Verifiable Credential（VC/VDC)の活用におけるガバナンスに関する有識者会議（第１回） 議事録

令和7年3月 10 日（月）15:30-18:00

出席者（敬称略）

（委員）

- 板倉景子　（OktaJapan 株式会社 RegionalCSO）
- 板倉陽一郎　（ひかり総合法律事務所パートナー弁護士）
- 笠井玲子　（株式会社ローソンインキュベーションカンパニーデジタルソリューション推進部 シニアマネジャー）
- 佐古和恵　（早稲田大学理工学術院教授）
- 瀧俊雄　（株式会社マネーフォワード執行役員グループ CoPAFintech 研究所長）
- 中村素典　（京都大学情報環境機構 IT 基盤センター長・教授）
- 中村龍矢　（株式会社 LayerX 部門執行役員 AI・LLM 事業部長）
- 富士榮尚寛　（一般社団法人 OpenID ファウンデーションジャパン代表理事）

（ゲストスピーカー）

- 舟橋克実　（DID/VC 共創コンソーシアム）
- 今井康之　（DID/VC 共創コンソーシアム）
- 宍倉孝亮　（DID/VC 共創コンソーシアム）
- 橘博之　（マイナウォレット株式会社）

（デジタル庁：事務局）

- 楠正憲　（デジタル社会共通機能グループ長）

その他関係者

（オブザーバー）

- DID/VC 共創コンソーシアム
- 一般社団法人 OpenID ファウンデーションジャパン
- DIF Japan
- 金融庁
- 経済産業省

（デジタル庁石井）

定刻になりましたので、ただいまより、「Verifiable Credential（VC/VDC)の活用におけるガバナンスに関する有識者会議（第１回）」を開始いたします。

本日はお忙しいところ、お時間をいただき誠にありがとうございます。私は事務局を務めますデジタル庁の石井です。どうぞよろしくお願いいたします。早速ではございますが、本会議の開催にあたり、事務局を代表してデジタル庁デジタル社会共通機能グループ長、楠よりご挨拶申し上げます。

（デジタル庁楠）

ただいまご紹介にあずかりました楠でございます。

委員の皆様におかれましては、お忙しい中、本会議にお集まりいただきまして、誠にありがとうございます。VC/VDC の活用におけるガバナンスに関する有識者会議第１回の開催にあたりまして、事務局を代表して、一言ご挨拶を申し上げます。

本有識者会議はデジタル署名による真正性・改ざん防止等の機能を実現する汎用的で機械可読の

データ形式・データ流通形態として注目されている Verifiable Credential を中心として、安心・安全に利用されることを目指して、その留意点を整理するために開催するというものでございます。

VC の概念そのものは数年前から具体的な形を取り始めて、関連企業や団体の設立をはじめとして、徐々に注目を集めて参ったところでございます。その後、World Wide Web Consortium における標準化の取組等を経て、現在では民間セクターを中心として、VC の発行及び利活用に関する議論が活発化していると認識しております。近年では、例えば新型コロナウイルス感染症対策の一環として導入致しましたワクチン接種証明書も VC の一形態として、実用化された事例の一つとして挙げられるのではないかと思います。これはデジタル庁が立ち上がる前でしたけれども、私自身も技術検討に入っている中で、当時トラストフレームワークを WHO で決めようとしてなかなかうまくいかず、見切り発車の中で、いわゆるパスポートのトラストフレームワークに乗ったり、一部 WebPKI でも検証できるようにしたり、というような形で、まだかなり試行的な位置づけ、意味合いが多かった。また一方でフォーマットに関しても取り決めることは実に多いと痛感した出来事の一つでございます。

また一方で、VC を取り巻く環境は、長年の議論と経験を積み重ねてきた PKI、公開鍵基盤等と比べますと、まだまだ発展途上の段階にあると考えておりまして、この安心・安全な利用を実現していこうとすると、さらなる議論の蓄積が必要と認識しているところでございます。

本会議におきましては、VC の健全な発展と普及・利用を促進していく上で、現行の制度や仕組みを踏まえた対応の検討、また将来的な課題の洗い出しといった多岐にわたる議論を行う予定でございます。委員の皆様からはぜひ忌憚のないご意見をいただいて、活発な議論をできればと考えておりますので、本日は何卒どうぞよろしくお願いいたします。

（デジタル庁石井）

ありがとうございました。それでは本日ご出席いただいている委員の皆様より簡単な自己紹介を頂戴したいと思います。設置要綱に記載している五十音順にご指名させていただきますので、呼ばれた方はマイクをオンにしていただき、お名前とご所属について、おひとり 30 秒程度で自己紹介をお願いいたします。それでは初めに、板倉景子委員、よろしくお願いいたします。

（板倉景子委員）

板倉景子と申します。

約 20 年、ID・セキュリティ業界で働かせてもらっており、現在は Okta というアメリカに本社を置く IDaaS のソフトウェアサービスを提供する会社で、日本周辺リージョンの CSO として働いております。この後は IHV モデルについても触れられるかと思いますが、Verifier となる事業会社さんなどが IDaaS を利用してクレデンシャルを検証していくことになるかと思いますので、どういう観点で、どうやって検証していくべきなのかというところを中心に、意見を出させていただくと考えております。よろしくお願いします。

（デジタル庁石井）

ありがとうございました。続きまして、板倉陽一郎委員、お願いいたします。

（板倉陽一郎委員）

弁護士の板倉です。

データ保護と、個人情報について企業等からご相談を受けるという仕事を基本的にはやっておりま

す。その他、消費者関係も日弁連（日本弁護士連合会）では消費者問題対策委員会という活動も行っております。この分野はデータなのか消費者保護なのか難しいところですが、法律の関係で、主にコメントしていくと思います。よろしくお願いします。

（デジタル庁石井）
ありがとうございました。続きまして、笠井玲子委員、お願いいたします。

（笠井委員）
株式会社ローソンの笠井と申します。
私はローソンの社内の中で、コンビニも関わる規制改革と、事業開発の担当をしております。主に本件に関わりましては、コンビニにおけるセルフレジ等の非対面でのお酒・たばこの年齢確認において、本人の確認及び年齢の確認について議論を継続して行っているところです。一方、経済産業省に2年間出向した経験もあり、データを共有する事業者の認定制度などに携わったことがございます。この辺りも含めまして、当議論のガバナンス等に関して、ご意見を出させていただければと思います。よろしくお願いいたします。

（デジタル庁石井）
ありがとうございました。続きまして、佐古和恵委員、よろしくお願いいたします。

（佐古委員）
早稲田大学理工学術院の佐古と申します。
私は長年、NEC で暗号の研究をしておりまして、現在は暗号プロトコル技術をベースに、情報セキュリティ、プライバシー保護、そして公平性保証の研究をしております。Verifiable Credential はデータに単に署名がつくだけではなく、どういう内容に署名しているのかというコンテキストをプラスして署名技術が使われていくのではないかと思って、とても楽しみにしています。どうぞよろしくお願い致します。

（デジタル庁石井）
ありがとうございました。続きまして、瀧俊雄委員、よろしくお願いいたします。

（瀧委員）
マネーフォワードの瀧でございます。
この度はどうぞよろしくお願い申し上げます。当社は、よく銀行 API を大量に色々なところと繋いでいる、ある意味、データのトークンのユーザーのような立場もあれば、自ら確定申告や様々な手続を行う、SaaS の、ある意味発射台的な場所にもいるという。私たちが持っている情報をベースに何か Issuer として機能するケースもあれば、使わせていただくというケースも色々あると思っています。そういう実装向きのところで貢献できればと思っております。どうぞよろしくお願いいたします。

（デジタル庁石井）
ありがとうございました。続きまして、中村素典委員、よろしくお願い致します。

（中村素典委員）

京都大学の中村でございます。

私は前職の国立情報学研究所の時から学術の認証について取り組んでおりまして、ID フェデレーションですとか、その普及活動で、さらには学生証の VC 活動とか、そういった方向を現在色々と検討しております。そういった側面から議論できればと思っております。よろしくお願い致します。

（デジタル庁石井）

ありがとうございました。続きまして、中村龍矢委員、よろしくお願いいたします。

（中村龍矢委員）

LayerX の中村と申します。

現在では LayerX でエンタープライズ向けの AI 事業の責任者をしております。私はもともとブロックチェーン、特にイーサリアムというコミュニティのセキュリティ面のコントリビューターをやっていたり、その後、秘密計算ですとか、差分プライバシーのようなプライバシーテックと言われている領域で事業化に取り組んでいました。現在もプライバシーテック協会という団体の理事も務めております。今日はそういった観点から、技術の社会実装的な観点で貢献したいと思っております。よろしくお願いします。

（デジタル庁石井）

ありがとうございました。続きまして、富士榮尚寛委員、よろしくお願いいたします。

（富士榮委員）

OpenID ファウンデーションジャパンの富士榮でございます。

デジタル・アイデンティティの世界、20 年少しやらせていただいております。Verifiable Credential についても 6,7 年ウォッチはしているかなと思っております。今回資料提供もさせていただいておりますけれども、U.S.とか EU で、テクノロジーのみならず、ガバナンスを含め、もしくはその運用含め、どういうふうに検討議論がされているかという話をずっと追いかけてきておりますので、その辺の知見から貢献できることがあるかと思っております。よろしくお願いいたします。

（デジタル庁石井）

続きまして、本会議の進め方についてご説明いたします。

本日の資料はデジタル庁ウェブサイトにも掲載しておりますので必要に応じてお手元でご確認ください。本会議の趣旨・目的についてご説明させていただきます。本会議は近年、デジタル署名による真正性・改ざん防止などの機能を実現することができる機械可読かつ汎用的なデータ形式・データ流通形態として注目されている Verifiable Credential に関し、今後の適切な利活用を促進するため、現行の法令・制度との関連性を踏まえ、その利用プロセスに関わる留意点を整理するとともに、今後の活用に向けたユースケースに関する議論を行うことを目的といたします。

検討内容につきましては、大きく二点ございます。一点目は、VC の利用プロセスに係る留意点の整理として、VC の発行者が満たすべき要件及び責任について、また VC の適切な利活用に向けたその他留意点についてご議論いただきます。二点目は、VC の利活用が見込まれるユースケース等についてご議論いただきます。後続の設置要項の記載内容につきましては、先ほど委員の皆様からの自己紹介もありましたので、時間の関係上割愛とさせていただきます。

議事次第について説明させていただきます。まず初めに、委員の互選より本会議の座長を決定させ

ていただきます。続きまして議事ですが、まず本日は DID/VC 共創コンソーシアム様とマイナウォレット株式会社様を本会議にお招きしておりますので、各社様のお取組内容についてご紹介いただきます。その後、事務局より VC に関する各種制度等についてご説明させていただきまして、事務局資料に関するご議論をしていただきます。そして最後に事務局より、閉会・諸連絡をさせていただきます。また本日、富士榮委員より参考資料として、デジタルクレデンシャル利用用途に応じた管理要件に関する資料をご提出いただいておりますので、必要に応じてデジタル庁ウェブサイトにてダウンロードいただきご参照いただければと思います。

本会議の進め方について、ご質問・ご意見がございましたらご発言ください。

＜質問・意見なし＞

それでは要綱に従いまして、委員の互選により本会議の座長を決定させていただきたいと思います。事務局といたしましては、中村素典委員をご推薦したいと考えておりますが、いかがでしょうか。ご異議がある方は Teams 機能の挙手ボタンを押下ください。

＜異議なし＞

ご異議ございませんでしたので、本会議の座長を中村素典委員にお願いすることとし、これ以降の議事進行を中村座長にお願いしたいと思います。それでは中村座長、よろしくお願いいたします。

（中村素典座長）

それではただいま座長にご推薦いただきました中村から、これから座長として進行させていただきたいと思いますので、よろしくお願いいたします。

それでは議事に早速移って参りたいと思います。本日は VC の利活用に取り組んでいる事業者・団体として DID/VC 共創コンソーシアム様とマイナウォレット株式会社様をゲストとしてお招きしております。まずはそれぞれのお取組内容についてご説明いただきます。

各社様十分間程度で順番にプレゼンテーションをいただきまして、最後にまとめて皆様からのご質問を受け付けたいと思いますので、よろしくお願い致します。それでは最初に DID/VC 共創コンソーシアムの舟橋様、今井様、宍倉様、よろしくお願いいたします。

（DID/VC 共創コンソーシアム今井）

DID/VC 共創コンソーシアムの、ご紹介に預かりました、こちらの立ち上げ事務局を担っております三菱UFJ信託銀行の今井と申します。ほか、船橋、宍倉も出席させていただいております。本日はどうぞよろしくお願いいたします。事務局様、資料の投影をお願いできますでしょうか。

（デジタル庁石井）

こちらで資料投影させていただきます。

（DID/VC 共創コンソーシアム今井）

ありがとうございます。それでは4ページまでお進みください。前置きとして、我々のコンソーシアムではビジネス共創と相互運用性の実現を目指しており活動しております。まず、当社が DID/VC に着目し

たきっかけは、例えば当社ですと金融機関などは様々な基幹システムなどを使用しておりますが、ベンダーロックインに陥るケースがございます。ベンダーロックインは金融に限らず、その他の事業会社でも同様だと考えております。その中、Verifiable Credential につきましては、デジタル署名による真正性・改ざん防止などによってデジタルデータの流通形態の相互運用を実現させるということで、ベンダーロックインから抜け出すこともできる可能性のある技術だと捉えております。我々はユースケースを起点に、ビジネスルールや法規制を検討しております。続きまして、アーキテクチャの観点では、我々は車輪の再発明はいたしません。W3C であったり、Trusted Web など、標準化団体や学術機関が定める規則をもとに、ユースケースに応じてどんな規則を選定すると良いかを議論しております。

5ページにお進みください。こちらのスライドが、コンソーシアムが目指す姿で VC が相互運用できるイメージを指し示したものになります。これまでの実証であったり、本番基盤、開発されているものがあるものの、VC の相互運用性が実用できている事例はまだ国内ではあまり見られていない認識であります。我々のコンソーシアムでは右側 ToBe の姿を実現したイメージでして、1つ目は VC を他の基盤に持っていっても読んでもらうことができる相互運用性の実現、2つ目はガバナンスの整備、3つ目は、例えば Status List などは一定の場所を設けて見に行きやすい形を作る効率的な共有のあり方を目指しております。

6ページにお進みください。我々のコンソーシアムは、実現したいユースケースを起点に、ビジネス共創を検討する分科会とそのユースケースの実装上のシステムや法律などのルールを整備、検討する分科会の2つが二輪となって運営しております。

8ページにお進みください。こちらは今現在金融庁様やデジタル庁様などと取組中の FinTech 実証実験のユースケースの例になります。例えば、三菱が本人確認した結果を二次活用できる形にして Holder へ発行し、Verifier となる地銀証券の口座開設、保険やローンの申込みといった特定取引の本人確認に再活用できる仕組みを実証中です。実証にあたって、Verifier は差し出された VC を見て、結果だけを鵜呑みすることがないように Issuer 側のガバナンス体制を共有するような仕組みを構築しています。そのガバナンスの観点につきましては、実証にあたり、警察庁様からアドバイスいただいたものです。念のため補足しますと KYC 内容を共通化するようなことはいたしません。各社の KYC は金融庁ガイドラインに従いリスクベースアプローチで行われるものと認識しております。詳細は後ほどのスライドでご説明します。

9ページにお進みください。こちらは電子レシートのユースケースです。例えば、セルフメディケーション税制では、医薬品などを購入した際、領収書を自宅で5年保管する必要がございます。こまごまとしたレシートを現物・紙で保管することは、引っ越しなどの際に紛失する恐れがあったり不自由な点があるため、デジタル化であったり、VC 化による保管の簡易化というのが期待されるかと考えております。一方で電子レシートについては課題も判明しておりまして、デジタルゆえに小売事業者さんが電子レシートを吐き出すと受け取る個人との紐付けができてしまうことから、個人情報としての管理負担が生まれてしまうことであったり、小売事業者にとっては購買データはもともと自社の資産で、マーケティングであったり商品開発に活かすものという考え方が当然にありますので、法令整理やステークホルダー調整というのは、まだまだこれからになっております。

10 ページは、生体 VC を活用したチケットの不正転売防止、11 ページは中小企業に対する法人カードの発行にあたって信用情報を共有することができないか、というようなものを検討しているユースケースですけれども、時間の都合上、いったん割愛させていただきます。12 ページ目以降のところ、宍倉よりご説明させていただきます。

（DID/VC 共創コンソーシアム宍倉）

私から現在 FinTech 実証実験ハブでやっていることについてご説明させていただきます。13 ページをおめくりください。こちら OIDF の KYC ガイドラインからの抜粋となりますが、本人確認分科会では、一度実施した本人確認結果を2次活用できるようにしてユーザーの手間を削減するということを目指しております。

次のページおめくりください。足元実施しております実証実験のスキームですけれども、Issuer の実在性を担保するために、GLEIF が発行する ISO17442 に基づく 20 文字の英数字で構成される識別子、LEI を使うこととしております。LEI は FATF のレコメンデーションの中でも推奨識別子として言及があるものでございまして、実を言うと、本邦の金融機関に馴染みがある国際識別子となっております。今回の実証スキームでは、GLEIF が、QVI という Issuer を審査する機関を認定して、その QVI が今回の実証における Issuer の実在性などを定期的に確認して LE vLEI 発行し、問題があればその LE vLEI を失効するといった役割を持たせております。Issuer は LE vLEI を Trusted List 運営者、信頼できる Issuer 一覧の運営者に対して、自身に関する Issuer の属性を登録していくということになっています。ここまでが実証の前準備という形になります。Trusted List に登録された Issuer、今回のユースケースでは銀行とさせていただいておりますが、利用者に対して自行と取引が現在進行形で継続されていて、継続的な顧客管理でも問題がないというようなことを証明する取引時確認 VC というものを発行します。そのほかに公的個人認証法第十七条第一項第五号で定められる カ方式事業者、これは後ほど説明をさせていただきますけれども、公的個人認証等を活用して本人確認を実施した結果を、署名検証結果 VC として利用者の Wallet に発行する。利用者はこの2枚の VC を Verifier となる特定事業者に VP して金融機関のカスタマーデューデリジェンス情報と JPKI による本人確認結果、この2つを提示してみなすと。これを犯収法上有効な本人確認とできないかということを検証しているのが足元の取組となっております。

次のページおめくりください。カ方式というものは、あまり耳馴染みがないかと思いますので、補足説明をさせていただきます。犯収法施行規則第六条がありまして、ここには公的個人認証を用いたワ方式と呼ばれるもののほかに、民間の事業者が発行する電子証明書を活用した本人確認方法として、このカ方式というものが規定されております。

その流れとしましては、左側の図を参照ください。まず①利用者キーペアを用意する。次に②、③でカ方式事業者が利用者に対して JPKI などで本人確認を実施し、その際に利用者から署名の検証に用いる公開鍵の連携を受ける。④でカ方式事業者が利用者の公開鍵と利用者自身を紐付けた電子証明書を発行する。次に、特定事業者に対して⑤、⑥で申込書などの書類を徴求して、⑦で必要事項を入力した申込書に①で生成した秘密鍵で署名を行う。⑧で署名済の申込書と④で受け取った電子証明書を特定事業者に送付する。最後に⑨で特定事業者は受領した申込書の電子署名のの検証と電子証明書の有効性確認をカ方式事業者に対して行う。ワ方式、公的個人認証に似た流れですけれども、こういった流れで進める、実は、既存法の中で本人確認方法がございます。これに VC を当て込めないかと考えたものが右側となります。Wallet でキーペアを生成してカ方式事業者による本人確認までの流れは同じで、④で発行される電子証明書を署名検証結果 VC と置き換えます。次に申込書について、必要事項を入力した情報をもとに Wallet 内で Holder 自身が Issuer となって、申込書を VC 化した特定取引情報 VC というものを自己発行します。ここに金融機関の取引時確認 VC を任意で組み合わせて、この3枚を VP 化して特定事業者に対して提示、特定事業者はVP検証を行うことで、カ方式に沿った本人確認方式を現行法でもできないかというようなことを、今実証ハブの中で見ているというところです。

17 ページおめくりください。足元進めております実証実験ハブの中で、今一番問題となっているものが、技術的な要素というよりも、ガバナンスの問題、特に適格性に関するものとなっております。例えば

金融機関が他の金融機関と連携する際には、マネロンガイドラインに基づいて連携先のリスク管理体制を評価する必要がございます。一方で Issuer、Verifier が 1 対 1 の関係で評価したものをさらに×n で広げていこうとすると、Verifier 側にかなりの負担がかかりまして、様々な金融機関の KYC を参照するということが逆に Verifier にとっての負担になる可能性が出てまいります。

今回、コンソーシアムでは Trusted List への掲載プロセスの中で、Issuer の適格性を評価して、List に掲載さえしていれば Verifier はそれを信じて取引できるという方向でできないかと検討しておりましたが、その審査の能力であったりとか、審査をする権限があるというものはどこかというと、金融庁ぐらいしかないのではないかといったような意見も各社のコンプライアンス部署から出ておりまして、難航しているというところです。

次に Wallet Provider の適格性ですけれども、Issuer の適格性はしっかり管理したとしても、Wallet がセキュリティホールになってしまった場合は、なりすましによる口座開設みたいなことが起こり得るため、ここについても一定の共通のセキュリティ水準が必要だろうというような認識です。一方で本コンソーシアムの中で評価するとしても、同じく競合他社が集まっている座組ですので、ある程度独立した第三者的な組織が、審査組織としては望ましいかと思われます。

最後ですけれども、Verifier の適格性ですが、Issuer が VP できる Verifier を管理すべきという意見があることを承知しております。一方でこれをやると、VC をビジネスと捉えた時に、あまりファットなビジネスモデルにはなり得ないので、この Verifier 管理負担というものがビジネス化を妨げる要因となり得るかと思われます。また提示先を本格的にコントロールするのであれば、Wallet 側での対応が必要となりますので、Issuer が提示先を決めて Wallet Provider が対応するという複雑性も考慮が必要かなと思います。例えば、大学が卒業証明書 VC を出して Holder が就職活動に利用したいと言った時に、その提示先範囲というものを大学がコントロールすべきなのかというような問題にもつながるかと思います。PDF ですと Holder の自己責任の中で自由に情報提示ができる中で、VC になった際に、どこまで Holder 保護が必要なのかというところは、ぜひご検討いただけますと幸いです。コンソーシアムでは今回の実証で W3C の Bitstring Status List を使っておりますが、指定 Verifier 以外のアクセスを遮断するようなアクセス制限みたいな措置をしますと、技術として国際標準から外れてしまうというような課題も見つかっているところです。

（DID/VC 共創コンソーシアム 今井）

DID/VC 共創コンソーシアムからのご説明は、一旦以上となります。

（デジタル庁石井）

ありがとうございました。マイナウォレット株式会社の橘様よろしくお願いいたします。

（マイナウォレット株式会社橘）

よろしくお願いします。マイナウォレット株式会社の橘と申します。

それでは少し画面共有をさせてください。

改めまして私、マイナウォレット株式会社代表取締役の橘博之です。本日は事業のご紹介、DID/VC を活用した今後の取組や課題について皆様にご共有させてください。どうぞよろしくお願いいたします。

弊社は、マイナンバーカードを活用したデジタルウォレットを開発しています。約 1 億人に普及した日本が誇るデジタル基盤を使って、ブロックチェーン、DID/VC などの技術を世界で一番簡単に使える社会にし、デジタル技術によってより豊かな社会の実現、というのを目指しております。

マイナウォレットとはアカウントアブストラクションの仕組みを活用し、マイナンバーカードの中にある秘密鍵を用いて利用可能なセルフカストディアルウォレットです。カードの紛失、更新、盗難の場合でも、公的個人認証サービスを利用し、ウォレットのリカバリーに対応できます。Web3.0 ウォレットにおける永遠の課題、秘密鍵の管理から解放されたウォレットです。また、一人につき一つのウォレットしか作成できないことから、いわゆるシビル耐性を持ち、実在する人間が所有するウォレットであることを証明することが可能です。また、今後、デジタルアイデンティティウォレットの機能も実装予定でして、複数のフォーマットの VC の受取であったり、プレゼンテーションに対応予定です。

こちらはマイナウォレットの実際の利用シーンです。四桁の暗証番号を入力し、利用することができます。裏側では公的個人認証サービスを使って当人認証を行っています。こちらが確認できれば、ユーザーはウォレットの利用が開始できるような流れになっております。

ブロックチェーン上へのトランザクションを送信する場合もとても簡単です。今回は ENS でジョンさんという方にトークンを送るサンプルですけれども、実際にトークンの量を入力して送信することができます。次にトランザクションの内容というのを事前に確認します。マイナウォレットはアカウントアブストラクションの技術を活用しているので、ユーザーのガス代の負担を行っています。そのため、ユーザーはガス代に必要な ETH、つまりネイティブトークンを交換所等で購入することなく、すぐにトークンの送受信が可能です。内容の確認ができたら、先ほどと同様の手順で四桁の暗証番号を入力してカードをかざして署名を行います。署名はスマートコントラクト上で検証されて、その検証が通れば自治体のトランザクションから実行されます。

マイナペイはマイナンバーカードのかざし利用を活用した決済ソリューションです。カードをタッチするという誰もが慣れ親しんだ UX で、NFT、トークンの受取や所有確認、少額のトークンの送信が可能になります。カードだけで利用でき、スマートフォンを持っていないユーザーでも利用が可能になっております。

こちらの動画は USDC というステーブルコインを持っているユーザーがマイナペイで決済を行う動画です。交通系 IC と同様の UX でかざし利用を行ってトークンでの支払いが実現できております。

こちらは去年の 11 月に新潟県長岡市の山古志地域で行った実証実験の動画になります。

〈動画音声開始〉

マイナウォレット。本実証実験では、新潟県長岡市の山古志地域にてマイナンバーカードをデジタル資産ウォレットとして活用するサービス「マイナウォレット」によるタッチ決済のフィージビリティ検証を行いました。実証実験に用いるデジタル通貨には、ブロックチェーン上で発行・流通しているアメリカドルと連動したステーブルコイン「USDC」を使用しました。実際に小学生から 80 歳代まで幅広い年齢層の方にステーブルコインのチャージや決済を体験していただきました。

〈動画音声終了〉

今回、この山古志村デジタル村民の皆様の協力のもと、幅広い年齢の方に参加いただき、実際にステーブルコインのかざし利用について、本当に簡単に利用できることが確認できました。結果としてたくさんの反響をいただきました。引き続きこういうユースケースの創出のため、実証を進めてまいります。

今後弊社は、誰もが安心して使うことができるウォレットとして、Web3.0 ウォレットの機能の提供を開始します。その際、より安心安全な取引を実現するために、DID/VC を活用していきたいと思っております。その後、金融機関と連携を行い、並行して国や自治体と課題解決に寄与するサービスの提供を行い、ブロックチェーン技術の社会需要に向け、先行事例を率先して創出していきたいと考えております。

次に、我々が考える DID/VC のユースケースや検討している実証実験の内容になります。1 つ目はかざし利用での住民割のユースケースです。福岡市様と特区制度を活用した実証を検討しており、かざし利用で少額のステーブルコインでの支払いを行う予定です。この際に福岡市民の方に住民割引を行うことを考えています。もし住民割引を行う場合は、住民証明の手段が必要となるので、公的個人認証サービスや DID/VC の活用を検討しています。VC を発行する場合、Issuer の適格性をどのように担保するべきかというのは一つの論点として残っていますが、今回は実証ですので、VC の有効期限を短くできるという点も考慮しつつ、検討を進めてまいります。

次にウォレットと金融機関等との口座連携になります。こちらに関しても、さまざまな連携パターンが考えられ、内容や手法は現在検討中です。本人確認のコストを減らす利便性、そして安全性のバランスを考えた仕様を検討していきたいと考えております。

3 つ目は、DeFi へのアクセスの際に公的個人認証サービスや DID/VC を活用するものです。先日開催された BGIN Block#12 でもアカウンタブルウォレットという同様の取組が議論されておりました。DeFi は課題が多く、我々は DeFi を積極的に推進する立場ではありませんが、一方で Web3.0 のユースケースとしては非常に大きいものとなっており、ウォレット事業者としてより安心安全に DeFi を使えるようにしていきたいと考えています。具体的には本人確認であったり、資格情報の確認ができたユーザーだけが利用できるような流動性プールを作成し、いわゆる KYC 済のユーザーだけが使える外部の資金が混ざらない DeFi の実証を検討しています。この際、どのような VC にすべきか、Issuer はどうするのかというような論点が多数残っております。

4 つ目は自治体や民間、DAO による給付金やトークンの配布での活用です。こちらは未来の展望ではありますが、給付条件になるような属性や資格情報を VC 化することができれば、その保有者に対して給付するのは国や自治体だけではなく、民間や DAO も可能になってきます。例えば扶養している子供の人数を証明する VC があれば、多子家庭の給付を国や自治体ではなく、民間でも実現できると考えています。一方、このような公的・準公的な性質を持つ VC の場合、Issuer の責任は非常に重く、大きな論点になると考えております。

最後に要望や課題のご共有になります。1 つ目は、VC は VC ごとの専用のウォレットでの受取ではなく、様々なウォレットで受け取れる方向に進んでほしいという要望です。VC ごとの専用のウォレットがある場合、VC が普及する未来において、ユーザーは複数のウォレットを管理する必要があり、結果的に UX を損ね、また複数ウォレットに入った VC、クレデンシャルの紐付けなどの課題も存在していると認識しています。Web3.0 領域を含め、多様な DID/VC のユースケースが開拓されていくためにも、さまざまなウォレットにVCが発行可能な、バランスの取れたガバナンスを望んでおります。2 つ目は、Web3.0 ウォレットとしての DID/VC 活用についてです。DID/VC をブロックチェーン上で活用する取組は、ツールなどは出てきてはいるものの、実際の実例が少なく、エコシステムとしては成熟していません。Web3.0、DID/VC、隔てることなく、研究者、開発者、コミュニティ全体を支援するような取組の必要性を感じております。最後になりますが、公的個人認証サービスと DID/VC の併用についてです。VC の発行等において、マイナンバーカード、公的個人認証サービスの利用を検討していますが、VC における利用については今後整理が必要な論点があるのではないかと考えております。

我々からは以上になります。ありがとうございました。

（中村素典座長）

はい、ありがとうございました。ただいまお二つ、各社様のご説明いただきましたけれども、まずは今までの発表につきまして、ご質問、あるいはご意見ある委員の方は挙手、あるいはチャットでお知らせい

ただけますでしょうか。まず富士榮委員からお願いいたします。

（富士榮委員）

お二方ともご説明どうもありがとうございました。

それぞれについて何点か質問はあるのですけど、ちょっとピックアップしながらいきたいと思います。まず DID/VC コンソーシアム様の方です。おっしゃる通り、Issuer のガバナンスについては非常に重要な話だと理解しております。まずはテクノロジーでできることとルールでできるところの区分けと、責任の所在というところを定義していくのがよろしいのではないかと、まずは雑観として思いました。例えば U.S. の AAMVA がやっている Mobile Driver’s License のガイドラインを見ていると、Issuer が発行先となる Wallet に関しても管理をするということを求めています。EU の ARF では Verifier の制限をどう実装するかについて、後段で Trusted List の話が出てきましたけれども、議論が行われていると思いますので、その辺はすでにご覧になっていると思いますが、参考にしていただくといいかと思いました。

あと、クレデンシャルの再利用というところがフォーカスかと思ったのですけれども、身元確認書類に本当に該当するものをリユースして良いものになるかどうかというところを少し考えた方が良いのではないかなと思っているので、見解を聞きたいのですけれども、資料を拝見していると、もともとの身分証明書をもとに、特定の銀行が作成した確認済であるという旨の証明書を、色々なところで使いまわすというふうに見えているのですけれども、この Verifier の目線で見た時に、さっきカード会社を例であげていらっしゃいましたけど、これは身元確認、本人確認をカード会社がやるという話ではなくて、銀行が確認したというものを受け入れる場合は、自分でやらなくても、銀行がやってくれたのでそれを受け入れるというふうな、シナリオだと思いましたが、まずこれはリユースと言っていいのかどうかというところの意味がよくわからなかったので、それを再確認させていただきたいなと思います。

そしてその場合に Issuer は誰に当たるのかでいうと銀行だろうと思っており、銀行はそれを Holder があちこちで使うというところについて、どこの責任を負うのか、もともとの身分証の発行者は、例えばマイナンバーカードを使うのであれば、国という話になるでしょうけれども、そこはそれを使って発行された、銀行が身元確認を行った派生クレデンシャルですよね。

こちらについてのトレーサービリティはないわけなので、銀行はそのリユースされているクレデンシャルについて、取消を含めた管理とか、状態管理というものをちゃんとしていくのが必要最低限の要件になると思うのですけれども、このあたりについて、言及があった Trusted List の話もあったと思いますけれども、どのように、どこまで実装されていこうとしているのか、Wallet に入ったものをどこまで消せるのか、Verifier に提示された後のものをどうやって revoke できるのか、この辺についてもう少しお伺いできればと思いました。

マイナウォレットさんの話についてはブロックチェーンのところと、VC、マイナンバーカードというところの関係性はよく読み取れませんでした。ブロックチェーンを使われることの意味について、どういうことを考えていらっしゃるのかお伺いできればと思いました。例えば、ガバナンスを行うために、Verifier が署名検証を行う範囲を限定するために、コンソーシアム型のチェーンを使うとか、そういう意味合いだったりするのかなと推測したのですけれど、その辺を教えていただければなと思いました。

すみません、長くなりましたけど以上でございます。

（中村素典座長）

では一旦ここでご回答いただきましょうか。

まずは DID/VC 共創コンソーシアムさんからお願いいたします。

（DID/VC 共創コンソーシアム宍倉）

DID/VC 共創コンソーシアムの宍倉です。いくつかアドバイスと質問をいただいていたと思っております。質問の方、回答させていただきます。

身元確認書類に相当するものを VC として出してよいのかというところですけれども、今回ご紹介したスキームで犯収法施行規則第六条に定める力方式は、すでに民間事業者が発行する電子証明書を用いた本人確認というものが法に定まっていて、その観点からすると、民間がすでに電子証明書を出している、国が認めたものかと思われます。

技術的にそれに当て込むことができるかというところだけを見ておりまして、我々のほうで民間事業者が身分証明書に相当する電子証明書を発行してよいかといったところは、検証スコープに入れていないところであります。

もう少し詳しく申し上げると、このカ方式事業者は、国が認定する認定特定認証事業者であるのですけれども、認定プロセスの中で発行する電子証明書の有効性確認のステータス管理の義務を負っているというところでもございますので、この最新化ができないというような時には、そもそも認定が取れないというようなところもありますので、発行先の Holder の最新性は担保されると思っております。

一方で、銀行が出した取引時確認 VC を本人確認に使うかどうかという論点に関しては、今日ご紹介した事例の中では身元確認のものとしては使わないという整理としております。あくまで任意で、銀行が実施している反社会的勢力チェック結果を補完的にマイナと組み合わせて使うという、任意の組み合わせ VC として位置づけているところではあります。

一方で、ご指摘いただいたクレジットカード会社が銀行の本人確認を信じて取引できるかというところは、すでに事例が犯収法施行規則第十三条にございまして、銀行 API を使う方式ではあるのですけれども、それと同じような形で VC が使えないかと。課題は多々あると思うのですけれども、ぜひ検討していきたいと思っているところです。

（富士榮委員）

ありがとうございます。銀行 API の話との違いが、VC の特性としてオフラインのシナリオですね。こちらをどこまで考えるかが VC の良さだと思うので、逆にそれをなくしてしまうのであれば、フェデレーションなり API で済むじゃないかというところも考えながら、VC を使う意味合いを考えていかれると良いのではないかと思いました。

（DID/VC 共創コンソーシアム宍倉）

ありがとうございます。

（中村素典座長）

続きましてマイナウォレット様も簡単にご回答いただければと思います。

（マイナウォレット株式会社橘）

では少しクイックになんですけれども、まずマイナウォレットはデジタルアイデンティティウォレットである以前に Web3.0 ウォレットになりますので、そういった意味でブロックチェーンを使うということがベースのユースケースになってきます。

そのため、ブロックチェーン上でのユースケースの中で、DID/VC というもの、あるいはクレデンシャ

ルというものをどういうふうに活用できるかっていうのを考えている、というのが我々の DID/VC の見方なのかなと思っております。

（富士榮委員）
　ありがとうございます。

（中村素典座長）
　ありがとうございます。では次は2番目の笠井委員からお願いいたします。

（笠井委員）
　ありがとうございます。DID/VC 共創コンソーシアムさんに少しお尋ねさせていただきます。
　17 ページ目の適格性の問題のところ、まさにご提示いただいたところかと思うのですけれども、このような議論があったのか、少し教えていただきたいなと思いまして。結局、その各ステークホルダーのガバナンス、適格性を確認するところに結構コストもかかるのではないかという議論があるのではないかなと思います。本来、一度本人確認を銀行がすれば、それを使いやすくすれば、お客様にとっても使いやすいし、コストも下がるような感覚があったのではないかと思うのですけれども、リスクガバナンス強化にもそれなりにコストがかかると思っており、例えば、Verifier の方々からダイレクトにマイナンバーカードを確認する方が安いのではないか、コストがかからないのではないかとか、このようなコンソーシアムの中でコストとこのやり方のバランスは、議論としてあったら教えていただきたいと思います。

（DID/VC 共創コンソーシアム宍倉）
　ありがとうございます。ご指摘の通り、まだビジネス的なこの方式を実装した時に、公的個人認証よりもコスト的に優位性があるかは現在検証できておりません。この金融機関含む特定事業者のところで、一番本人確認のところでマイナではできない部分というところがありまして、それが先ほど申し上げた反社会的勢力ではないかどうかの判別です。今、警察庁のデータベースで、いわゆる反社会的勢力情報があって、そこは一部の特定事業者はアクセスできますけれど、機微な情報でもあるので全員がアクセスできるわけではありません。
　そのデータベースにアクセスできる事業者が、確認した内容を VC で発行する。このお客様は、我々のところできちんとチェックをして、いわゆる反社会的勢力じゃないということまで含めて確認しましたというような VC ですと、マイナではできない価値が出てくると。逆にそこを確認できない、直接的に警察署に照会できないとか、そういう事業者が自前でそういう情報収集して対策をやっている、コストをかけているというところがございますので、単純にマイナと比較して経済的合理性があるかというよりは、そういった諸々の反社会的勢力等の情報を収集するコストまで含めて、こちらに合理性があるかというところで、判断していければと思っております。

（笠井委員）
　わかりました。ありがとうございます。

（中村素典座長）
　よろしいですか。では次は板倉陽一郎委員お願いいたします。

（板倉陽一郎委員）

弁護士の板倉です。感想めいたものになってしまうかもしれませんが、この手の話をする時に、参考にしなきゃいけない事件としては、過去の某金融機関と某通信事業者の事案があろうかと思います。いずれもちゃんとした会社だろうと思っていたところ、完全に双方が穴になっていて、非常にたくさんの不正利用がされたと。もう一つ、これ自体ではないですが、覚えておかないといけないのは、悪い人は我々よりもさらに合理的でありまして、一番穴があって一番儲かるところに全精力を突っ込んできます。

最近ですと、皆さん、知らないかもしれませんけど、ある独自のデジタル地域通貨事業は、1 万円で 1 万 5 千円分の地域通貨が買えるのですが、どこかが甘かったのか不正利用されたというのがあります。

なので、特に金銭の移動を伴うような VC の発行、先ほどお金の移動には使わないというふうにおっしゃっていましたが、少しでも考えているのであれば、今より少しでもそのセキュリティが下がるようなものは参入してはいけないというのが基本ではないかと思います。

もう一つは Wallet Provider です。過去の某仮想通貨取引所の話を皆さんご存知かと思いますが、問題があったのはどうもその Wallet Provider の周りではないかというふうに分析されているところであります。

よくわからないのに事業を始めるというのは、絶対あってはならないと思います。つまり、最初のコンソーシアムのご発表で、基本的には銀行が責任を持つようには書かれていましたが、よくわからないけど銀行であるがゆえに Wallet 側ドリブンで事業を始めて、その仕組み等は全く分からないというものは必ず排除していただくような仕組みにしていただかないと、もう何が何だか分からないまま全部やられて、廃業することになり、Wallet 側の会社は引き続き生き残っているということはあってはならないのではないかと思っております。

それから、加盟店管理はしたくないとおっしゃっていたと認識しましたが、基本的に加盟店管理責任がないところから、さまざまな金融法上の問題が生じていると認識しておりますので、加盟店管理はしないという仕組みで制度を設計されるとなると、少なくとも消費者保護の関係者は絶対に許さないとなると思いますので、加盟店管理はすると、発行者はすべて責任を持つ前提でやっていただくと。それでも商売になるかというところで一つ考えていただいた方が良いのではないかと思います。

犯収法上の仕組みにつきましても、危ないものは随時、今度規則を改正してやめていくという方向でもありますし、日本が不適切な利用の穴になると、とにかく悪い人たちはそのような国を標的にして悪いことをするわけです。世界で一番穴があるところを狙ってくるわけです。そこを、商売になるかもしれないという理由でレベルを下げるという方向には今ないのではないかと思います。世界の中で一番甘いところが狙われるわけですから、そうならないようにしていただきたいと、特に金銭の移動を伴う場合はそう思います。

それ以外のものについては、リスクの判断で、資格の証明などについては、もちろん検討していただいて構いませんが、お金の流れが生じるところは世界中から一番悪いところが狙われるという前提で考える必要があると思います。

特段、回答を求めるものではありませんが感想です。

（中村素典座長）

感想ということですので、次の質問の方に移りたいと思います。

では、板倉景子委員からお願いいたします。

（板倉景子委員）

私もちょっと半分感想半分質問というところで、特にマイナウォレット様の事例についてです。

こういった VC の事例を考えるときに、重要になってくるポイントとして、失効管理があると思っていまして、正しくクレデンシャルを消したい時に消せないと、プライバシー問題につながると思いますので、このあたりについて検討していく必要があるだろうと。もし何かご検討されていることがあればお伺いしたい。もう一つは特に金融機関との口座連携で、先ほど板倉先生からもありましたような過去の事例では、そこの部分の本人確認で、メールアドレスだけで紐付けができたりというところで事故になったというような事例もありますので、生体情報とのバインディングだったり、顔写真照合をいかに使っていくのかが一つのポイントになってくると思っております。

そのあたりの生体情報との紐付けについても、何か予定されているところがあればお伺いしたいと思う次第です。

（中村素典座長）

では回答ありましたらお願いいたします。

（マイナウォレット株式会社橘）

ありがとうございます。まさにいわゆる Issuer の適格性というか、どういう VC を発行するのか、管理するのがどのくらい大変なのかみたいなところがあると思いますので、そこは今弊社でもすごく検討しているところです。また、いわゆる生体情報との紐づけに関しても、我々は、現状、公的個人認証サービスを活用することを前提においていますが、もちろんそういったところの検討もしている最中です。

ですので、いろいろとみなさんで議論いただいた結果だったりとか、こういった場でアドバイスいただいたところを随時反映していきたいと考えております。

（板倉景子委員）

ありがとうございます。

（中村素典座長）

では最後になるかと思いますが、瀧委員お願いいたします。

（瀧委員）

ご発表ありがとうございました。私からは DID/VC 共創コンソーシアム様に向けて一つコメントと質問がございます。大きなコメントとしては、金融機関というのは、個人であれ、企業であれ、最も実在性の確認を実地でも行っている、他の社会的機能の中でも群を抜いて、それをやっている団体だと思っていますので、そこから VC が提供されていくという構図はすごくいいものだと思っています。

私からの質問は、私もデジタルインボイスの推進とかの協会をやったりしておる立場ですけれども、よくある話として、例えば消し込みがしたいですといった話に最後つながるものでもあるのですが、請求書の送り元と、そこの請求書に記載されている銀行口座情報、これを送金する時には統合 ATM スイッチングサービス経由で相手の名前が出てきて、お金を送りますと。ただ、これが本当にその人なのかがわからないところに事業所 ID なのか LEI とかが紐付けられて、その LEI が非常に信頼できるということになっていくと。今までであればファックスで送られてくるものとデジタルインボイスで、情報の信頼度に変わりがないよねって思われてきたところから、かなり被仕向け先の情報として信頼ができるようなタイ

プの情報に変わるわけでございます。

そういうユースケースというのは、コンソーシアムの中で議論としてあられましたか、もしくはどうお考えですかというのを率直にお伺いしたいのと、この時によく議論になってくるのが、結局 LEI というのは法人マイナンバーというか、法人単位で識別されることが多いと思うのですけど、当社もやっているような請求書のサービスとかは部署ごとに違う ID を付しているところもあります。なので、法人 ID と事業所 ID の差分とかで、もし何かお感じのことがあれば、ぜひ教えていただきたいというところになります。話せる範囲で結構です。どうぞよろしくお願いいたします。

（DID/VC 共創コンソーシアム宍倉）

ありがとうございます。DVCC の宍倉です。

LEI は EUDIW の動向等と比べて、国際標準的にこれを普及させるべきかどうかという議論はありつつ、注目している機能として、所属企業の身分、従業員の身分を証明するような使い方もできるというところがあります。

〇〇部の部長にはこの vLEI で、△△部の部長にはこの vLEI で、と違った vLEI を発行するということもできますので、企業単位のマイナンバーみたいなものではありつつも、その下に紐づいている所属している従業員のところにまで掘り下げた VC というのが発行できるので、今おっしゃっていただいた請求先の部署の責任者の名前単位で発行する、そういうものと連動させることはできるかと思っております。

一つ前の質問に戻りまして、請求書に紐付けたユースケースのインボイスに対して VC を何か適合させることができないかといったことは、レシートのユースケースを考えた時に俎上には上がったのですけれども、深掘り議論できたことはないです。

（瀧委員）

どうもありがとうございます。

（中村素典座長）

挙手がありましたので、では、中村龍矢委員お願いいたします。

（中村龍矢委員）

マイナウォレット様へのご質問で、DeFi との組み合わせというのは本当に DeFi のプラットフォームを作っていた身としても非常に興味深く、かつ、求められたテーマなのかなと思うのですけれども、それをどういうふうに実際に社会実装していこうかという観点のご質問です。一点目が Uniswap の例が出たと思うのですけれども、どうやって DeFi の事業者に強制するのかというところで、色々な国の人がトランザクションを投げている中で、日本の仕組みでとりあえず Verify されたアカウントがあるという中で、どういう段取りでルールにしていくのかなというところ。二点目は技術的な仕様を把握しないと、かなりナイーブなご質問ですけれども、そういう特定の国の認証システムに紐付けられたアカウントであるというのが、紐付けられたというのを Verify した後にどういうふうに売買とかを防ぐのかというのは気になったところでございます。

（マイナウォレット株式会社橘）

ご質問ありがとうございます。

まず一点目ですけれども、今我々として出している例は Uniswap なのですが、現状、流れとしましては、DeFi 側がこういったいわゆる適格投資家であったり、そういうインスティテューションがこういった DeFi を使いやすくするように、ミドルウェアを挿せるような仕組みを提供し始めています。

今回 Uniswap も V4 でフック(Hooks)という機能がリリースされました。こちらを利用すると、任意のバリデーションロジックのようなものを差し込むことができます。そうしますと、例えば我々で言うと、マイナウォレットからしかアクセスできない流動性プールというのがすぐに実現できて、そうしますと、誰の資金かも分からないようなところと、プールを分けることができるので、綺麗なプールで取引ができるということが実現できるようになっています。これは Uniswap だけではなく、ほかの DeFi でも同じような取組というのが少しずつ最近始まってきているので、これは少し我々としても注目している領域です。二点目ですけれども、すみません、もう一度質問をお願いしてもいいでしょうか。

（中村龍矢委員）

二点目は、安全ですとなったアカウントの売買とかをどう防ぐのかと。

（マイナウォレット株式会社橘）

そうですね。ありがとうございます。それに関しては、国際的な動向であったりとか、そちらは少し我々もキャッチアップはしていないですけれども、マイナウォレットの場合は、そもそも公的個人認証サービスをベースに作っていて、暗証番号を入力できないとそもそもトランザクションが送信できないので、その場合に、我々の場合ですと、例えばマイナンバーカードと暗証番号を盗まれたりとか、あるいはそれを売買するということがない限りは仮にアカウントを売ったとしても操作することができないというような形になっています。

（中村龍矢委員）

ありがとうございます。

（中村素典座長）

よろしいでしょうか。ちょっと時間押してしまいましたが、たくさんご質問いただきましたので、ご回答いただきました。取組内容の紹介につきましては以上といたしまして、次に本有識者会議の趣旨であります VC に関連する各種制度等についてということで、こちらの資料につきまして事務局からご説明をお願いしたいと思います。

（デジタル庁當波）

事務局でございます。資料 4 の「VC に関連する各種制度等について」について、事務局當波よりご説明させていただきます。本日先ほどのところでお時間を取りましたので、簡単に飛ばしながらご説明をさせていただければと思います。

まず全体の説明が少々長くなっておりますので、簡単に流れからご説明させていただきますと、まず今回、VC のご説明と、今回の検討会におきまして、様々スコープを切っているところがございますので、まずそちらについてご説明を差し上げたいと思います。

今回は VC を用いた本人確認をスコープとさせていただいておりますので、そういった本人確認の課題、またその脅威のご説明を差し上げたいと考えております。加えまして、先ほども例がありました PKI のような法令・制度・仕組みとの関連性、また留意点を IHV モデルをベースにまとめさせていただいてお

ります。また続けて、そういったこれまでの仕組み・法令といったものを踏まえて、どういったところに留意をしなければならないのか、どういったところに考慮しなければならないのか、というところを、事務局としての案ではございますが、簡単にまとめさせていただいております。最後に、今回の会議におきまして、事務局としてご議論をいただきたいポイントをまとめております。こちら3章と4章の事務局の整理について深掘りするご議論をいただければと考えております。

まず議論対象についてでございます。今回の会議のテーマは先ほどから何回も用語が出ております Verifiable Credential、VC でございまして、こちらはデジタル署名による真正性・改ざん防止等の機能を実現することができる機械可読かつ汎用的なデータ形式でありまして、これは W3C における Verifiable Credential Data Model のこと自体を指す場合もございますが、今回の会議におきましては、mdoc でありますとか、他の証明書の形式も含めて、デジタルにおける証明書の発行に着目して、議論を進められたらと考えております。

先ほどの説明同様、スコープは mdoc であるとか、他の形式も含むところでございます。

また今回、IHV モデルに限らず、デジタル証明書の利活用というところで会議を開かせていただいておりますが、こちらの Issuer に着目して、整理を行わせていただきたいと考えております。IHV モデルにおけるガバナンスにおきまして、議論するべき点としては、こちらの Issuer、Holder、Verifier、また Verifiable Data Registry、Status List Provider、Wallet Provider といった形で、さまざまな論点があるところではございますけれども、今回はあくまで IHV モデルに限らない証明書の流通ということで、クレデンシャルの発行というところ、Issuer のアクションに関するところを中心として、整理を進めさせていただきたいと考えております。

また最後にもう一点、スコープを切らせていただいております。具体的には本人確認に関する用途に焦点を当てて議論を行わせていただきたいと考えております。しかしながら、本人確認用途の VC に限らず、汎用的な VC と共通する留意点もあると考えておりますので、こちらにつきましては、縛られすぎずに参考としてご議論いただければと考えております。特にこちらの最後のお時間に、ユースケースの議論をする時間を設けさせていただいておりますが、こちらについては本人確認に限らず、これは資格証明・属性証明も含めて、広くご議論いただければと考えております。

本人確認についてでございます。今回の議論のスコープは本人確認ということで置かせていただいているというのは先ほどご説明した通りでございます。こちら本人確認という行為自体は以前から存在するものではございますが、デジタル環境の制限、またその特徴もありまして、特にそのデジタルにおいては、誰が誰であるかを証明・確認、アイデンティティを確立することの重要性が増していると考えております。

正しい利用者であるか否かを区別するところ、またこの基準・定義を設定するというところは、現在のディープフェイクでありますとか、AI といった攻撃手法の高度化も含め、依然として重要かつ困難な課題であると考えておりますが、こちらの VC の利活用においても、この信頼性を担保するために、こういった脅威を踏まえた整理・議論が必要と考えております。

また今回のスコープとしている本人確認につきまして、より正確な議論のために、用語については本スライドの通り、初回登録時などに利用者情報を収集・検証・登録する行為を身元確認（Identity Proofing）、またあらかじめ登録された本人であることを確認する行為を当人認証（Authentication）、という用語を使わせていただきたいと考えております。また本人確認という用語につきましては、こちらの2つを総称して呼ぶこととさせていただきたく存じます。

また、本人確認に関する議論の参考として、デジタル庁で実施しております、本人確認ガイドラインの改定に向けた有識者会議の資料を参考として付けさせていただいております。こちらにつきましては

身元確認プロセスの分解、それぞれのプロセスにおける脅威、またその対策についてまとめさせていただいております。こちらについては議論の際に、必要に応じてご利用いただければと考えております。

それでは3章の各種法令・制度・仕組みとの関連及び留意点ということで、まとめさせていただいております。今回は VC の利活用に向けた議論の参考といたしまして、既存の法令で本人確認に関するもの、また法令に限らず、PKI といった仕組みも含めまして、それらについてざっくりと IHV モデルに当てはめ、整理を行わせていただいております。法令に依らず、PKI や業界団体の取組といった仕組みも含めまして、信頼性向上のために、必要な議論が参考としていただければと考えております。

まず発行者に対する法令・仕組み等についてでございます。まず先ほどから何回も出ております通り、PKI、公開鍵基盤の事例といたしましては、電子署名法であるとか、CA/Browser Forum の基準も含めて、各種基準への準拠というものがあると考えております。また加えまして、こういった基準に加えて、その基準に準拠しているということを担保するための仕組み、これは調査・監査・審査、またこのペナルティも含めて、そういったガバナンスの仕組みが構築されていくと考えております。またそれらに加えて、そもそも証明書の失効であるとか、CP/CPS のようなものを用意することも受けまして、標準化された技術、これらの PKI にデジタル署名を健全に利用するための周辺の技術でありますとか、プラクティスも含めて、認証局が信頼に足る主体であること、またこの利用における真正性が積み重ねられていると考えております。参考として、電子署名法の認定基準で求めている基準を掲載させていただいております。お時間の都合で省略させていただきます。

続けて発行者に対する法令・仕組み等の例といたしまして、本人確認書類を求める既存の法令の例といたしまして、本人に対して一に限り発行される書類というものがあるとご説明させていただければと思います。こういった本人に対して一に限り発行される書類を求める法令というものが、例えば行政手続や保有個人情報の開示請求で求められるところでございますが、こういったものは本人確認書類の貸与、貸し借りのリスクを減らして、身元確認の確実性を高める役割があると考えております。
またこのアイデンティティドキュメント、身分証の複製・派生という考え方につきましては、デジタルの特徴として、データの複製が可能であるという点、原本のまま複製ができてしまうというような点が挙げられると考えております。また複製でないとしても、派生 ID、Derived ID という形で、ある証明書の中身をコピーするような形で、別の方が証明書発行を行い利用するようなケースもあると考えております。この Derived ID の場合におきましても、証明権者は派生の作成者であるというところで、原本からの一意性を喪失させるもの、原本の管理者の管理が行き届かないところがございますので、こういったものも追加の信頼性を向上させるための措置なしでは、原本と同様の性質を持つ書類として流通させることは困難であると考えております。

またこちらも簡単に、民事訴訟法上の真正な成立というところと、公文書・私文書というところを踏まえてまとめさせていただいております。先ほどの本人確認書類を含め、公的な機関が発行する書類は公文書ということで、民事裁判によって真正に成立している、その文章が作成名義人の意志に基づいて作成されたものであると取り扱われることになっております。一方、民間が発行する VC を含む私文書につきましては、電子署名法3条の推定規定であるなり、他の方法によりこれが立証される必要があると考えておりまして、またその中身の証拠力、実質的証拠力を含めまして、その円滑な取引のためには、利用形態ごとのリスクに応じて、基準・ツールでありますとか、その基準への準拠を担保する仕組みというものを設けて、その信頼性を向上させることが必要なのだろうと考えております。

続けて検証者に対する法令・仕組み等についてでございます。本人確認の行為自体はこれまでも法令によらない形で、民間において多く行われてきたものであると考えておりますが、特にそのリスクが高い手続、確実な本人確認が求められる手続におきましては、例えば業法のような形で、その規制対象と

なる業界における不正の防止であるとか、健全な発展といった目的を踏まえて、本人確認の義務を課す、または本人確認の方法を定めてきたと考えております。こういった形でリスクに応じて、こういった検証者にもルールが設けられていると考えております。

また検証者について、法令等が設けられている事例といたしましては、公的個人認証サービスのマイナンバーカードの署名用電子証明書、また利用者署名用電子証明書におきましては、大臣認定の形で署名の検証を行う署名検証者等につきまして、業務の設備でありますとか、検証の方法が基準に適合しているということを確認し、大臣認定を与えております。こういったところを通じて、適切な利用を担保する仕組みが設定されている事例でございます。

また VC の利活用に限らないところとして、こちらのプロセスに依らない法令・仕組み等というものも関係していると考えております。例えば個人情報保護法であるとか、電気通信事業法、また刑法といった法律、またアプリストア事業者の規約であるとか、その他プライバシーであるといった、消費者に対する配慮が必要となる点というものが、この他にあると考えております。VC の利活用におきましても、そのユースケースであるとか、利用形態によりまして、まだ未成理の論点がある可能性があると考えてございまして、これらについては、個別の整備が必要になってくるだろうと考えております。

また参考として、昨年春のマイナンバー法の改正により規定されました、カード代替電磁的記録について、こちらスマートフォンにおいて活用できるクレデンシャルの例としてご紹介させていただきます。カード代替電磁的記録につきましては、発行の手順、またユーザーのデバイスからの送信の手順、また受信者・検証者側の手順について、法令により規定が行われております。具体的には、発行については、法定された手続きに基づいて、J-LIS が行いまして、送信用プログラム・確認用プログラムにつきましては大臣認定を設けるなどして、その利用にかかる信頼性・安全性を担保しております。また、こちらもご参考ではございますが、マイナンバーカードがその信頼性の高い身分証として、不正利用に対処するために、さまざまな仕組みが講じられてございます。また一般に、Derived ID・派生 ID につきましては、元の証明書の記載事項が更新された際の反映等に課題があると考えております。また中身の正確性というところに加えまして、発行者自体の信頼性というところを担保するというところも含めて重要な観点であると考えております。

まとめになります。お時間もありますので、こちらについては省略させていただきます。

続けて、先ほどの各種法令も含めて、事務局として整理を行ったものについてご説明させていただきます。まず、VC の利用時の考慮事項、問題点がある、問題点が起こり得るところといたしましては、そもそもクレデンシャルの内容が真であるか否かといった発行プロセス、またこの発行されたクレデンシャルの信頼性に関する問題があると考えております。また、もう一点、発行されたクレデンシャルが真である、クレデンシャルの中身が正しいという場合においても、誤った使い方をされるという、発行されたクレデンシャル自体及びその流通に関するその問題に分けさせていただいております。

これらにつきましては、こういったクレデンシャルの中身の発行プロセスの本人確認のところでありますが、委員からもご指摘がございましたクレデンシャルのライフサイクル、失効の管理に関するところの信頼性、またクレデンシャルの発行者自体の信頼性があると考えております。また発行されたクルデンシャル自体とその流通に関する問題につきましては、特に Issuer と Verifier の間で認識の不一致、こういった性能、こういったものが実現できるクレデンシャルであると誤認をして利用されるケースがあると考えております。

こういったことを踏まえまして、事務局としてこちらの対応のほうを整理させていただいております。こちらにつきましては、まず様々な課題があるわけではございますけれども、結局 Issuer において、何を証明している VC であるかを確実に正確に把握して、それを Verifier、ユーザーに対して、公表・正しく誤

認のないように伝達をするというところ、また Verifier におきましては、検証したい目的において求められる証明の要件でありますとか、ユースケースごとのリスクを正確に把握した上で、必要十分な証明ができる VC を受け入れることが必要であると整理させていただいております。

具体的には、例えば一次情報源を管理する人が誰であるかといったところ、また記載されている情報は、住所のように引越しが発生して変更されるようなものか、名前・性別のように変更する場合はあれ、長期間信頼しても良いと考えられるものか、また発行プロセス自体の信頼性、また加えて、情報の開示とその透明性という形で整理を行わせていただいております。

また、先ほどから話が出ております Derived ID につきまして、簡単に参考として整理を行なさせていただいております。こちらの細かい説明については省略させていただきますが、Derived ID の場合、検証しなければならないところが一般的に増えるであるだろうというところを整理させていただいております。

また Verifier において、リスクを正確に把握して目的に沿った必要十分な証明ができる VC を使うというところでございますが、例えば属性情報、VC に格納される属性情報と申し上げましても、例えばそれを属性情報、属性の証明として利用するのか、資格の証明として利用するのか、今回のスコープとさせていただいております本人確認として利用するのかといったところで、本人性の厳密さでありますとか、リアルタイム性といった要件が異なってくると考えております。

また属性確認と身元証明の関係性についてでございますが、一般に卒業証明書でるだとか、ワクチン接種証のような、属性に関する証明書単体で身元確認は行えず、本人確認書類と組み合わせて、本人確認書類に記されている名前を持つ方と、いま目の前で申請されようとしている方が同一人物であるか確認した上で、その属性に関する証明書に載っている名前を本人確認書類が一致すると確認しなければならないと考えております。こういった身元確認につきましては、一般的には写真付き身分証でありますとか、公的個人認証サービスが利用されることが一般的であると考えております。

続けて Verifier において、リスクを正確に把握した上で、必要な十分な証明ができる VC を受け入れるというところでございますが、例えば同じ学籍簿といったところが、大学であるとか、学校の学籍簿が一次情報源であって、発行者・証明権者が同じ学校であるというような証明書でありましても、卒業証明書と学生証では目的・様々なリスクが異なるということで、例えば顔写真が付いているだとか、証明書の有効期限があるだとか、改ざん防止がなされていますといったところで、それぞれ同じソースをもとにしているクレデンシャルがございますが、様々な対応の違いがあると捉えているところであると考えております。

まとめでございます。これらの議論を踏まえまして、VC が社会一般で利用されるためには、利用者・Verifier にとって安心安全なその利用形態であるということが重要であると考えております。例えばそのプライバシーに配慮したユースケースを実現できる分散型の技術でありましても、これが正しく利用されず、事故が発生してしまうと、これは普及の妨げになってしまうと考えております。こういった観点から、事務局といたしましては、検討事項が少なく、またメリットが大きい事例を VC の初期ユースケースとして推奨していくというような形でまとめさせていただいております。例えば、推奨される VC の初期ユースケース、検討事項が少ないと考えられ、またメリットが大きいと考えられる事例の要件・性質といたしましては、例えば発行者が情報源を管理する、発行者自身が証明権者な属性に関するもの、不正利用のリスクが大きい手続に用いる書類であるとか、証跡であるとか、属性であって、まだ現在機械可読な形式で利用できない、デジタル署名が伴っていないようなものが、初期の VC のユースケースとして推奨できるのであろうと考えます。

本日議論いただきたいところといたしましては、これまでご説明を差し上げました、各種法令・制度・仕

組みとの関連また留意点について、事務局整理を踏まえて、VC を本人確認の用途で利用する上で、安心安全な利活用を進めるためにはどういった点に留意すべきか、というところを事務局の整理を踏まえてご議論いただければと考えております。また安心安全に利用できる環境の構築に向けて、個々の事業者・業界・国それぞれについて、どういった対応が望まれるかという観点でも、ご議論いただければと考えております。加えて、後半の事務局として、第3章の内容を踏まえて整理させていただきました内容につきまして、この留意点でありますとか、考慮事項、この事務局の整理が適切なものとなっているか、より適切な対応が考えられないか、その中でも優先順位が高い点、考慮が漏れている点、課題があるかといった観点でご議論いただければと考えております。加えて最後に、これまでの議論を踏まえまして、事務局の整理を行いました、考慮すべき観点を踏まえ推奨される VC の初期ユースケースの性質が適切なものになっているのか、他に最低限であるとしても加えなければならない要件があるか、またこれを踏まえて具体的なユースケースとしてどのようなものか考えられるか、これは官民それぞれについてご議論いただきたいと考えております。

事務局からの説明は以上になります。中村座長にお返しさせていただきます。

（中村素典座長）

事務局からのご説明ありがとうございます。

最後にまとめていただきました議論のポイントということで、大きく3つに分けてこれからのお時間でご議論お願いします。それではまず、最初に説明がありました「各種法令・制度・仕組みとの関連及び留意点」につきまして委員からご指摘、ご意見等ございましたら、挙手をお願いいたします。
では富士榮委員お願いいたします。

（富士榮委員）

長くならないように、一点だけ話します。安心安全で利用できる環境の整備のためにはというところは、記載ありました通り、一番の問題と言えば、VC というものがざっくりとくくられてしまって、それが何の用途なのかという点が、検証者や利用者にとって理解しにくいというのは、その通りだと思いました。その上で、今回の本人確認書類というものをスコープに考えた時に、やはり一番の問題がマイナンバーカードをデジタル化した証明書、いわゆるカード代替電磁的記録というものと、マイナンバーカードで本人確認を行ったことを示すデジタル証明書というものの差、違いを利用者や検証者がわかりにくくなっているというのが結構大きな問題だと思っています。

そうなってきた時に、単純な例ですと、銀行法では、銀行という名前をつけるということについては法律による規定があるように、マイナンバーカードを想起させるような名前の Verifiable Credential というものを何らかのレギュレーションで縛るような話も含めて、検討していく必要があるのではないだろうかと感じておりますので、今の A のところにありますような、どういう点に留意すべきかというと、ユーザーに誤認を招きやすい名称を使えなくするようなことは何らかできないだろうか、それに向けて何らかのレギュレーションというもので対応ができないんだろうかというところ、意見として申し上げたいと思います。

（中村素典座長）

ありがとうございます。特に途中で回答する必要がなければ最後にまとめて事務局からご回答いただく形で進めたいと思います。次は笠井委員お願いいたします。

（笠井委員）

私も富士榮委員と同様で、何のために VC を活用するのかという観点は非常に重要かと思います。先ほど言いましたように、マイナンバーを使った公的なものを直接的に使うのか、それとも民間の中で VC を作って運用していくのか、このあたりは必ず、今回の件で言うと、業法の中でもどのような位置づけか、先ほどの DID/VC 共創コンソーシアム様の方々は、犯収法の中で本人確認の手法のようにやり方まで定められている中での今回の手法ということで、ご紹介いただきました。

一方、私が担当しているようなお酒・たばこにおいては、年齢確認は求められているものの、その手法までは決まっておりません。各種業法においても、リスクがどうなのかということだけではなく、法律のあり方にも差がございますので、このあたりの整理が必要と思います。

また法律上のことかもしれませんが、一部の人しかアクセスできない情報が VC を通じて広がってしまうことについても、何か問題が発生しないのかという観点において、国が主導を持って整理をすべきではないかと感じました。場合によっては、先ほどのような業法の整理においては、マイナンバーカードの普及の観点も含めまして、デジ庁が横串で規律を整理するということも必要ではないかなと考えております。

（中村素典座長）

ありがとうございます。続きまして板倉先生、お願いします。

（板倉陽一郎委員）

制度というところで、本人確認一般についてなにか決めているものはなくて、みんな思い浮かべているレベルが違うのかもしれませんが、犯収法について言及されていたので、現時点で犯収法の施行規則は厳しく改正される方向であると。それは国民を詐欺から守る総合対策の中でやられているわけで、例えばカードを斜めにする方式（eKYC）もやめると、保険証もやめると言っている中で、最低限のレベルに達しているのかということですね。最低限のレベルに達しているというのは、つい技術的に大丈夫とかいう言いがちですが、この実際の利用の場面も含めて大丈夫なのかというところであります。
それを考えると、先ほども大体結論を申し上げてしまいましたが、金銭の移動を伴うような本人確認に、現時点でエコシステムも発揮しませんと関係者がおっしゃっている中で、直ちに犯収法施行規則で大丈夫ですと言えるような状況にはないのではないかと思います。

繰り返しになっていまいますが、過去の某金融機関と某通信事業者の事案というのは、日本を代表するような、最後まで責任持たなければいけないような会社が二つ揃って大失敗をしたわけでありまして、そこに新規参入を促す用途で犯収法施行規則をいじるというのは、現時点ではないのではないかと思います。

もちろん、反論があれば、頑張りますとおっしゃっていただいても良いと思いますが、とりあえずはそれ以外のもの、金銭の移動を伴わないような、本人確認でまずはやってみていただいて、今、用意されている犯収法施行規則のすべての方式の最低線、最低線では困るわけですけど、すべての方式よりも上回りましたというぐらいになったら、使っていただいても良いのでは、ということだろうと思います。

（中村素典座長）

ありがとうございます。では次は瀧委員お願いいたします。

（瀧委員）

富士榮さんと板倉先生に乗っかるコメントになるのですが、私もここに記載している本人確認の表現

は犯収法に基づく、ある意味、一番厳格なタイプのものもあれば、参考情報程度に扱われるものであったりとか、犯収法関係なくとも本人確認をする、少しトラストがあればいい、そういったものもあるわけでして、本人確認にも色々なグラデーションがある中で、例えばレンタルビデオとかは最近ないですけれども、そういうところで会員証を作るレベルのものでも、本人を確認する行為はあります。なので、そのグラデーションに合わせた議論がいるのだと思いました。

一つ例を取ると、例えばクレジットカードを作る時に、所属している企業の名前を書き、場合によってはカード会社から在籍確認の電話がかかってきたりするわけで、これなどは信用情報として、本人が在籍している確認をしているのだと思うのですが、大きい会社に属しているということは、日本社会だと非常に大きな信用力の担保になっているような点もありますので、そういうグラデーションの中で、旨味が大きいところを、やっぱりこういうものはたくさん使われて初めて納得が生まれていくものだと思うので、探っていく必要があるのかなというのが一つコメントとしてございます。

金銭移動の話を板倉先生もされていましたけれども、さっきのインボイスに絡んだお話とも似ているのですが、例えば今、銀行のインターネットバンキングでお金を送りたい時に、銀行によって二要素認証のあり方とか、どういう時にハイリスクの取引ですね、と発動するのかは、個々の銀行で、それはそれで正しい形ではあるのですが、異なっていると思っています。

こういったものを揃えていくことをしていかないと、なかなかインターオペラブルな VC だと思ってもらえないところがあると思っています。API の議論で恐縮ですけれども、イギリス等は UX を揃えるようなことをされているわけです。あとあまりリスク判定を厳しくやりすぎると非常に不便になるというのがありますから、例えば欧州とかだとパーキングメーターとかであれば、リスクを取って OK にしてしまおうということもするわけでして、そういう使い勝手に応じて、少し甘さを許容していくことが、どうしてもこの利便性、特に資金移動の関わるところだと起きていくと思っていまして、そういうグラデーションの中でユーザーが多そうなものをなんらか判定していけるといいと思いました。

（中村素典座長）

ありがとうございます。板倉景子委員、お願いいたします。

（板倉景子委員）

2 点だけクイックにお話します。

先ほどの DID/VC 共創コンソーシアムの方でも話がありましたけれども、Issuer の適格性をどうやって担保していくのかというところについて、論点整理ができるといいと思っています。どういうふうに発行していけばいいのかというやり方について、お話があったと思うのですけれども、実際誰がどう適格性を審査するのか、もしくは耐監査性という意味で、自社でも内部監査においてどういったところに整理していかないといけないのかを、確認できると良いかと思ったのが一点。

あと普及に関して、やはりユーザーからしてみると、プライバシーというところにおいて、そのデータがどういうふうに保管されて、誰の責任で、どう動いているのかというところの透明性がないと普及のブロッカーになると思いますので、そういった点について、透明性を持ってユーザーに対して説明ができるようにするというところが VC の普及において非常に重要なポイントになると考えています

（中村素典座長）

ありがとうございます。一通りご質問いただきましたので、ここで事務局よりまとめてコメントいただく形でよろしいでしょうか。

（デジタル庁當波）

皆様コメントいただき大変ありがとうございます。事務局の當波でございます。

まず富士榮委員からもご指摘いただきました通り、安心安全で利用できる環境の整備がまず重要であると考えております。また今回マイナンバーカードのカード代替電磁的記録と、マイナンバーカードで本人確認をした、というところの証明書の区別がわかりにくくなっているというご指摘をいただきました。こちらについては、今後、カード代替電磁的記録が実際に使われていくというところが今後ありますので、我々も VC の普及状況も踏まえながら、必要な策を講じられればと考えております。

次に笠井委員からのご指摘につきましても、何のために VC を活用するのかという観点が重要であるとご指摘をいただきました。また他の委員の皆様からも同様のコメントをいただいていたかと思いますが、どういった扱い方がされるのか、またその使い方に応じたリスクは、これまでもそれぞれの業界ごとに構築されてきたところがあると考えておりますので、VC というところで、全てが全て同様の整理を行うということは難しいと思いますが、まず実際のユースケースとして、可能性が高いところから順番に整理を行えたらと考えております。

また、今回の会議なども通じて、そういったレベル感の違いというものがあるのだ、というところは、もうすでにお示しできると考えておりますので、こういったところは積極的に取組をさせていただけたと思います。

また板倉弁護士からご指摘をいただきました犯収法施行規則に関するところは、我々は犯収法の所管でございませんので、具体のコメントは難しいところであるのですけれども、例えば国民を詐欺から守る総合対策でありますとか、そういった本人確認の手法について、本人確認に対する脅威、最初のご説明でも申し上げましたディープフェイクでありますとか、AI といったところも含めて、だんだん攻撃が高度化しているというところも含めて、レベルが上がっているというところは認識しておりますので、そういったところを踏まえて、VC の利活用においても、どういったあの脅威に対して対応できている VC なのかというところは、実際の Issuer の方にも Verifier の方にも分かりやすくの示していく必要があると考えております。

また瀧委員からもご指摘をいただきました少しトラストがあれば良いというユースケースについては、ある意味、国の関与があまり必要ないところで行われきたというところでございまして、あまり国からどうこう今から申し上げるというところがどこまでできるのかというところはございますが、例として挙げていただきました在籍確認の電話のような、ある意味デジタルでより効率的にできるであろうというようなところについては、今後もそのハードルを取り除くことをしていただけたらと考えております。

また最後、板倉委員からのご指摘についてですが、プライバシーであるとか、データの管理者が誰であるとか、説明責任、責任分解点がどこにあるのかを明確にするべきだ、というご指摘をいただけたと認識しております。そういったところの透明性を持ってユーザーに説明できるように、というところについては、今回の会議の結果のまとめにも反映できたらと考えております。事務局からの回答は以上になります。中村座長にお返しいたします。

（中村素典座長）

事務局からのご回答ありがとうございます。

次の議論のポイントとしましては、資料では 4-1 から 4-3 でご説明いただいておりました内容で「各種法令・制度・仕組みを踏まえた VC の利用」という観点で資料のご説明をいただきましたが、この内容につきまして、ご意見・コメントのある委員の方がいらっしゃいましたら挙手でお知らせいただければと思

います。では笠井委員お願いいたします。

（笠井委員）

特に留意する点ということで、私が思い浮かぶところではありますが、Verifier が VC を利用する頻度にもよるとは思うのですが、例えば Issuer が事業者としていなくなってしまったり、Holder である Wallet がなくなったりすると、使う Verifier としては大変困る、というところです。

ですので、34 ページのところに失効のメカニズムや有効期限の管理不足が課題として提示されていますが、そういった持続的に、この機能が必要な際に、どういった確認が必要なのかという事にフォーカスを当てると議論がしやすいのではないかと思います。

参考までにですけれども、例えば検証の仕組みは、電子委任状法の電子委任状取扱業務に定められており、そういうようなところが失効のメカニズムの参考になると考えています。

この話の延長線には多分、相互運用性の話も出てくるかと思っており、どのような形でのデータ形式であれば、流通が長く続くのか、安全にできるのかということは課題でもあり、解決するポイントかと思っております。

もう一つですが、私の業界のところだけかもしれないので、優先順位としては高くはないかもしれないのですけれども、例えば、この対象の VC を使われる事業者が、同業界の中でしか使われないような場合に独占禁止法に引っかからないのかどうかは事業者としては非常に気にしているところです。かといって、VC を使う Verifier を不特定多数にできないところもあったりもしますので、非常に私自身が悩んでいるところであるのですけれども、課題として提示させていただきます。

（中村素典座長）

はい、ありがとうございます。富士榮委員お願いいたします。

（富士榮委員）

中にもありましたが、Issuer の信頼性についてどのように確認をしていくのか、こちらについては CP/CPS の話も例として挙げられていましたけれども、一つ加えて言うならば、それをどのように機械可読にしていくのかというところも踏まえて、検討していくというのがポイントになるだろうと思います。例えばイタリアでは、OpenID Federation というスペックを使ってトラストチェーンをたどりつつ、関連する情報を確認していく手法も検討されていたりしますので、そういうところをうまく使いながらやっていけると良いのだろうと思いました。

もう一つは 39 ページに参考として挙げられていた身元確認書類と、属性確認書類、こちらは基本的に合わせて提示されるケースが多いという話がありましたけれども、それぞれの証明書は同時に提示をされるとして、同じ主体を表している証明書なのかどうかというバインディングの問題を確認できるような方法の確立も急がれるところだと思っています。

これは EU 等でも方法を検討されている部分だったりするので、他国とも歩調をあわせてやっていくというのは、先ほどの笠井委員のインターオペラビリティの観点から含めても考えていくべきことだと思いますので、テクニカルにも他国と歩調をあわせてやっていただけると良いのではないかと思いました。

（中村素典座長）

ありがとうございます。次は板倉先生お願いいたします。

（板倉陽一郎委員）

先ほど、また前倒しで言ってしまいましたが、こういう仕組みが導入された場合に、DID/VC 共創コンソーシアム様のご意見ですと、Issuer は銀行に限るということで、そこはそれなりに永続性があり、社会的責任もあるという前提だと思いますが、やはり Wallet ですよね。

全体として、こちらの仕組みに限らず、クラウドサービスに対する監督というのが、個人情報保護法の改正の議論の中でも本当に監督できているのかというのがありましたが、より一層、Wallet で、ブロックチェーンを使うかどうかは、別に関係ないと整理はされていますが、親和性が高いのでブロックチェーンも使いますと言った場合に、本当に意味が分かって導入するのかという疑念があります。たまたま銀行はコストをかけて本人確認をしているからそれを切り売りしたいのではないかと思われないためには、やはり Wallet についての適切な理解と、また業務委託先になるわけですが、きちんとそれを監督するのだというような前提でなければ、参加していただくのは難しいのではないかというふうに思います。

日本はサービス提供側がドリブンになることは多いです。ベンダー側に技術も法務も人材も居られて、どうしてもユーザー企業に対してベンダーの方から働きかけてサービスをやっているという若干倒錯した状態が一般的ですが、それはベンダー側がかなり社会的な責任を持って色々サービスを提供している分には良いですが、よくわからないけど Wallet のところは新規参入しやすいから色々入ってくると、コストをかけて本人確認しているからそれが商売になるのであれば、加盟店管理もしなくていいし流そうかと、そこまで言うとそうではないとおっしゃるかもしれませんが、そういうふうに見える状況にありますので、きちんと Wallet については委託先の監督をする、意味がわからないところは使わない、加盟店管理はきちんとやる、こういう前提でやっていただきたいと繰り返しておきます。

（中村素典座長）

ありがとうございます。次は瀧委員お願いいたします。

（瀧委員）

一つ前のテーマと若干被る話かもしれないのですけれども、いま投影されている属性情報を、例えばユーザーさんが能動的にちゃんとアップデートしてくれるかというのは、今の時期でいうと確定申告がそうですけれど、何か手続があって、それで間違ったことがあった時に不利益を被るようなインセンティブがないとなかなか難しいというポイントがあると思っていまして、ゆえにプッシュ通知とか Webhook とか、なにか能動的なアクションを取らなくても、自動で自分の情報をちゃんとアップデートする仕組みが備わって、初めて新鮮な情報の保持ができると考えています。

続いて Issuer の話で、2つトピックがあります。電代業（電子決済等代行業）で銀行からこの人の銀行口座についてのデータを取っていいですよというトークンは、だいたい保持している会社が1年に1回、銀行からモニタリングを受けるというサイクルで制度が始まって7年ぐらい回っております。年次で異なるモニタリングを百数十行から受けることは現実的ではないので、中身を事実上標準化して、標準化した中身に対して監査法人のレポートを取って、レポートを取るだけでは足りないので、自主規制機関が5～10 年に 1 回当たるような形で中身を見に来るということで、ある意味、銀行ではない、そういう VC を取り扱う人たちの監査を担保しているというのが実務的な現状です。電代業というのは、現状では主に通帳のコピーを取るというレベルのトラストを保持している制度になりますけれども、一つ参考となる頻度というのはそれぐらいというのがあると思っています。

これをやるときに、金融機関がある意味 VC を Issue いただいている立場であられると思うのですけど、結構問題なのが人事異動です。最後、中身が適切であるかというのを担保しているのは担当者が

いて、その担当者に電話が通じるかとかですね、困った時にちゃんと問題解決に向けて調整が頼めるかですけど、人事異動が 2、3 年に一度起きるので、その時にちゃんと情報がアップデートされないことがよく起きます。なので、これから Issuer をちゃんと認証しましょうという流れになっていくときには、人事異動というものにちゃんと耐えられるようにしておく必要があるなというのもベタですけれども重要だと思っております。

（中村素典座長）
ありがとうございます。板倉景子委員にお願いいたします。

（板倉景子委員）
今までの話をお伺いしていて、改めて今後の検討を進めるときに、やはりスコープを分かりやすくしておくことが非常に重要だと思います。先ほど冒頭で説明があったように、本人確認が、身元確認と当人認証を含むという観点において、一旦身元確認が終わったアカウントについて、それが当人認証の時に別の人である可能性があるというリスクはまた別の話だと思っていますので、じゃあどうやって安全に当人認証するのか、という話をしているのか、身元確認をしているのか、というところを明確にした上で、かつ身元確認では安全だったけれども、当人認証において何らかの状況によってセッションハイジャックのようなものが起こり、なりすましが発生している、というようなケースについて、ちゃんとケアをしていくことが重要になっていくと思っています。

（中村素典座長）
ありがとうございます。中村龍矢委員お願いいたします。

（中村龍矢委員）
少しベタになりますけれども、全体的には Verifier のインセンティブというか、Verifier が正しくこのスキームを使うインセンティブが気になるところでして、それがないと普及しない、もしくは変な形で使われて事故が起き得るかなと思っています。
具体的に申し上げると、Issuer は全体的に体力があるところが多いと思うのですけど、Verifier は多種多様なサービスが使うと。それもある種、この Verifiable Credential の良いところなのですけれども、そもそもあまり開発コストがないとか、リソースが少ないという企業の場合に、ここでいっぱい上がっている Verification のいろんな論点をちゃんと運用するということを、どういうふうに、どういうモチベーションでやっていけるかというところです。
よく選択的開示のような議論があり、ゼロ知識証明で一部だけ検証するなどがあると思うのですけれども、ゼロ知識証明の検証という結構難しい実装を臨床部分でやって、それでちゃんとセキュリティも担保してということをやってくれる会社がどれぐらいあるのかは気になるところですので、そのあたりが議論されていくと良いと思っております。

（中村素典座長）
ありがとうございます。一通りご意見いただきました。全体として、今までやっていた身元確認・当人認証というものの延長線上として VC というのがどう使えるのか、何に注意しないといけないのかということ、VC になったことによって更に精度をよくできるようになること、逆にそれによって注意しないといけないこと、今までできなかったことが更にできるようになること、についてどうするのかとか、いろんな

観点があるだろうと思うので、そういったところも VC として、どういうふうに事務局として捉えているのかの整理も資料として何かあると良いのかなとお話をお聞きしながら思いました。

では一通りご意見いただいたということで、事務局からまとめてコメントお願いできればと思います。

（デジタル庁當波）

事務局でございます。改めて様々なコメントをいただきありがとうございます。

まず笠井委員からのご指摘でありますが、Wallet や Issuer がいなくなるリスクも考えなければいけないというご指摘をいただきました。こちらについては用途にはよると思うのですけれども、例えば永続的なのであれば、ブロックチェーンとの相性が良いということも考えられますし、組み合わせる技術のセットも含めて、逆に論点が増えてしまうということもあるかもしれませんけれども、そういったところも含めて、検討を進めるべきと考えております。また独占禁止法の論点については、事務局としても把握できていなかったところでありますので、ご指摘いただきありがとうございます。

続けて富士榮委員からのそのご指摘でありますが、インターオペラビリティの点につきまして、これは業界のなかでのインターオペラビリティもあれば、国際でのインターオペラビリティもあると考えておりまして、議論をどう両立させるかというところについては、またご意見・ご知見をいただければと考えております。

板倉弁護士からのご指摘についても、クラウドサービスの監督というところのご指摘をいただいたというふうに認識しております。こちらについては難しい論点ではありますけれども、例えば今後、Wallet の提供事業者の認定であるとか、そういった仕組みが設けられれば、より適正な形になるでしょうし、そういったところも今後検討を進めていくべきなのであろうと考えております。

また瀧議員からのご指摘についてですが、間違った時に、その不利益があるような、インセンティブやディスインセンティブがないと、というご指摘をいただいたと認識しております。これは中村委員からのご指摘にもありましたが、そういったそれぞれのインセンティブ・ディスインセンティブについては、今回の会議の資料にも反映できていないところがありますので、今後整理が行えたらと考えております。
また瀧委員からいただいた事例についても大変ありがとうございます。そういった、事務局としても把握できていない例が多数あると考えておりますので、またぜひ委員の皆様から、そういった事例のご提供をいただければと思います。

また板倉委員からご指摘をいただいたところでありますが、今後のスコープをわかりやすくというところ、身元確認・当人認証それぞれ異なるところがあるというところも今回の資料にすべて反映できているところではございませんでしたので、そういった点もきちんと抜け漏れがないようにケアをできればと考えております。

最後の中村委員からのご意見、インセンティブ・ディスインセンティブのところは先ほど触れましたが、Issuer 側が体力のある人で、Verifier 側は場合によっては体力がない多種多様な方がいるというところで、これもどういった証明書によるかというところもあると考えておりますが、そういった先ほどのインセンティブ・ディスインセンティブというところも含めて、これまで以上に、今の紙であるとか、電話で、口頭で、というようなところよりも、トラストを高められるような仕組み、Verifier にとってもインセンティブを受けられるような仕組みを構築できればと考えております。事務局からの反応は以上になります。中村座長にお返しいたします。

（中村素典座長）

ありがとうございます。板倉先生が挙手されていますが、なにかコメントありますでしょうか。

（板倉陽一郎委員）

事務局からのご説明や、富士榮委員のお話にも何回も出てきましたが、こと本人確認という意味ですと、「ある時点で本人確認した」ということしか、VC ではできないわけで、それとブロックチェーンというのはあんまり相性良くないですよね。これが属性の確認に使うということであれば、一生変わらない、学校を卒業しましたという話だとか、剥奪されない資格の話でしたら、ブロックチェーンで消えないというのは良いのかもしれませんが、「ある時点で本人確認しました」という情報が永久に消えないで流通するというのはむしろ混乱を招くわけで、不適切なユースケースなのではと思います。

だから今本人確認をメインに議論しているので、どうしてもそうなってしまいますが、例えば本人確認と関係なく、銀行が提供できるものとしては、この人は VIP ですとか、メンバーシップ等に使いたいというのはあると思う。こういうパターンというのは、普段もアナログで結構やられているわけで、ステータスマッチとか言いますけど、マイルを稼いで上級会員になると、ホテルでも上級会員3ヶ月までお試しできますとか、そういうものには良いかと思いますが、本人確認というのは、何と組み合わせるかという意味ではブロックチェーンは全然相性が良くないのではないかという気がしています。

（中村素典座長）

ありがとうございます。3 つ目の論点に移りたいと思います。先ほどからの議論を踏まえて、推奨される VC の利用形態とは、利用用途やユースケースについて、ご指摘やご意見をお願いいたします。佐古委員お願いいたします。

（佐古委員）

今まで一点目、二点目がかなり本人確認に特化した話だったのでみなさんがおっしゃる通り、消費者保護という観点から運用が厳密にならざるを得ないと思ってお話を聞いていました。

その観点で富士榮さんが当初おっしゃられた、「本人確認に特化した VC には新たな名前をつけるべき」、というところにとても賛成します。私が以前、民間企業で働いていた時に、PKI はかなり厳密な運用をしていたので、私が公開鍵暗号を使ったシステムを提案しても、皆さんが「公開鍵暗号？PKI？ 無理です無理です」と、PKI という3文字を聞いただけでその技術を敬遠するという体験をしたことがあります。

その話はビットコインが出てきて、ビットコインも公開鍵暗号を使っているという事が知られて、少し公開鍵暗号に対する拒否感というのは減ったように思うのですけれども、VC を本人確認用に限定して議論してしまうと、同じようなことが起こるのではないかという心配をしております。VC は単なるデジタルデータに誰かが署名したものを別の人が検証するという手続を、フォーマットとして整備してきたものに過ぎませんので、そういう VC のライトウェイトな使い方、先ほど瀧委員も色々なグラデーションがあるとおっしゃられたと思うのですけれども、色々なグラデーションがあるという使い方を阻害しないように、厳格にやるものと、そうじゃないものが、名称で分けられると良いと思いました。

もう一点コメントがあるのですけれども、先ほどのお題は各種法令・制度・仕組みを踏まえた VC の利用ということですけれども、VC がデジタルで実現されていることによって、従来紙では出来なかったことも出来てくる、先ほど中村委員からもそのような話がありましたけれども、もしかしたら今の法令・制度・仕組みが、ゴールにしていることは消費者保護だったり、公平性だったりというところで、本質はすごく良いところを言っていても、手段まで細かく書いてしまっているところが、無きにしもあらずと理解していますので、本質は保ったまま、デジタルだからこそ、手段は少し異なっても同じようなゴールが実現できるのではないかと思いますので、今までの仕組みを見直すということもこれを契機にできたら良いと思い

ました。

（中村素典座長）
　ありがとうございます。ここのお題が推奨される、という表現になっているのが、デジタル庁的にそういう表現が好ましいのかというところも、なかなか難しい気がするのですけれども、先ほどからご意見が出ていましたように、色々なユースケースの中で注意すべき点とか、従来通りのことをまずは考えてどうすればいいかとか、そういった中で、従来的な取組・活用については、こういう観点で注意しなさいとか、それがさらに将来に向けて、夢が広がるような使い方、あるいは個人認証のような話ではないものについては、特に何か言うものではないですよとか、そのあたりもスタンスを明確にしながら言わないと、安易に推奨という表現を使うのはよくないという気もしますね。
では瀧委員からお願いいたします。

（瀧委員）
　最初に DID/VC 共創コンソーシアム様に行った発言を繰り返してしまうのですけど、右に書いてあるようなところで言うと、請求書は、デジタル署名が伴っていないものがほとんどで、かつそれを受け取った会社はここに本当に振り込んでいいのか、毎回、特に初回の取引の時には、非常に恐れながら送金をしているわけです。
　変な話ですけど、PDF で請求書を受け取るなりして、法人用のインターネットバンキングで数字を打ち込んで、これは正しいのかと考えながら送金して、社名が一応これだから合っているかな、というのでやっているという意味では、非常にペインと言いますか、リスクがそもそもで存在していて、不正利用されている可能性もありえるもので、署名が伴っていないという意味では、ここではかなり満たしているタイプになるのかなとは思った次第です。
　もちろんそれをどうやって添付するべきか、例えば、デジタルインボイスにつけることができるのかとか、デジタルインボイスだから VC ではなくて e シールではないですか、という議論も最近はありますので、やり方には色々あるのですけども、せっかくデジタル庁さんがデジタルインボイスに関しては所管をされているので、これだけでは満たされないところがあって、銀行 API が普及するとか、色々なことも必要になってくるのですけど、推奨というよりはナッジしたい項目の一つかと思いました。
　もう一つ、今のモデルのいいところは、最後リスクを取っているのが送金元になる会社ですよね。なので、大なり小なりビジネスジャッジメントで、犯収法とかではない判断をすることができるという面も良いと思っていまして、事業者さんとしては、どこかで事業が単に楽になる、手間が減ると認識してもらえる良さがある。なので、そういう面でも割とここの最初資料を拝見してすぐに思いついたのはそのユースケースなので、逆にナイーブな意見を言っているかなという部分もあると思いますので、それへの突っ込みも含めて議論が深まると良いなと思い、提示させていただきます。

（中村素典座長）
　ありがとうございます。板倉先生お願いいたします。

（板倉陽一郎委員）
　金融機関が提供できる属性として、反社会的勢力じゃないというのがあったのですけど、それはそもそも良いのかというのがあり、逆は良いのではないかと思うのですよね。つまり、クレジットカード会社に頼むと VIP しか入れないところが取れますといったようなものを運べるというのは割とニーズがあるので

はないかなと言うのと、仮に間違えても、店もお金さえ払ってくれれば損害もないので、そのあたりからやってはいかがですか。つまり VIP メンバーシップ属性の第三者提供ですが、そのやり方は誰もダメージにならないし、少なくとも逃げない。飲食店が口コミだけでやるのは、常連さんを介することによって、お店を予約したのにこないとか、そういうのを防ぐわけですが、銀行からの紹介ということであれば、一般に適当に予約を募るよりは良いお客さんが来るといったようなことで、ニーズがあるし、基本的には飲食店とか、そういう VIP 向けのサービスというのは不特定多数に提供しているわけで、その人がものすごく誰かに興味があるわけではないというところで、リスクも低いので、検討していただいてもいいかと思いました。

（中村素典座長）

ありがとうございます。VC 自体というよりも、ビジネスモデル的な話題にも絡む話なので、そこをどううまく整理するかというところは難しいかなと思いながら、お話は聞いておりましたけれども、そういうところも踏まえながら、うまく VC が普及していくと良いかなというところで、情報提供していけると良いのだろうと思いました。

では3番目の議論のポイントにつきまして、事務局からまとめてコメントがありましたらお願いいたします。

（デジタル庁當波）

事務局でございます。

まず佐古委員からいただきましたご意見については、今回は本人確認に特化した話でありましたので、消費者保護といった観点から厳密な話ばかりになってしまったというところは、まさにその通りであると考えております。これまでの議論においても、様々なレベルでありますとか、グラデーションというご指摘をいただいているところかと思いますが、他のグラデーションにおいては、どういったことに気をつけるべきかというところ、最後の板倉弁護士からいただいたご指摘の中でも、例えば VIP 会員であるということを銀行が証明するのはありなのではないか、最悪お金を払ってさえいただければ良いので、というようなご指摘をいただいたかと思いますが、より軽いユースケースを踏まえた議論に今後広げていくべきなのであろうというふうに考えております。

また、佐古委員からのご指摘で、VC がデジタルであるというところで、これまでできなかったことができるというようなご指摘をいただいたかと思います。最終的なゴールは公平性でありますとか、消費者保護であるとしても、細かく PKI で求めていること全てを求めなければならないというわけではないというご指摘もいただいたかと思います。そういったところも含めて、先ほどの一つ前の論点でも、例えばブロックチェーンであるとか、ほかの技術とどう組み合わせたらどういったことが実現できるというところの話を申し上げたかと思いますが、そういった技術の組み合わせごとの整理というものがさらに必要になっていくのであろうと考えております。また、技術の組み合わせというところにつきましても、そういった形で様々な使われ方、様々な標準の組み合わせが、かなりばらけて出てしまうというところも可能性としてございますので、そういったところを徐々に揃えていくというといったところの営みも今後必要であるのではないかなと考えております。

また瀧委員からご指摘をいただいたところで請求書の事例をいただいたかと思います。そういったユースケース、これまで署名が伴っていなかったユースケース、特に請求書でありますとか、金銭が絡むようなユースケースの場合は、例えば PDF の請求書に署名が伴っていたとしても、例えば金額を手打ちで打ち込んで 0 の桁を間違えたら事故が起こるというようなところ、機械可読であるからこそのユース

ケースもあるかと思いますので、そういったところを踏まえて、今後整理を行いたいと考えております。
　板倉弁護士からのご指摘は先ほども触れたかと思います。事務局からの反応は以上になります。中村座長にお返しいたします。

（中村素典座長）
　ありがとうございました。本日の議論のポイント3つにつきましては、一通り議論させていただいたかと思いますので、以上で事務局にお返ししたいと思います。

　（デジタル庁石井）
ありがとうございました。それでは本会議の閉会にあたり、事務局を代表してデジタル庁デジタル社会共通機能グループ長、楠よりご挨拶申し上げます。

（デジタル庁楠）
　どうもお世話になっております。デジタル庁の楠です。
　まず、委員の皆様におかれましては、活発にご議論いただきましてありがとうございました。ゲストとしてご参加いただいた DID/VC 共創コンソーシアム様、またマイナウォレット様におかれましては、実際に民間で取り組まれているユースケースをはじめとして、民間で抱えていらっしゃる課題についてご紹介いただきましてありがとうございました。
　なかなか難しいなと思うのが、二昔前であれば役所はルールを作ってから、いろんなサービスが世に出てくるという順番でしたけども、最近は FinTech にしても、RegTech にしても、AI エージェントのような、色々な新しいものも出てくる中で、役所のスピードとは関係なく、民間とか世界中からどんどん色々な新しいものが出てくる中で、役所として振り落とされないように考えていかないといけないと。こういう意味で法律も見直すべきところがあれば、どんどん見直していくべきだと思う一方で、PKI の教訓の話もいろいろと出てきましたけれども、我々も認定認証局がなかなか伸びない中で、世の中的には WebPKI であれ、コードサイニングであれ、立会人型の電子契約であれ、色々なものがどんどん伸びてきた歴史というのも、このコロナ禍でもあったわけでして、これから行政としてどういった関わり方をしていくか、民間の活動をきちんとエンカレッジして、イノベーションを促進していけるか、というところは、色々と悩みながら進んでいるというところもあるのかなと思います。
　今日主に話題に上がった本人確認は、犯収法をはじめとして、法律で厳格に手続を決めている分野でもありますので、これはしっかりとリスクを踏まえて、議論を詰めていかないことには、具体的な規制改革につなげていくということは、難しい部分というのはある一方で、それ以外にも、データの内容を容易に検証できるようになることで、今よりももっと便利で効率的にできることは実はいっぱいあるのではないかというようなご提案もあったかなと考えております。
　来年度、具体的に私共として、どういうふうに活動していくかというのはこれからの話になりますけれども、本日皆様からいただいたご意見やご提案も踏まえて、今後の活動に生かしてまいりたいと考えておりますので、引き続きご指導ご鞭撻のほど、何卒よろしくお願いいたします。

（デジタル庁石井）
　ありがとうございました。本日いただいたご意見は、次回以降の議題や方針に反映してまいります。本日の議事録につきましては、後日、委員の皆様にご確認いただいた後、デジタル庁ウェブサイトにて公表させていただきます。

また、次回会合の開催を含む今後の方針につきましては、本日、ご議論いただいた内容を整理するため、一度事務局にて持ち帰らせていただいた後、改めてご案内いたします。委員の皆様におかれましては、引き続きどうぞよろしくお願いいたします。

以上をもちまして、「Verifiable Credential（VC/VDC）の活用におけるガバナンスに関する有識者会議（第 1 回）」を終了いたします。ありがとうございました。

以上