国家戦略特区ワーキンググループ　ヒアリング（議事要旨）

（開催要領）

１　日時　平成28年４月22日（金）13:30～14:06

２　場所　永田町合同庁舎７階特別会議室

３　出席

＜ＷＧ委員＞

座長　八田　達夫　アジア成長研究所所長
　　大阪大学社会経済研究所招聘教授

委員　原　　英史　株式会社政策工房代表取締役社長

＜提案者＞

眞柄　泰利　サイバートラスト株式会社代表取締役社長

東　　久貴　サイバートラスト株式会社技術本部長

鈴木　重雄　サイバートラスト株式会社
　　セキュアIoTプラットフォーム推進事業本部長

板東　直樹　サイバートラスト株式会社社長室長

＜事務局＞

川上　尚貴　内閣府地方創生推進事務局次長

藤原　　豊　内閣府地方創生推進室次長

（議事次第）

１　開会

２　議事　Secure IoT Platformによる“IoT Sim City”実証実験

３　閉会

○藤原次長　それでは、国家戦略特区のワーキンググループヒアリングを始めさせていただきます。

今日も八田座長、原委員にお出でいただいておりますが、最初の30分は、こちらはサイバートラスト社の方々にお出でいただいております。

特区も近未来技術の実証をする特区ということで、ドローンとか自動走行とか規制緩和の話とともに、色々なプロジェクトも特区のプロジェクトということで地域で実証実験が行われているところでございますが、それに色々とまた貢献いただくようなお話が今日お聞きできると聞いておりますので、話を伺いたいと思っております。

それでは、八田座長、よろしくお願いします。

○八田座長　どうもお忙しいところお越しくださいまして、ありがとうございます。

それでは、早速、御説明をお願いします。

○藤原次長　原委員からも一言よろしいですか。

○原委員　是非ワーキンググループでお話を伺えればと思います。

○眞柄社長　では、お手元の資料を元に御説明申し上げます。

めくっていただきまして、私たちのプロフィールが書かれてございます。ここで申し上げたいのは、私どものほうで左端にあります「端末認証サービス」と書かれておりますのが、現在私どもの売上げの約２割でございまして、この４年間で年平均40％ほど伸びているビジネスでございます。

本日御説明申し上げますのは、これをベースにしてIoTの社会に向けてセキュアな環境を作りたいという、今、前段で御説明がありましたけれども、この１・２年の間に私ども自身でいくつかPOCを実施していますので、今日はその御案内となります。

○八田座長　POCというのは。

○眞柄社長　失礼しました。Proof of conceptで実証実験でございます。

次のページに行きまして、その端末の認証のサービスがどういったものかということでございますけれども、今、私どものほうで国内の160万台の端末、端末と言いますのはパソコン、モバイルフォン、タブレットを示していますが、OSについてはWindows、iOS、Androidになります。そういった機器の中に秘匿メモリ、外からは一般的には見ることのできないメモリ領域が各社持たれておりまして、その中に私どもの電子証明書をインターネットを経由して入れさせていただくサービスになります。

これが何がいいかと言いますと、会社の中にあります、例えば、ファイルを取りに行くときには、ここにありますけれども、VPN機器と書いてありますが、そういったところを通して会社の中に入るのです。この通したところの中にどうやって認証するかというときに、私どもの電子証明書を使って、間違いなくサイバートラストという国際的な監査を受けた認証機関が出している電子証明書なので通しましょうというサービスをさせていただいています。とりわけアプリについては、コンシューマービジネスは強いのですけれども、エンタープライズの企業向けのビジネスが弱いということで、セキュリティに関しては何も彼ら自身が施策を打っていないものですから、この間iPhoneとかタブレットが企業に導入される中でこういう伸びを示していて、先ほどのとおり、この３年間で年平均３割から４割伸びているのがこのビジネスということになります。これによって企業が認可した間違いない端末ですよということと、証明書が入っていて、企業にアクセスされたときにはその通信が暗号化にもなります。したがって、セキュアだというのがこのサービスになります。

これを使いまして、今、私どものほうで、これに加えまして位置情報と時間情報、いつ、どこで、どのデバイスがという認証の基盤を作ろうとしているというのが、次のページになりますけれども、真ん中にありますライフスタイルイノベーション、ワークスタイルイ

ノベーションの中にありますSecure IoT Platformというところになります。認証機関において、どこで、何が、どうなったかというデータをセキュアにお預かりするというサービスになります。お預かりしたデータにつきましてどうするかというのは、後ほどまた御説明します。

ところで、今、最も安全なIoTのデバイスは何かと言いますと、おそらく車になると思います。いわゆるコネクテッドカーと言われておりますけれども、コンピューターを搭載して色々な車載情報をクラウドに上げて、それを車のメーカーが見て自動診断をしたり、あるいは直近ですと、そういったデータを使って自動車保険を適用するというような話も既に出ていると思います。そのときに、テスラという会社は御存じだと思うのですけれども、こういった会社が、車なのですけれども、IoTと位置付けた場合にどういった形で認証やらセキュリティを担保しているかというところがこちらのYouTubeに書かれておりますので、10秒ぐらいなのですけれども、画面のほうを御覧いただけますでしょうか。こちらがYouTubeのリンクになります。Auth KeyとかSSL Server、Client Certsと書いてあるのは、まさに今、私どもの申し上げた電子的に証明をしたり、認証したりというシステムを車の中に搭載して組み上げて、自動車をテスラは走らせているということになります。

こういったことをテスラが自分だけでやっているかと言うと、今オープンイノベーションと言われていまして、色々な人たちが集まっていいものを作ろうという流れがあるのですが、こちらの場合は、実はこのプレゼンはどういうことかと言うと、ハッカーのイベントでのプレゼンです。ここに実はテスラのCTOとファウンダーのStrubelさんが来て、コミュニティを使っていいもの、セキュリティ（安全なもの）を作ろう、そのベースが、今申し上げたとおり認証の基盤だったりするというのがこの図になります。

2020年には、全世界に250億台のインターネットにつながるデバイスが存在するだろうと言われる中で、一早く日本の中でこういった安心・安全なIoTが利活用できるプラットフォームを導入することで、地域の格差なく色々なところでビジネスが起きて、色々なイノベーションが起きるのではないかというのがこの絵の中身です。

次のページに行っていただきまして、その中で私どもがいくつかこの間、実証実験をさせていただいたのが、これからやろうとしているものがこちらになります六つの中身になります。

ヘルスケアですけれども、労働安全衛生法が昨年12月に一部改正になりまして、50人以上の会社の事業主にはメンタルヘルスが求められていますけれども、他方で、私どもは東芝と、こういったデバイスの機器認証と通信の暗号化、要は個人の健康情報をクラウドに上げるときには一応ネットワークを暗号化しなさいというガイドラインが出ておりますので、そういったものを組み込んで、私どもの社員にテレワークを旭川でさせました。そのときにどういう健康状況かというものをさらに森林浴もさせました。森林浴というのは色々な地域で今取り組まれておりますけれども、エビデンスがないと理解しています。私どもの場合は旭川医大の住友先生にこのデータの解析をお願いして、森林浴をしたときに

一体どういう生体情報になっているのか。いつ、どこを歩いたら、何時に歩いたらどうだったかというのを分析していただきました。その模様が８ページ目になりますけれども、８ページ目からはずっと我々がやって、９ページ目はどういう効果があった。10ページはそれを住友先生が学会に発表されたのです。日本産業ストレス学会というところに昨年12月に、私どものデータを使って発表されております。こちらは副交感神経にいい成分が森から吐き出されている。この10ページの図で行きますと、右上のグラフです。α-Pineneと書いてありますけれども、これが副交感神経にいい作用を働かせるということになります。そのとき歩いた我々の色々なデバイスから取ったデータが全て改善したというのが左の棒グラフになります。こういった実証実験をしてまいりました。

11ページ目になりますけれども、その間に機器以外からアンケート調査も社員にしております。睡眠の質はどうだったかとか疲労の蓄積はどうだったかというアンケート調査等々も、このデバイスから出されるデータを基に分析をした結果が11ページになります。

それを踏まえて12ページ目になりますけれども、12ページ目は、実際にその間、NEDOのクリーンデバイス社会実装推進事業というものを私どもが東芝と一緒に受託をいたしまして、心のばんそうこうというプロジェクトになります。こちらにつきましては、私どものほうで、旭川の森の環境を東京のオフィスに持ち込んだらどうなるんだという実証実験をしました。旭川のほうでは森から吐き出される先ほどのα-Pineneという物質をアロマオイルにして、ディフューザーでたいたらどうだろうというものをオフィスに持ち込んだのと、森の音をハイレゾ音楽で聞いて社員がどういうストレス具合になるかという変化を確認しました。そのときに取った私のデータが今表示されております。私は大泉に住んでおりますので、これを３週間やりましたけれども、大泉からオフィスが溜池にありますので、そのときのそちらにありますデバイスから出されたデータを住友先生にまとめていただいたのがこれで、私の心拍数とか睡眠がどうだったか、これが睡眠時間になるのですけれども、あとはストレス具合といったものがこういったデバイスから取れたという御報告が去年の３月の時点です。今年はさらに、オフィスの中でどういう状況だったかというのをビーコンを入れて、例えば、喫煙コーナーですとかベンディングマシンがあるコーナーに置いて、オフィスの中でどういうストレス具合かというのを今計測して、３月末にちょうど２期目が終わったところで、今月中にレポートアウトされます。

14ページ目につきましては、取っているデータの内容になります。

それを基に15ページ目ですけれども、今ある会社とこのモデルを実際に導入されたい、社員の方の平時のストレス具合を測りたいということで、今ウェアラブルを使って今のような実証実験をしようということでお話が進んでいるところです。

次に、17ページ目になります。Automotiveです。こちらは私どもが本当にその運転手がその時間にその場所で運転をしているのですかという認証をするデモがありますので、これは画像を御覧いただきます。

私どもは機器は認証するのですけれども、本人は認証しないのでどちらでもいいのです

が、生体認証がかかりますと、我々のほうが間違いないですとなってエンジンがかかって、エンジンがかかると顔認証が走って、１秒間に10回ぐらい認証のデータをクラウドに上げるというデモです。

これで何ができるかですけれども、本当にその人がその場所からそこまで行ったのだったら、保険に適用できるのではないですかというのと、このデータと車から吐き出されるCANのデータをビッグデータとして解析すると、その人が本当に安全に運転しているかどうかが分かりますので、そのデータを基に私どもから、例えば、保険会社にそういったデータをやることで、間違いなく眞柄は練馬から港区までこの時間、このルートを通って行きましたよという認証を我々が提供できるということによって、車の運転のビヘイビアによってダイナミック課金ができるというモデルにつながるのではなかろうかとやっています。

19ページ目は、さらにそれに運転手の生体情報を取ったらどうなるかという御説明になります。今これはまさに色々なバス会社とお話を進めているところでして、こちらはどういうことかと言うと、先般、軽井沢で夜行の長距離バスで悲惨な事故が起きましたけれども、仮に運転手の方の生体情報をリアルタイムで読んでいたら、何か異常を検知したときに最終的に止められるのではないかというところまで行けるのではないかということです。こちらについては、今お話をしている方々の中からは、バスは60歳で定年させているのと、２種免許の取得者が中々少なくて困っておられる。もし、こういったところで健康情報を客観的に取れるのであれば、定年を延ばせるのではないかという話も伺っています。

20ページ目ですけれども、こちらがハッキングのイベントでございまして、実は先ほどのものづくりに関わるのですが、テスラは自身でセキュリティのリソースを全部抱えてやろうと思っていないです。コミュニティを巻き込んでセキュリティのリサーチャーを巻き込んで、なおかつここに赤い部分がありますね。これはバウンティー・プログラムと言いまして、バグを発見したら最高１万ドル差し上げますというキャンペーンを常時やっています。こういうことでものづくりをどんどんコミュニティを巻き込んで作っていこうというのが、今の多分先端のやり方だと思います。それによってテスラは何をしているかと言うと、リサーチャーたちのプレゼンを聞いていますと、テスラのシステムは航空機並みのセキュリティを担保されていると言っています。これが多分今後のやり方だなということで書かせていただきました。右にあるGMのサイトを見ますと、あれはしてはいけない、これはしてはいけないということで、レガシーの車のメーカーとテスラの差がはっきりしています。ちなみにトヨタ、日産を探しましたけれども、一切こういうことはやっていません。

23ページ目に、インバウンドのほうもゼンリンとこれは２年ほど前に実施いたしました。韓国からフェリーで来られる方にWi-Fiを証明書で認証して、ただで使わせる代わりにあなたのプローブデータを見させてくださいということで、300人にチェックした結果のヒートマップになります。

これを使って次のページに行きます。24ページに今、民泊の話がありますけれども、海

外におられる方にどうやってキーを渡すかとか、アナログでやるのではなくて、例えば、電子証明書で我々はその人がどこから来た人か、ビザによって何日間滞在するかというのを電子証明書に書き込むことができますので、そのデータを使って全部済ませたらどうでしょうか。韓国の方だったら韓国の地図を出し、民泊するのだったらその鍵をITを使ってIT鍵で開けるということができるのではないかというのが、ここの内容になっています。

26ページはリアルタイムモニタリングになります。明日、スーパーラグビーが秩父宮で行われますけれども、私が今、ラグビー協会でボランティアを130名ほど毎試合動員して、ボランティアがちゃんとその場所にいるんですかというリアルタイムモニタリングの実証実験をさせていただいています。その状況は10秒間に１回ほどスマートフォンにアプリを入れていまして、それをクラウドに上げて位置を確認するという内容になっています。これが一つです。

29ページ目はドローンになります。昨年、首相官邸に色々落ちましたので、私どものほうで安全に法の中で自動航行させるための色々な取組をしております。その中で、今、農産物の育成栽培、これは旭川のほうで取り組んでおります。水田のデータです。プレシジョン・アグリカルチャーというのはアメリカにもあるのですけれども、水耕栽培のデータというのは、プレシジョン・アグリカルチャーはまだ世界にないので、我々は今、農協と組んでやろうとしているのが一つ。もう一つは、ソーラーパネルの保守点検です。これはサーマルセンサーを積んでやろうということであります。これが一つです。

もう一つ、32ページ目ですけれども、私どものほうで自助の訓練しているところの話をしていまして、時間もないものですから申し訳ありません。

34ページ目に、継続して正しい情報を出しましょう、それを共有しましょうというアプリを使って、今年の秋に代々木公園で１泊２日の滞在するキャンプをやります。そのときに持たせるアプリケーションがこれです。いつ、このルートで、どのような状況だったというのを地域にある防災マップの上にどんどんその情報を重ねることによって、有事の際にそれをシェアして有効利用していただこうというものです。

今日のお話の最終的な内容なのですけれども、こういったばらばらな取組があるのですけれども、私どもとしては、できればいつ、どこで、誰が、どのデバイスがという認証を新しい社会のプラットフォームにできないかなと。250億台の世界でIoTのデバイスがネットワークにつながる中で何が接続されているかが分からない。本当にその人に送金していいのか分からないという時代がまもなく参ります。そのためには、水やガスや水道のように、IoTに関する安心・安全なインフラができるのではないかという思いで取り組んでおりまして、それを今ばらばらにやっているのは、ある地域で全部できないでしょうかというのが今日のIoT Sim Cityと書いてある35ページのところになります。なぜかと言いますと、私どもは今年も旭川にこのデバイスを付けてテレワークをしに参ります。そのときに空いている時間に、例えば、ドライビングのデータを取ってください。取っていいです。そのデータを使って、例えば、今、UBERというものがありますけれども、地域に行きますと、

公共交通も中々不便です。空いている時間で運転の履歴がいい人について、我々の社員が運転したらどうですかと。有象無象のUBERの個人の運転手ではなくて、ちゃんと会社が身分を証明して、なおかつ運転の履歴が良かったら地域のおじいちゃん、おばあちゃんのための交通機関にお役立ちできますよということなんかも組み合わせで実証実験できるのではないかと思っているのです。そのようなことをさせていただきたいということが36ページから色々書かれております。

37ページを見ますと、今、我々が直接取り組んでいるヘルスケアとかオートモーティブとかインバウンドについて色々書かれていまして、これをさらに色々地域で我々が行くことによって、色々な用途ができるのではないかと思っています。例えば、オートモーティブと下に書いてありますけれども、今申し上げたとおり、例えば、私ども首都圏にいる社員がテレワークに行きます。空いている時間を使って地域の公共交通、ワンボックスカーぐらいだったら運転できますから、運転の履歴がいい人に対しては、首都圏から来て時間のある人に運転させたら、おじいちゃん、おばあちゃんたちのためになりませんかということが意味です。そのときには、お客さんを乗せなければならないので２種免許が要りますとか今はあると思うのですけれども、我々はそういうことではなくて、運転の履歴で客観的なデータがあるのだったら、例えばどうでしょうかというようなことがつらつらと書かれております。

最後の38ページ目ですけれども、それに対してステークヘルダーが誰かとか、色々書かれてございますけれども、最終的にはこういった、いつ、どこで、どのデバイス、あるいは誰がというセキュアな環境をこの国で作っていただいて、それに対してこれから来るべきテスラなどがどんどん入っていきますから、それは日本が一番安全に運転されている、使われているというインフラが出来たらいいのかなというところに向けての取組で、それを繰り返していくとある地域でまとめて実験させていただけないでしょうかというのが書かれてございます。

以上でございます。すみません、少し長くなりました。

○八田座長　どうもありがとうございました。

原さんから御質問ありますか。

○原委員　最後の御提案に関しては、国家戦略特区の枠組みの中で近未来技術実証特区という枠組みになりますので、そんなところも活用しながら、こういったことができていくといいのかなということを考えてお聞きしたのですけれども、特に今、動いている話で言うと、先ほどUBERの話もございましたが、自動車のライドシェアについては法案審議中でありますけれども、今度国家戦略特区で新しい制度の枠組みを作って、どこか特区の中で実証的なことをやってみるということになります。そのときに、今お話をいただいたような自動車の運転履歴を取って、この人は本当に危ない運転をやっているとかいうのが分かるようになるということができていくと、今の従来の伝統的な安全規制の枠組みから、もっとこういう実態による安全の管理ができるようになる。

○眞柄社長　エビデンスをベースにしたものです。
○原委員　ということに切替えていけるのかなと思うのですが、これは現時点で損保会社とのお話というのは。
○眞柄社長　まだしていないです。
○原委員　今の段階では先ほどの実証実験をやって、これから進めていこう。そのときに、例えば、乱暴な運転をしているとかいうのを取ろうとすると、どのあたりが引っかかるのかというのをもう少し教えていただけますか。
○眞柄社長　乱暴な運転をしようという判断を誰がしますか、誰が何のロジックを持ってしますかというのは、大体お話をしていると御指摘を受ける点です。
　私どもがあるバス会社とこれをお話したときに、２社とお話をしていますけれども、先ほどのバイタルセンサーを付けるお話を、１社からは、それは国が基準を出してもらわないとなかなか難しいなという御指摘を受けました。もう一社のほうは、そういう異常を検知するというより、まず、今どうなっているのかを知りたい。今は目視と問答によって、質問によって大丈夫かということを確認しているだけということでしたので、色々差があるのですけれども、いずれにしましても、それは先ほどこういったデータを御覧になって、私たちの専門外ですので、例えば、メンタルヘルスでしたら旭川の住友先生がこのデータを御覧になっていますが、そういう検知をされる大学なのか専門家の方にビッグデータを見ていただいて御判断をするという仕組みが必ず私は必要なのかなと思っていまして、そこはまだ我々は取り組んでいないです。
○原委員　まず、どういう運転をしているのかというデータを取るところの問題がまずあって、そこから先に、またどこまでやったら乱暴だと判断するんだという判断基準の問題を作っていくという、そういう実験をしないといけない。
○眞柄社長　そういうことになります。それでデータが取れるかどうかの問題がございまして、これは日本のメーカーの場合は全てブラックボックスですので、これは車のメーカーの今の私の印象からすると、差別化要因になっていますので、なかなかこれを取得するというのは困難です。このデモでは擬似的にiPhoneのXYZを拾えるデータがポジションを取れますので、これをステアリングに付けて位置を遷移したのです。本当はそれが車の車体から出ているのですけれども、ここはなかなか難しいところがあるかなと思っています。
　ですので、データを本当に取得するためのルールと言いますか、我々は取りようがないのが実態で、取ったところの後で先ほど分析をされる方が出てこないと、何かを検知して自動的に止めるというところまでは行かないかなと思います。
○八田座長　37ページに色々な関連法が書いてあるのですけれども、とりあえずこの規制が一番邪魔だというものの最右翼はどれですか。
○眞柄社長　例えばですけれども、ドローンのところに書かれているSIMを搭載して常時通信ができることというのが今後ドローンに限らず出てくると思うのです。これは今はSIMについては地上で使いなさいという決まりが確かあったと思います。空中で使えないので

す。ですから、これがありますとより広範囲に我々のほうは色々なものを通信しながら、認証しながらサービスが提供できるという社会になると思います。
○八田座長　これは随分前から要望があったものですね。
○藤原次長　そうですね。ドローンの事業者が既に産業競争力会議などでも発言して、総務大臣もかなり前向きな発言をしているのですけれども、ただ、その後の進捗が今一つまだ分からないところがございます。
○八田座長　他には。
○眞柄社長　あと、先ほどの、おそらく今後、首都圏の企業、私なんかはIT企業をやらせていただいていまして、100人規模の会社ですけれども、東京に実はないのです。そのとき、先ほど申し上げたとおり、ITに関連して色々貢献できることもあると思っていまして、その中では色々な免許制、例えば、先ほどのUBERのようなところというのは公共のものに貢献したいという流れがございますので、そこについては、例えば、先ほどのUBERとか２種免許のところというのは、何らか先ほどのエビデンスベースで色々動かしていただくような社会になればいいかなという思いはございます。
○八田座長　そうすると、かなり他のことはあれですか。事業としては新しくやろうと思っているけれども、特に規制が障害になるということはない。
○眞柄社長　規制が直接あるというのは、いくつか例えば、ドローンに関しても今あったと思いますけれども、我々が考えているのは既に色々上がっているようなのです。それよりも今みたいに組み合わせたときに何が起こるかというところに対しては、まだ逆に何もないのかなという気もしておりまして、これは逆に言うと、我々の実証実験をまとめてやるところにおいて、色々分かることはあるかなと思います。例えば、勉強不足で申し訳ないのですけれども、民泊のときにどのように本人を確認して、どういう形で民泊のときに鍵を開けていて、どのような形で返却させるのかとか、私どもでまだ理解していない部分がありますので、もし、そういうところにルールがあるのでしたら、全部デジタルでやってもいいのではないでしょうかとか、例えば、今ドローンで物流を考えられていると思いますけれども、人に物を渡すときにどうやって受渡しの認証をするのかとか、そこはルールとかあるのだと思うのですけれども、我々からしてみたら全部デジタルで認証できますので、いつ、どこで、誰が、誰に、何を渡したというのは認証要求ができますから、例えば、そういうところというのは勉強不足で大変申し訳ないのですけれども、あるのかなと思います。
○原委員　多分これをやろうとしたときに、すぐに規制に引っかかるという問題よりは、先ほどの自動車の安全規制の問題であったり、むしろこれからの規制体系を作っていくことに向けての実験という面が強いのかなと思って伺っているのですけれども、先ほどの自動車の履歴情報と言いますか、運転状況のデータを取得するということを仮にやろうとすると、どことどこと話が付けばいいのですか。
○眞柄社長　これは多分各メーカーの固有の資産になっていると理解していまして、テス

ラの先ほどのビデオを見ても、そこはブラックボックスなのです。絶対に触らせていないところなのです。それを開示すると何が起きるかと言うと、外から車を急ブレーキで止めることもできるので、なので、一つあるとすると、例えばですけれども、損保会社とお話を十分していただいて、どういうデータがあったらその人が安全に運転できるかという基準があると、そこは出してもらえると思うのです。そのデータはこの口からちゃんと出しますよというそういうモデルを作っていただければいいのかなと思います。ソフトウェア業界ではよくある話です。全部出さないけれども、ここの切り口からこのデータの形で出すよということはよくある話ですので、それは自動車メーカーと損保会社が御理解いただいていくと、より安全なのは間違いないと思いますし、これを逆にカーシェアの話にしても、海外から来られる方にしても、そういった履歴を取れば安全に車を貸すことのできる社会になりますので、まずは自動車メーカーと損害保険の会社のお話になるのかなという気がします。

○板東室長　加えますと、ビヘイビアから運転の仕方、アクセルの踏み方、ブレーキの踏み方で個人を特定できるというのは、多くの自動車会社が御指摘されていることでございます。つまり、ビヘイビアから個人を特定することができる。したがいまして、そこの部分が個人情報保護とどう絡まってくるのか。実はここは非常にあやふやでグレーなところであるということが言えると思います。

ただ、このビヘイビアをきちんと分析することで、全く新しい交通体系が生まれるかもしれない。ただ、実はそこのところがみんなよく分からなくて、正直言って、オープンデータとして活用するというところにまでは行けていないというのが現状でございます。

○八田座長　そうすると、とにかく非常に大きな可能性がある。そして、ここの個人認証ということがそこの鍵である。ただし、この規制をピンダウンするのはなかなか難しくて、まずは実験してからそれが見つかっていけばいい。そういう感じなのですね。そうすると、実証自体は別に特区を使わなくてもできるということになりますか。

○原委員　多分できている部分が相当程度あって、ある程度、その部分部分は進んでいるということだと思っているのですけれども、それこそ先ほどのような自動車の話であれば、損保会社まで巻き込んだような新しい仕掛けを作っていく上で、ある程度国もコミットしたような実験というものができると、よりやりやすいかもしれませんねということではないかと思うのです。

それこそIoTの話というのは、成長戦略でも第４次産業革命とか華々しく言っているのですが、なかなか具体的なところが進んでいないので、もし、特区の中でこういったことを一歩進める可能性があるのだったら、近未来技術実証特区が１年ぐらいという話もあるので、どこかでやれるといいのではないか。

○八田座長　全くです。私も是非どこかでやればいいと思うのだけれども、結局規制のところは、普通はネタがあってから特区に指定するわけなので、規制改革ネタ発見地区というのもなかなか難しいかなと。

○原委員　そういうときは既存の特区でどこかでやったらいいと思うのです。仙北市だったら既にドローンとかやられているわけですので、そういったところで、その延長上でやってみるとか。
○八田座長　なるほど。事業として最初にやってみる。
○原委員　そういうことを１回ここでお話を伺って、どこか御関心のある特区の自治体が見つかったりするとやれるのではないかということです。
○八田座長　分かりました。
○眞柄社長　最後に１点だけ、私どものほうから今日急遽そのハンズアウトだけお渡ししておりますけれども、私どもの技術自体が日本で特有で、当社特有の技術ではないということです。電子認証そのものがグローバルで標準化されているものを使ってやっていますというのが一つです。そのおかげで私どもはインテルと２年ほど前にリリースさせていただいたのは、インテルのCPUの中に電子証明書を入れる専門のエリアがあるのです。それを開示されたのは国内では私どもだけということで、そういう信頼関係もあるという意味で一つ資料を配付させていただきました。
○板東室長　それから、本日お配りしました資料の24ページだけは、民泊のところのキーでございますけれども、ここだけは大変恐縮ですが、非公表ということで。
○眞柄社長　あと20ページが著作物ですけれども、勝手に切り張りをしておりますので、20ページもコンフィデンシャルと入れさせていただきますけれども、こちらの公表は控えていただければと思います。知的所有権が私にはないものですから。
○八田座長　非常に面白い話をどうもありがとうございました。