なゆえに、罪刑法定主義、憲法31条に違反するのかどうかが争点となった事案です。事案は、デモ行進をしてジグザグ行進をしたことが「交通秩序を維持すること」という条件に反するという構成要件に該当するのかというところが争点となったケースですけれども、アンダーラインを付した部分を見て頂きますと「具体的な場面に当該行為が適用を受けるかどうかの判断を一般人ができるかどうか」これが基準であるというのが団藤補足意見です。どなたかの先生が構成要件を包括的にすべきだという非常にすばらしいご意見を言われましたが、構成要件が包括的な場合、具体的な場面で「これはやばい」と一般人が感じられるならいいではないかというのが、特に日進月歩の技術革新のされるITの場面ではこのような解釈適用が許されるのではないかというのが私の主張でございます。なお、横浜地裁川崎支部の私の判決は被告人は納得して控訴せず確定しております。以上でございます。

○大橋座長　御説明ありがとうございました。

それでは、今までの御説明に関して、御意見、御質問等をお願いしたいと思いますが、まず最初に、元検事でもあります立命館大学の田中先生からコメントをいただければと思いますけれども、お願いできますでしょうか。

○田中専門委員　発言の機会をいただきありがとうございます。デジタルガバメントワーキング・グループ専門委員の田中と申します。

現在は、大学で行政法規上の刑罰規定について、行政法の観点から研究をしております

が、ただいま御紹介いただきましたように、研究者に転じる前は検事をしており、さらに、法律家に転じる前はシステムエンジニアをしておりました。そのような立場から、デジタル時代における刑事法の在り方について、５分程度時間を頂戴してコメントさせていただきたいと思います。

まず、どれだけ厳重な対策をしていても技術の進歩や思いもよらなかった方法によってセキュリティが突破される可能性というものは否定できません。このことはデジタルの世界に限ったことではありませんが、先ほどJASPAR様から御示唆いただきましたように、デジタル社会における不正行為を抑止する手段として刑罰の活用を検討することは非常に重要であると思っております。

次に、稲谷先生、西貝先生、中島先生からそれぞれ、デジタル時代における刑事法の在り方に関連して御説明を頂戴しました。いずれも非常に重要な内容で大変勉強になりました。先生方の御説明で刑事法の観点からの論点は出尽くしたと思われますので、私からは、現場の経験を踏まえて、法政策的、行政法的な観点からコメントいたします。

まず、いわゆる行政刑法と呼ばれるものの大部分が実際には適用されることがなく、機能不全に陥っているということが多くの行政法の研究者から指摘されています。刑罰規定は条文として存在することに意味があるのではないかという意見もありますが、行政規制の実効性という観点からは、条文として存在するだけでは抑止効果は乏しいと言わざるを得ません。また、適用されない刑罰規定が存在すること自体が、かえって刑罰全体の威嚇力を損ねるという指摘もなされています。

したがいまして、デジタル犯罪についても、抑止力という観点からは、刑罰規定を設けるだけでなく、それを実際に適用するということが不可欠だと思われます。抑止力を実質的に機能させるためには、立法過程において現場の警察官や検察官に対して、当該刑罰規定がいわゆる象徴立法ではなく、実際に適用されるべき刑罰規定なのだという、そういうメッセージを伝えることが重要です。また、実際に適用されることを前提とするのであれば、明確でかつ証拠収集を含めた立件の可能性まで考慮した構成要件を検討する必要があります。行政法規上の刑罰規定には、実際に適用されることをおよそ想定していないと思われるようなものも多く、デジタル犯罪についても同じ轍を踏まないよう、適用段階をも見据えた議論がされることを願っております。

その一方で、技術の発展という観点からは、萎縮効果を生じさせないことも極めて重要です。ここからは主に、元システムエンジニアの立場からの発言になります。

先ほど西貝先生からも御指摘があったように、技術者からすれば、刑罰の対象となるのかならないのか、裁判になってみないと分からないという状態は非常に困ります。許される行為と許されない行為の境界が明確に示されれば、エンジニアは法令を遵守した上で技術開発を進めることができますが、最高裁まで行ってみないと分からないという状態は、場合によっては禁止されることよりもたちが悪いと言えます。

例えば、ファイル共有ソフト、ウィニーの開発者が著作権侵害の幇助犯として起訴され

て地裁で有罪となった後､高裁で無罪となって最高裁で確定したという事例がありますが、裁判所でさえ見解が分かれるような法律解釈の下で技術開発を進めろというのは、技術者にとっては酷と言わざるを得ません。ちなみに、ウィニー事件の上告審判決には、著作権侵害罪の幇助は成立するが、検察が起訴したことは配慮に欠けるという反対意見が付されていますが、法律上は犯罪に該当するが運用で何とかしろというのは、立法の不備を現場に押し付けるものであって妥当ではないと思われます。技術者からしても、そのような不安定な状態では、安心して技術開発に携わることができません。イノベーションを阻害しないためには、犯罪の成否を条文の規定からできる限り明らかにすべきだと思います。

したがいまして、不正行為の抑止という観点からも、イノベーションの促進という観点からも、デジタル犯罪の構成要件は、法律の専門家であれば解釈が可能というものではなく、法律に疎い一般人であっても明確に分かるようなものにすべきではないでしょうか。デジタル時代における刑事法の在り方を検討するに当たっては､多くの行政法規のように、難解で不明確な刑罰規定を設けてそれで終わりとするのではなく、刑罰規定が社会にどのような効果を与えるのかについて、立法段階でしっかりと検討した上で、さらに事後的に検証を行い、場合によっては条文を見直す必要もあると思われます。

少し長くなりましたが、要するに、デジタル犯罪に対処するには、刑事法についてもデジタル化を進める必要があるのではないかというのが私の問題意識です。

以上です。

○大橋座長　ありがとうございました。

なお、本日は、法務省刑事局より吉田管理官、栗木参事官、警察庁交通局より新田審議官にも御参加いただいておりますので付け加えておきます。

それでは、委員の方々、その他の皆様方から御意見を頂戴できればと思います。手を挙げていただければ指名をさせていただきます。

まず、髙橋委員からお願いいたします。

○髙橋（滋）委員　本日は貴重なお話をどうもありがとうございました。

幾つかあるので、最初に２点だけ申し上げたいと思います。

まず一点は、JASPAR様に、それから、法務省、警察庁にお聞きしたいのですが、今御指摘されたサイバーセキュリティの危険というのは、多分、技術に強くて自動運転に興味がある方だったら既知の話なのではないかと思うのです。ITに詳しい方であればこういうセキュリティの問題があるというのは、恐らく、明白な話だと思います。そういうときに、悪意を持っている方々が、仮に自動運転が実際ある意味で施行でもいいし試験的な施行でもあるとされるときに、こういうことについて刑法の抑止がないということから悪意で利用されるおそれがあるとなると、危ないということでこの技術が止まってしまうのではないかと思うのです。世界から遅れてしまうということになると思います。こういうことを日本社会として見過ごしていいのかということだと思うので、そういう意味でJASPAR様にそういう危惧あるのかどうかということをぜひお聞きしたいと思います。そして、私はあ

ると思いますので、法務省、警察庁に対しては、これは今ある危険があるのだから、刑事的な手当てをすべきなのではないかと思うのですけれども、その辺について御意見をお聞かせいただきたいと思います。

それから、第二点ですが、西貝先生も稲谷先生もおっしゃったように、サイバーセキュリティについての脅威に対処するには、機動的な立法、刑事立法というのが必要だと思います。そういうときには失敗を恐れずに機動的に対処することは重要だということなのですが、法制審議会の運用の仕方として、こういうものについて迅速に対処する体制になっているのかどうかということをお聞きしたいと思います。特別部会なりをつくるなりして、恒常的に世の中の技術の発展に機動的に対処できるような構成づくりになっているかどうかということをぜひ法務省にお聞きしたいと思います。

以上です。

○大橋座長　ありがとうございます。

もしほかにも委員の方で御意見があればまとめてお伺いできればと思いますけれども、ございませんか。

玉城委員、お願いします。

○玉城専門委員　ありがとうございます。

質問をする前に少しだけ意見を述べたいのですけれども、ハッキングとクラッキングの定義について意見を述べさせてください。実は弊社の会社名がH2Lで、ハッピーハッキングライフという名前になっておりまして、ハッキングという名前自体は犯罪ではなくて、高い専門性や技術力によってシステムやプログラムを構築したり改変したりすることなので、できれば犯罪行為を指す場合はハッキングと言わずに、クラッキングもしくはクライムハッキングと呼んでいただければと思います。

意見はさておきとしまして、稲谷先生がお話しされていた、認証ではなく情報の通信の部分、インプット、アウトプットの部分です。そういう部分の妨害や不正な情報取得、ノイズ発生自体も問題であるというのは、大変分かりやすいSociety5.0の、サイバーだけではなくてサイバーフィジカルが融合することによる、つまり関わることによる犯罪発生のかなり重要な論点だと思われます。

一方で、カオス理論による環境やインフラへの悪影響の犯罪特定というのは大変難しく、例えばなのですけれども、バタフライ効果というのがカオス理論、時系列変化を伴う環境の変化というのは予想するのが難しいという意味でバタフライ効果と呼ばれているのです。ただ、今分かっている環境変化に関して作為的に制御モデルをつくることも犯罪ではないかと私は思います。

例えば、渋滞発生に関してなのですけれども、不等間隔で自動運転したり不要不急な車線変更を作為的に増やしてしまうと。そうすると、渋滞が発生してしまうのです。ただ一方で、自動車のユーザーさんは、そうすると運転の快適性が上がったり、自分だけ先に進めたりして、そうすると、ソフトウエアとしては売れると思われるのです。自動車運転、

自己だけ満足する制御モデルをつくってソフトウエアを配布するというのは、結果的に経済損失12兆円となる渋滞を助長する行為ともなります。そういった交通インフラ全体へ悪影響を与える制御とかそういうところも既に分かっているのであれば、検討されるべきだと思います。

そして、ちょっと気になっているところでして、現在、このようなカオス理論による環境やインフラの悪影響について、先ほど御説明をいただいているのですけれども、分かっているカオス理論に関して、刑事罰の研究や議論ではどのように捉えられているのかというのをちょっと先生方に、先ほど丁寧に説明いただいたのですけれども、伺いたいと思います。

私自身は環境への悪影響は、日進月歩がありますので、開発者が知っていなかったという場合であったり、あとは、開発者がそもそもシステムとして環境への悪影響を制御できないからできないという、致し方ないという観点でも議論をして定義を進めて、先ほど髙橋委員もおっしゃったように、機動的な対応が求められるのではないかと思います。

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。

手が挙がっている２名の委員に関して、それでは、JASPARさんから、髙橋委員から御質問があったのですけれども、御回答いただくことはできますでしょうか。

○一般社団法人JASPAR（根本情報セキュリティ推進WG副主査）　JASPARの根本でございます。今、髙橋さんから指摘がありました内容について回答させていただきます。

言われているとおり､車両に関する主となるハッキング事象がやはり昨今増加していて、多くのお客様が認識しているという状況です。そして、そのお客様が、やはり安心、安全のためにセキュリティ対策の充実化というものに対する期待が高まっていると我々は考えております。

現在、我々を取り巻く環境として、車に大きな技術革新が起きている中、車両技術が今後とも大きく進化できるように、品質と同様にセキュリティ対策は非常に重要だと認識しておりますので、JASPARとして必要な標準化技術を早急につくり上げたいと考えております。

以上になります。

○大橋座長　髙橋委員、今の御回答で御趣旨は満たされているのでしょうか。

○髙橋（滋）委員　どうでしょう。要は具体的な危険があるという御認識なのでしょうかと。これから自動運転というのをいろいろと車両技術が発達して標準化も進めるのだろうと思うのですが、それを要するに刑法的な規制がない状態で、本当に安心して技術を進められるという状態であるという御認識なのかなというのをお聞きしたかったのです。

○一般社団法人JASPAR（根本情報セキュリティ推進WG副主査）　我々は標準化技術をつくっていく上で、車にどんな脅威があるのか、どんな攻撃を受けてどんなことになるのかというのを、新しい機能を踏まえてJASPARの中で常に議論をしております。よって、その脅

威というもの、リスクというものが高いというところが見つかりましたら、その事象を整理して、そこから導き出される標準化技術をつくっていくということでございます。

実は我々、刑法にどのような期待があるかということを、JASPARの中で危険なリスク、リスクが高い事象について常に刑法の在り方を議論しておりませんでした。なので、そこについて回答することというのはできませんが、我々技術をつくる側としては、常に脅威リスクを分析しておりますというところが回答となります。いかがでしょうか。

○髙橋（滋）委員　どうも。

○大橋座長　落合委員は今の関連するものであれば。あるいはお待ちしてもいいですけれども。

○落合専門委員　関連はしますけれども、ほかのもあるので後で大丈夫です。

○大橋座長　分かりました。

それでは、法務省さん、栗木参事官、いかがでしょう。

○法務省（吉田管理官）　法務省でございます。私は法務省刑事局刑事法制管理官の吉田と申します。栗木に代わって、私からお答えしたいと思います。

先ほど御質問いただいた点のうちのまず第１点目、現在生じているサイバー空間における危険に対して刑事的な手当てが必要ではないかという点についてでございます。御指摘のとおり、刑事法の在り方については、デジタル社会の進展も踏まえつつ検討していく必要があるだろうと考えております。刑事的な対応としては、大きく分けて、手続の問題と、それから、罰則を中心とする実体法の問題とがございまして、手続法に関して法務省では検討会を立ち上げて、捜査公判手続のデジタル化の方策を今検討しているところでございます。問題の関心は、罰則を中心とする実体法の方かと思いますけれども、これについてもこれまで幾度かにわたって刑法の改正を行ってきております。コンピューター犯罪あるいは不正指令電磁的記録の罪をはじめとするサイバー犯罪に対応するための改正をこれまで幾度かにわたって行ってきたところでございまして、今後も新たな犯罪に適切に対応できるようにしていく必要があると考えております。

その上で、先ほどのお話にありましたように、刑罰を新たに設ける、あるいは加重する、強化するということになりますと、その分野への国家の介入、国家権限が入っていくということになりますので、当然萎縮効果が生じないかということも考えていかないといけないと思いますし、また、それだけの必要性があるのかというのを吟味していく必要があるのだろうと思います。実際に我々のほうで罰則の新設などを検討する際には、まずもって現行法で適切に対応できない事態としてどういうことがあるのかということを考えていきますし、また、どういう趣旨でどういう行為を規制の対象とすべきなのか、それを罰則として適切に切り取れるのか、さらには、類似の行為があるときにそちらを罰則の対象としないとすれば、そのように特定の行為だけを対象とすることにどれだけの合理性があるのかといったことも含めて、様々な観点から検討を行っているところでございまして、サイバー犯罪の領域においても同様に考えていく必要があるだろうと考えております。

以上が第１点目についてでございます。

それから、第２点目の、法制審議会が、こうした社会が動いていく中で機動的に対応できる体制になっているのかという御指摘、御質問についてでございます。法制審議会は、法務大臣からの諮問を受けて、刑事、民事の基本法制について調査審議を行うことを目的とする審議会でございます。審議会としては総会と呼ばれる会議がございまして、諮問がなされますと、まずその総会で議論が行われることになります。さらに、専門的な見地からの詳細な議論が必要であると総会で判断されますと、そこで部会が設置されるということになります。その意味で、部会の設置をするかどうかは総会の判断でございます。その部会においてどの程度時間をかけて議論するかというのは、まさにその諮問事項の内容によることでございまして、例えば、昨年の国会で成立した危険運転致死傷罪の改正に関しては、部会は２回ほどで終わって結論が出たということでございます。他方で、今、国会で御審議いただいている少年法の改正については３年以上の議論が行われたということでございまして、内容によるということでございます。諮問をするかどうかは大臣の御判断になってきますけれども、その前提として、どういう事象が社会で起きていてそれに対して刑事法的な対応が必要なのか､あるいはどういう形での対応が必要なのかということは、事務当局である法務省刑事局、あるいは民事法であれば民事局のほうで常に検討していくということになろうかと思います。

以上でございます。

○大橋座長　髙橋委員、以上の御回答はどうですか。

○髙橋（滋）委員　法務省にお聞きしたいのですが、今の参考人の方のお話をお聞きすると、サイバーセキュリティについて包括的に議論するということが今、必要なのではないかと思います。かつ、その際には、機動的に、例えば、個人情報保護法ですと、通常５年見直しなのが個情だと３年見直しで技術の発展に対応しています。そういう意味で、早い段階で法制的な手当てを迅速にしていくことが肝心である。こういう体制にしていくということについての新しい立法の在り方を考えるということが、今、求められているのではないかと思うのですけれども、それについてはどうでしょうか。

○大橋座長　お願いできますか。

○法務省（吉田管理官）　法務省でございます。

御指摘は理解するところでございまして、我々のほうでもサイバー犯罪への対応の在り方は常に社会の情勢を見ながら考えてきているところでございます。その上で、この領域については、刑法が今議論に上がっておりますけれども、刑法だけで対処しているものではないので、ほかの法領域というか刑事法の中でも幾つかに分かれていく中で、我々がどこまで自分の所管を踏まえてどう考えていくべきなのかということも一つ頭に置いておく必要があるのだろうと思っております。

いずれにしても、技術の進展が早いというのはそのとおりだと思いますし、新たな犯罪事象が出てきて、我々も検察の現場でどういうことが起こっているかということは情報と

して得ておりますので、例えば、新たな犯罪事象が起きてきて、現場で適用できないような事態が生じているということになりますと、それは新たに捕捉すべき事態ではないかということも含めて検討しておりますし、またこれからもしていきたいと考えております。

○大橋座長　今回の御発表の中で、構成要件の在り方についてもより包括的に考えるべきではないかとか、あるいはこれまでの構成要件の中で立件可能なものとして、この新たな犯罪に対する適切な対応の中で新しい考え方を取り入れるべきではないかという御指摘が幾つか見られたのですけれども、そこの辺りについては同意されるということで良いでしょうか。

○法務省（吉田管理官）　構成要件の在り方については、先ほど少し言及があったと思うのですけれども、憲法上の要請である罪刑法定主義が規律する世界でありますので、包括的に、その意味にもよるとは思いますけれども、幅広く取ればいいというものではないのだろうと思います。明確性の問題もそうですし、また過度に広範な規制になってもいけないということも問題になってまいりますので、その辺りはこれまで我々としては立法事実を踏まえながらどういう行為をどういう根拠で規制するのか、そのためにはどういう規定ぶりにすべきなのかということを、刑事法学者の先生方からまさに法制審議会で御議論いただきながら検討してきたところでございまして、その基本的な姿勢は維持することになるものと思います。

その上で、そういう考え方に立ちつつも、例えば、ある特定の事象が起こったときにそれだけを見て規制をするのではなくて、似たような事象として論理的に考えられるものを専門家の御知見も借りながらいろいろと想定をしていって、同様の当罰性がある行為があり得るのだということであれば、それを念頭に罰則をつくるということはあり得るのだろうと思います。

○大橋座長　ありがとうございます。

それでは、警察庁、お願いできますか。

○警察庁（新田審議官）　警察庁の交通局担当の審議官の新田でございます。

警察庁交通局は道路交通法を所管しておりますけれども、昨今の自動運転技術、レベル３に対応した改正も行っておりまして、レベル３になりますと自動運行装置というものを前提として運行されるということですから、サイバー攻撃ということもちゃんと視野に入れながら法律的対応をしていく必要があるという認識でおります。そういった自動運行車に対するサイバー攻撃への対応としては、我々の所管外の法律にはなりますけれども、国土交通省が所管している道路運送車両法において、不正改造等の禁止とか、あるいは令和２年の改正により、レベル３以上のものを想定して追加された特定改造等の許可、その許可を経ないで勝手に改造等をするということがあれば罰則はあるといった制度なども構築されております。こういった法令の適用に当たっては国土交通省、それから、法務省とも連携し、サイバー攻撃に対してもしっかり対応できるようにアンテナを高くしていかないといけないなと思っているところでございます。

ちょっと雑駁ではございますけれども、そういったことです。
○大橋座長　信号機の制御機能に干渉するというのは、警察庁の所管所掌なのですか。
○警察庁（新田審議官）　信号機の制御機能への干渉に対応し得る規定としては、道路交通法第115条がございます。先程のJASPAR様等のお話からすると、サイバー攻撃のタイプとしてはコネクティッドカーを通じて信号機、管制システム等にサイバー攻撃をして、信号機を操作するものを想定されているのではないかと思います。この点、道路交通法第115条は、みだりに信号機を操作し、若しくは公安委員会が設置した道路標識若しくは道路標示を移転し、又は信号機若しくは公安委員会が設置した道路標識若しくは道路標示を損壊して道路における交通の危険を生じさせた者は、５年以下の懲役又は20万円以下の罰金に処するといった規定でございます。本条についての我々の理解は、「信号機を操作し」とは、作動していない信号機を作動させたり、信号機の信号の表示を変えたり、又は作動している信号機を停止させることを指しており、どのように信号機を操作するという手段や、その方法の態様に特段の制限はないと考えております。したがって、コネクティッドカーを通じたサイバー攻撃による信号機の不正な操作に対して、個別具体の事案によるものの、基本的に適用し得るものと考えているところでございます。
以上でございます。
○大橋座長　ありがとうございます。
法務省は手が挙がっていると認識してよろしいですか。
○法務省（吉田管理官）　ありがとうございます。法務省でございます。
今の警察庁の方からの御説明に補足して、刑法の関係でも御説明したいと思います。刑法には、電子計算機損壊等業務妨害という罪がございます。これは人の業務に使用する電子計算機に虚偽の情報や不正な指令を与えるなどして電子計算機に使用目的に沿うべき動作をさせず、または使用目的に反する動作をさせて人の業務を妨害する行為を処罰対象とするものでございまして、法定刑は５年以下の懲役または100万円以下の罰金となっております。先ほどお話のありましたコネクティッドカーを通じた信号機への干渉行為については、その信号機の中にある電子計算機に不正な指令を与えて誤作動を起こさせて、その結果、本来表示すべき信号と違う信号を表示させるなどした場合には、交通規制という業務を妨害するということでこの罪が成立し得るものと考えております。もちろん最終的には捜査機関が収集した証拠に基づいての判断ということになりますけれども、同罪が適用され得ると考えております。
以上です。
○大橋座長　ありがとうございます。
それでは、玉城委員からの御質問もあったので、可能であればお時間のあるまで手短に稲谷委員と西貝委員からそれぞれお願いできますか。
○京都大学（稲谷教授）　ありがとうございます。稲谷でございます。
玉城先生のおっしゃることは非常によく分かるところでございます。御質問があった、

カオスのような状態が生じうることを想定して、そこからシステムをどのように守っていくかという議論が刑事法でどのぐらいなされているのかについてですが、あまり現状ではなされていないと思っております。システムに対する干渉行為に関して玉城委員から御懸念があったところというのは、信号との干渉もそうかもしれませんが、車と車の干渉であるとか、あるいは車同士・車とインフラとのやり取りそのものが阻害されてしまうことによって重大な事象が起きるということだと思います。そちらについてどう考えていくかというのは、まさに先ほど申し上げたような問題になると思います。

もう一つは、カオスが発生することを理解した上で、あえておかしな挙動をする行為をどのように規制していくということに関してですけれども、私の理解におきましては、それはある種の干渉行為に伴う結果的加重犯の一種として、最終的に交通のようなもの、大きな公益みたいなものが阻害されるケースとして捕捉していく可能性があっても良いかもしれないと、お話を伺いながら思いました。

最後に、このような危険があるといっても、どこまで気をつけて製品やサービスを作ればいいのかという点を考えてくれないと、エンジニアのサイドとしては困るという話もあったと思うのですけれども、どこからをまずい干渉行為とするかといったところの線引きというのは、これまでも萎縮効果との関係で問題になっていたところだと思うのですけれども、まさにそういった点をすり合わせていくために、早い段階で開発者と規制当局・司法当局とが連絡をどんどん取っていって実質的な処罰基準みたいなものを明確化していくというやり方のほうがよろしいのではないかというのが私の感触でございます。ありがとうございました。

○大橋座長　ありがとうございます。

もしよろしければ、西貝先生も手短にお願いできればと思います。

○千葉大学（西貝准教授）　手短に申し上げますと、既知のカオス理論に基づいて渋滞をわざと惹起させる行為とかについては、自動運転システムというのが復旧したときにどのように自動運転の業務というのに取られるかによりますけれども、先ほど法務省さんからあったように、電子計算機損壊等業務妨害罪や偽計業務妨害罪の成立可能性が一応検討されるのではないかと思っております。電子計算機損壊等業務妨害罪に関しては中間結果という要件がありまして、電子計算機に使用目的に沿うべき動作をさせずというところの辺りがもしかしたら認定が難しいとか立証が難しいことがあるかもしれないと思っておりますが、偽計業務妨害罪のほうで渋滞のない円滑な交通を維持する業務などと例えばもし考えることは可能なのであれば、偽計業務妨害罪の可能性もあると一応理論的には考えられなくもないというところだと思います。

たしかお話の中で出てきたのは、既知の理論に基づくとこうなるという場合ですけれども、既知の場合にはもしかしたらそういうことが可能かもしれないのですが、未知のカオス理論というか、何かよく分からないけれども渋滞が起きているとかになってきますと、もはや偽計業務妨害罪というのは危険犯と解されておりまして、業務妨害の危険が発生す

れば足りるとはいえども､その因果関係が何が起きているのかよく分からないのであれば、誰のせいで業務妨害の危険というか渋滞が発生してしまったのかが分からないということで、立証が難しくなってくるのかなとちょっと思ったところです。

以上です。

○大橋座長　ありがとうございます。

それでは、手を挙げている落合委員、お願いいたします。

○落合専門委員　ありがとうございます。

そうしましたら、ほかの委員からもちょっと手が挙がっていないこともあるので、何問か質問させていただければと思っております。

稲谷先生に御質問がございまして、先生の御発表の中で社会インフラというお話がありました。今日は主に自動走行車の議論をされていたとは思うのですけれども、例えば、スマートシティーだったりそういう話が出てくるときに、あまり別に何か車だけの話とかをおっしゃられているわけではなくて、ということなのかと思って伺っておりましたが、それはそういうことなのでしょうかということがあります。あとは結果的加重犯だとかそういうところで、例えば、JASPARさんにというよりかは稲谷先生に伺ったほうがいいのかなと思ったので御質問します。自動運転車のシステムが改ざんされた場合に、ほかの自動車との関係でも要するに危険が生じるということで、個人的な生命、身体というだけではなくて、社会的法益の侵害みたいなような形がより容易に起こりやすいので、そういったところを捉えて構成要件の整備もするべきだろうし､結果的加重犯というところで､例えば、それによって人が死亡したような場合とかというのはより重く処罰するべきではないかという考えがあり得るとこういうことなのでしょうか、というのが御質問です。

あともう一点すみません、稲谷先生の捜査協力の話もあったと思うのですけれども、米国ですとCLOUD法ですとか、EUにおいてもそれに対応するような法制が整備されているということが2018年ぐらいから諸外国では行われてきていると思います。先生のほうで特にこういった協定として議論に値するだろうと思われる項目としてどういうのがあるでしょうか。

あと、西貝先生と。

○大橋座長　短くまとめられますか。

○落合専門委員　すみません。これで大丈夫です。

以上です。

○大橋座長　ありがとうございます。

髙橋委員、お願いします。

○髙橋（滋）委員　どうもありがとうございました。

法務省からの御回答で承ったところについてです。既存の規定でカバーできるか。そこをぎりぎりやって、できなければ新しい立法をする。そうすると、既存のところの構成要件がまずあって、それは要するに残っている。それでは、結局、新たな事象のなかですく

い取れないものが出てくるわけです。道路交通法の話をされましたけれども、交通の危険という要件が現にあるわけでから。

もう一つは、偽計業務妨害も、先ほど出たように、複数の人間が関与したときに、それが全体として道路交通の業務を妨害したときにどうやって立証するのだという話が出てくるわけです。すくい取れないものが出てくるときに、それを全部見直して、適切にその保護法益に対応できるように刑罰規定を見直すというのは、これは、技術進歩のこの時期には恒常的に実施していく必要がある。そうでないと、結局パッチワークになるのではないかという話になります。そこのところを直してほしいというのが今回の極めて重要なお願いなのだと私は思っているのですが、それについてのコメントをお願いしたいということです。

あわせて、例えば、刑法でも紙と電磁的な記録で本当にバランスが取れているのと、そもそも私は疑問を持っていて、例えば、電磁的記録不正作出の罪、電子的な記録の刑罰については、包括的に規定が置かれています。ところが、紙については有印と無印と分けていて量刑を分けている。要するに、印鑑というものを明らかに差別して保護しているわけです。ところが、電磁的な記録のところは例えば、印鑑を持っている本人認証とか意思のいわゆる確認というところを区別しないで、ざっくりと刑罰をかけている。きちんと対応ができていないわけです。要は、印鑑だけ突出して保護する刑法的な体系になってしまっていて、それとパラレルに、印章の偽造についても、電磁についての本人確認と意思確認のデータを偽造というところで、特に罰しているのかというと罰していないわけです。結局、パッチワークで対応してきた、デジタルの社会に対応できていない規定になっているのではないかという根本的な疑問があるわけであり、そういう点をきちんとこの際直してほしいというのが私のお願いです。その辺についてどう思っていらっしゃるのかということをお聞きしたいということです。

○大橋座長　ありがとうございます。

稲谷先生、手短にお願いできれば幸いです。

○京都大学（稲谷教授）　ありがとうございます。

落合先生からいただいた御質問ですけれども、最初の点に関してはそのとおりでございまして、今回たまたま出席される方の御関心の関係から自動運転車の問題を取り扱いましたが、社会インフラ全般に関係する問題だと考えてございます。

もう一つは、公共危険的な側面というものは私も大変重要であると思っておりまして、どちらかというと、単に個別の人が死んだというよりも、まさにその公共危険罪的な側面ですよね。往来危険であるとか転覆であるとか、ああいったタイプの危険として考えていくべき側面というものが含まれるであろうと考えてございます。

最後の域外捜査の協力情報に関してなのですけれども、こちらについてはちょっと時間の関係もあり、詳細は簡単に御説明するのは難しいのですけれども、アメリカと日本で捜査の手法とかで異なっているところが幾つかあります。そこで、双方の捜査の実施につい

て、どういった要件ですり合わせていくのかといった辺りは、協定を結んでいく上では重要になると思いますし、EUの方も同じようなことが言えるのではないかと現状では考えております。

以上です。

○大橋座長　ありがとうございます。

それでは、髙橋先生の御質問に対して、法務省、警察庁、順にお答えいただければと思います。

○法務省（吉田管理官）　では、法務省からまずお答えしたいと思います。

刑事法のパッチワーク化を解消すべきだという御指摘だったかと思うのですけれども、もともと刑事罰自体が謙抑的につくられ､運用されるべきだという考え方がございまして、現実に刑罰を設けなければいけない、それによらなければならない事象が生じたときにつくっていくということになりますので、ある意味、パッチワーク化というか、必要な部分に手当てをしていくということ自体は、刑罰というものの性質上一定程度はやむを得ないことだろうと考えております。

また、サイバー犯罪に関わる法領域も、刑法だけではなくて様々な法領域によって対応しておりますので、刑法だけで対応できるものでもないということでございます。そういう中にあって､電磁的記録の部分だけを取り上げて統一的に何かを法整備するというのは、難しい課題が様々あるのではないかと考えております。

以上です。

○大橋座長　ただ、紙と電子のバランスは考慮すべきかどうかというのは、ここはどうなのでしょうか。

○法務省（吉田管理官）　これまで電磁的記録についての改正を複数回行ってきておりますけれども、紙媒体と電磁的記録との性質の違いを踏まえて、電磁的記録については紙とはやや違う規制の仕方を行っておりますので、そういう意味で違いは考慮しながら法整備を行ってきているということでございます。

○大橋座長　その間に合理性がなければならないということですね。

○法務省（吉田管理官）　はい。

○大橋座長　ありがとうございます。

それでは、警察庁のほうからお願いできますでしょうか。

○警察庁（新田審議官）　御質問の趣旨は、サイバー攻撃で生じた事態をしっかりアンテナを高くして捉えて、それに沿った、それをもっと前から捉えて立法などをどんどん行っていくべきではないかという御趣旨だったかと思います。先程御説明したとおり、信号機に対するコネクティッドカーを利用したサイバー攻撃については､現行の道路交通法第115条は、御指摘のような事案に対して広く適用し得ると思っているところでございます。具体的には、先程申し上げたとおり、信号機を操作する手段にかかわらず、同条を適用し得るのではないかと考えているほか、同条中の「道路における交通の危険を生じさせ」とい

う部分につきましても、必ずしも現実に危険が発生したことは必要とせずに、道路における交通の危険を生じさせるおそれがある状態を生じさせれば足りると考えております。いずれにせよ、今後、どういった事象が考えられるかということについて、アンテナを高くして考えていかねばならないなというふうに考えているところでございます。また、同条に規定する罰則は５年以下の懲役又は20万円以下の罰金であり、こういったタイプの行政刑罰としてはかなり重いほうではないかなと考えているところですが、今後、委員御指摘の課題については、行政法だけではなく、往来危険罪が規定されている刑法体系の全体の中で考えていくべき問題と考えております。

以上です。

○大橋座長　ありがとうございました。

ちょっとお時間の制約のなかで、若干議論が必ずしも十分尽くされていたかどうかと思っていますけれども、中島先生から、やはり刑法といえども経済インフラであるというお言葉をいただき、また、田中先生からも、やはり条文としては適用されるものでないといけなくて、それが抑止力を生むのだと。更に究極的にそれがイノベーションを生み出す素地になるのだというお話もいただいたところですので、今回、個別の法律という話にはなっていませんが、そういうところをぜひ念頭に置いて、刑事法の在り方全般をデジタル化に合わせて見直すべきだというところのメッセージをしっかり受け止めていただければと思っております。

本日は諸先生方、JASPAR様を含めて御説明、本当にありがとうございました。ヒアリングはここまでとさせていただきます。お時間ありがとうございました。

（説明者退室）

（説明者入室）

○大橋座長　続きまして、議題２に移ります。「データ駆動型社会に向けた情報の整備・連携・オープン化」でありまして、これは＜不動産関連市場の活性化に向けたデータの整備・連携＞ということで、国土交通省にヒアリングを行いたいと思います。

本日は、国土交通省不動産・建設経済局より天河審議官、皆川課長及び井﨑課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。５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、早速ですがお願いできますでしょうか。

○国土交通省（天河審議官）　不動産・建設経済局審議官の天河でございます。どうぞよろしくお願いいたします。

それでは、資料に基づきまして御説明をさしあげます。

まず、１ページ目でございますが、経緯ということで、昨年７月の規制改革実施計画で閣議決定をいただいておりまして、書いてあることといたしましては、不動産IDとして不動産登記簿のIDを活用していこうと。それから、いろいろなデータベースとの連携、不動産関連データの整備を進めるということで、民間事業者によるデータ連携が進むように、国交省が主体的に各種取組を進めていきなさいということをいただいております。

この閣議決定を受けまして、この３月までに事業者様とか業界団体様、こういったところにヒアリングをさせていただきまして、いろいろデータ連携の在り方について関係府省庁と意見交換を実施してきております。

検討の状況でございますが、一番下の箱の中にございますが、２つの角度からやっておりまして、一つは不動産IDの内容・取組対象に係るルールということで、不動産IDとして何を使うかと。私どもは登記簿の不動産番号がいいのではないかと思っておりますけれども、まずIDとして何を使うか。それから、取組の対象不動産・対象取引といったところで、全ての不動産あるいは賃貸を含めた取引等を対象にしていきたいと思っていますが、そういったことをまずどういうルールにするかということを検討しています。

それから、IDの利活用・普及に必要なルールということで、これは実際にレインズとか業界団体、あるいはいろいろなポータルサイトを運営されている事業者、そういった民間の事業者さんが主になると思いますが、そういったところでどういったルールを決めてこのIDをしっかり使っていくかということ、この２つの観点からの検討を進めてございます。

次のページでございますが、IDのルールの整備についてということで、何でそんなことをやる必要があるのだということでございますが、新型コロナウイルスもありまして、不動産市場の先行きが不透明ということが一つございます。そういった中で、ますます不動産流通市場の活性化とか、さらには、不動産流通市場が活性化されれば、当該資産、土地、建物といったものの有効活用がさらに促進されていくだろうということが考えられます。それを進めるためには、新たなテクノロジーを積極的に活用していくということで、そういったことによりまして、官民が要します不動産のいろいろな情報がございますが、そういったビッグデータの連携を促進していくことで、より市場の透明性の向上とか、不動産に関わる意思決定の迅速化、あるいは高度化といったものを図っていきたいと思っています。

現状を見ますと、宅建業者さんとかデベロッパーさんにおきましては、いろいろなところに不動産に関する情報があるのですが、これをある意味人力で集めて名寄せをしているということで非常に大きな労力になっているということがありますので、こういった不動産のデジタル化、IDをもってデジタル化が進んでいけば非常に生産性が上がるということがあると思います。その裏返しといたしまして、消費者にとっても必要な情報が非常にタイムリーにあるいは低コストで得られるということで、消費者にとってもいいのではないのかと思っています。

そういったことが実現していきますと、今、いろいろ問題になっています所有者不明土地とか低未利用不動産、こういったものにつきましていろいろなことをやろうとしたときにいろいろなコストが下がってまいりますので、関連情報へのアクセスの円滑化を図る、そういったことによってこういった課題も解決することができるのではないかと思っています。

そして、課題といたしまして、各不動産にひもづく共通コードが存在しない。それから、

各主体間をまたいだ不動産情報の名寄せができない。要するに、情報がなかなかデジタル化されていない、連携していないということですが、これを解決するために不動産IDをしっかり整備していきたいと我々としては思っています。

想定される主なメリット・ユースケースといたしましては、先ほど申し上げた課題と反対になりますけれども、不動産市場の透明性が向上すること、あるいは取引が活性化する。それから、不動産業の生産性の向上や消費者の利便性向上、低未利用不動産の有効活用、所有者不明土地の探索といったことが考えられます。テクノロジーをしっかり使いまして、こういったいろいろな重複掲載防止とか、おとり広告排除、これはなかなか細かい話ですけれども、こういったことも考えられますし、AI価格査定といった新しい技術みたいなものも開かれるということが期待されるところでございます。

次のページでございますが、ルール整備に当たりまして、一つ課題がまずございます。この下の箱の３つ目ですけれども、区分所有でない共同住宅につきましては、不動産番号は１つしかないものですから、これに枝番を振っていかないといけないという課題が一つございますということが書いてございます。

次のページに参りまして、今申し上げた課題も含めて、①の課題ということで、共同住宅のIDの部分をどうするのか、それから、分筆とかその際どうしていくかといった、細かい話ですけれども課題でございます。

それから、ルール整備ということで、冒頭に申し上げましたけれども、レインズとか業界団体でいろいろな運営サイトを運営されております。それから、いろいろなデータベースにおけるルールの在り方を決めていかないと、それがばらばらになるとせっかくIDをつくっても意味がないものですから、しっかりルールを決めていきたいということが②でございます。

最後の個人情報に係る課題といたしまして、不動産番号につきましての物件情報につきましては、個人情報保護法の個人情報に該当すると整理されているということもありますので、そこをしっかり私どもとしていろいろな民間の取引などを見つつ、あるいは関係省庁と話をしながらクリアしていきたいと思っています。これにつきましては、現在、ベース・レジストリの議論が進んでいますので、こういったものもしっかり見ながら対応していきたいと考えております。

以上でございます。

○大橋座長　ありがとうございます。

時間があと10分弱なのですけれども、ぜひ委員の皆様方、御議論いただければと思います。

まず、村上委員からお願いいたします。

○村上専門委員　村上です。ありがとうございます。４点質問があります。

１点目が、この不動産IDは国土交通省さんが責任を持って管理運用していくということでいいのか。その際、法務省との調整状況が今、どうなっているのか、IDにするとなると、

不動産登記の義務化とか所有者不明問題が出てきますので、この点について教えてください。これが１点目です。

２点目が、自治体の固定資産台帳との連携のニーズが高いと思いますが、こちらについての検討状況を教えてください。

３点目、賃貸物件まで広げるということですが、その必要性について、誰にどんなメリットがあると考えているのか。

最後に４点目、３月24日の成長戦略ワーキングで、新経連さんから、国土交通省の不動産総合データベースの実証が終了して実用化に至っていないという説明がありました。実用化に至っていない要因と今後の予定を教えてください。

以上４点です。

○大橋座長　ありがとうございます。

落合委員、お願いします。

○落合専門委員　私のほうも２点ほどでして、まず第一点は、村上委員もちょっとお話しになったのですけれども、この不動産のIDというのにひもづけて、例えば、宅建業者とかですと何十種類もの書面を取り寄せてということをやられて、重要事項説明書を作られると思います。このため、どこまで広くデータをつなぐ基盤にしていくということで構想を持たれているのかというのが一つです。

もう一つが、個人情報の論点があると思っておりまして、これは民間の個人情報保護法については個人情報保護委員会のほうで整理がされているということもありますし、恐らくそれに寄せて整理がされていくだろうということも先日WGを開催しており、今後考えられますので、そういった点も踏まえて御検討いただければと思っております。

以上２点です。

○大橋座長　ありがとうございます。

高橋代理、お願いします。

○高橋（進）議長代理　農地とか森林も対象になるのか、あるいはそういうことに関して農水省と何か連携の余地があるのか、その辺を教えていただければと思います。

○大橋座長　以上が手の挙がっている方々でありますので、国土交通省さんのほうでお答えいただければ幸いです。

○国土交通省（皆川課長）　では私から。国土交通省の不動産市場整備課長の皆川でございます。よろしくお願いいたします。

まず、村上委員から質問がありましたIDの件ですけれども、国土交通省としては、このルールメイキングということで、どのようなものをどういう形で使っていくかということで、ルールメイキングを中心にすると考えてございます。当然、不動産登記、不動産の番号を使っていくということになれば、まさに法務省さんとの調整も必要となります。昨年の閣議決定でも不動産の登記のことを述べられておりますけれども、これを踏まえて、法務省さんとも既に話は進めております。確かに今おっしゃるように、義務化とかといった

広がりを、こういったところが進めば、さらにこのIDの利活用も進んでいくところもあると思いますけれども、その辺りも含めてこれからまた法務省さんとはよく調整、すり合わせをしていきたいと考えてございます。

それから、２番目の自治体の課税台帳などとの連携ですけれども、これは農地とか林地、そういったものの台帳など、いろいろ公的主体で台帳をいろいろ管理しているというのを聞いておりまして、今、IT室さんのほうでこういった公的機関の情報についてはいろいろ議論されていると聞いております。この辺りも法務省さんとも話をしながら関係省庁の皆さんともよく情報共有して活用の広がりを持たせていきたいと考えてございます。

それから、賃貸に関しては、売買に比べて賃貸物件のほうが非常に取引の頻度が、反復して何度も同じ物件が取引されるといった傾向にございますので、そういう意味ではIDをつけることによって価格がどのように変化していくか。例えば、リフォームとかそういったことを行った場合にはどのように価格が変化していくかとか、いろいろ価格がどう推移していくかという意味ではニーズがあると考えてございますので、そういった意味で賃貸も含めた議論ということでございます。

○国土交通省（井﨑課長）　不動産業課長をしています井﨑と申します。

村上委員から４点目で御質問がございました不動産総合データベースの件でございます。不動産総合データベースにつきましては、落合委員からもお話がございましたように、不動産取引をする際に、宅建業者がその不動産に係る様々な情報について調査、情報収集をして重要事項説明等を行うわけでございますが、その負担が非常に大きいということから、宅建業者が不動産に係る各種の情報を容易に入手できる、さらにその先には消費者に適切に提供できるようにということで、都市計画に関する情報などの各種の法令制限、また、道路等のインフラ整備状況やハザードマップ等の整備状況等について、宅建業者に情報を電磁的方法で提供するというシステムをデータベースでつくろうということで検討を進めてまいりました。平成25年から検討開始をいたしまして、順次検討を進めて、各幾つかの地域では実証実験等も行ってまいりましたが、そこで分かったことといたしまして、先ほど申し上げました都市計画とかインフラの情報、こういったものを、これは自治体が持っている情報が非常に多いわけですけれども、これらのインフラや都市計画等の情報について、それぞれの自治体がデジタル情報として提供している状況、また、その情報の正確性等がまちまちだということがございまして、なかなか現時点で宅建業者が重要事項説明として使うのに十分な正確性、最新性が担保されていないということが判明いたしました。

したがいまして、現時点で全国システムとして十分に機能するものを構築できる段階にはないということで、課題の整理に現時点ではとどめているところでございます。今後、このワーキング・グループで御議論いただいておりますベース・レジストリの整備が進みまして、正確性、最新性が確保された各種情報が充実していきますと、私どもが今日御説明しました不動産ID等のルール整備との連携によりまして、必要とされる不動産情報が効率よく収集、活用できるような不動産総合データベースの趣旨も実現されていくように取

り組んでまいりたいと考えております。
○国土交通省（皆川課長）　続きまして、皆川から。
今、落合委員からありましたIDとどのように情報をひもづけていくかという話でございますけれども、先ほど井﨑からも話がありましたが、最新性が担保された情報としてベース・レジストリの議論が今あるというふうに伺っております。IDとしてはある程度情報を結びつけていくのならば、そういった最新性なりというところとの関連も必要かと思いますので、ベース・レジストリも今動いているというふうに聞いておりますので、そことの兼ね合いもあればそれのニーズなども確認しながら検討していきたいと考えてございます。
それから、２番目にありました個人情報の扱いは、まさに私どもも今回、資料に載せておりますけれども、個人情報の話が大きな課題だと思っておりまして、先日のワーキングの議論の中でもいろいろ行政機関の情報の在り方についても議論を聞いております。その辺りも踏まえて、私どもの整理も併せてしていきたいと考えてございます。
それから、高橋委員からありました農地、森林ということですけれども、先ほど少し申し上げた公的機関のそういう土地台帳なり様々な台帳が連携するという動きもあるようですので、まず私どもとしては不動産取引として行われていくものを念頭に置いていますけれども、当然、連携できる部分はあろうかと思いますので、その辺りもまた関係省庁の皆さんとも検討や話をさせていただきたいと思っています。
以上でございます。
○大橋座長　ありがとうございます。
お時間がもう来てしまっているのですけれども、村上委員も手が挙がっていますか。
○村上専門委員　簡単に。
○大橋座長　どうぞ。
○村上専門委員　すみません。
ルール整備ということは、不動産IDの正確性を担保するのは法務省さんがやるということですか。それと不動産取引とおっしゃいましたけれども、取引されない不動産もID化は必要なので、その点を最後に教えてください。
○大橋座長　お願いできますか。
○国土交通省（皆川課長）　皆川でございます。
正確性という意味では、まずは登記情報がベースになろうかと思いますので、そこはやはり法務省さんの登記データをベースにやっていくということになると思います。
それから、取引されたものについても、基本的には不動産番号といったものをIDとして使っていくことということがあるかと思いますけれども、ただ、私どもとしてはやはり取引の機会に不動産番号というものを付記して、それで相手に渡ると。それがデータとしてたまっていくことでまた別の技術なりに活用できるというふうに考えてございますので、ルールとしては、一旦今の取引されていないものもIDが付与されると思いますけれども、実際に動き出すのはやはり取引の際ということをイメージしております。

○大橋座長　村上委員、よろしいですか。
○村上専門委員　不動産IDは取引されないものにも全部振られるということであればそれでいいと思います。
○国土交通省（皆川課長）　そうですね、全てのものにという意味でございます。
○大橋座長　ありがとうございます。
本日、ちょっと時間が押してしまって恐縮ですけれども、ここまでとさせていただきます。御議論の中で情報管理の責任の所在とか、あるいはその情報の更新、メンテナンスの在り方も含んでいるのだと思いますけれども､そこの辺りのところについては論点として、関係機関としっかり連携をしていただきたいということがあったと思いますし、同様の連携というのは固定資産税の徴収、あるいは管理時に不動産IDを使うことについても同様の論点があるということで、ここについては今後進めていく上でしっかり念頭において検討していただければということが御議論だったかと思います。
本日はお忙しいところありがとうございました。議題２は取りあえずここまでとさせていただきたいと思います。
○国土交通省（天河審議官）　どうもありがとうございました。
○大橋座長　ありがとうございます。
取りあえず本日の議事は全てこれにて終了となります。
最後に、藤井副大臣から一言いただければと思いますが、いかがでしょうか。
○藤井副大臣　内閣府副大臣の藤井です。
まさしく自動運転につきましては、これからの日本の産業の基軸であるとともに多くの皆様にとっての最大のサービスになってくると思います。そこの刑事法上の整備も含めてしっかりと。これは世界に立ち後れる可能性がありますので、そういう点でも法制のほうで、言わば足を止められないようにお願い申し上げたいなと思います。
また、不動産に関しましては、不動産を動かすことがまさに経済活性化に役立ちますので、これからも建設的な意見交換をよろしくお願い申し上げたいと思います。今日はどうもありがとうございました。
○大橋座長　ありがとうございます。
それでは、本日の会議はこれにて終了といたします。若干お時間が延びてしまって申し訳ございませんでした。本日はありがとうございました。